THE PRIVACY FALLACY

HARM AND POWER IN THE INFORMATION ECONOMY

IGNACIO COFONE

THE PRIVACY FALLACY

Our privacy is besieged by tech companies. Companies can do this because our laws are built on outdated ideas that trap lawmakers, regulators, and courts into wrong assumptions about privacy, resulting in ineffective protections to one of the most pressing concerns of our generation. Drawing on behavioral science, sociology, and economics, Ignacio Cofone challenges existing laws and reform proposals, and dispels enduring misconceptions about data-driven interactions. This exploration offers readers a holistic view of why current laws and regulations fail to protect us against corporate digital harms, particularly those created by AI. Cofone proposes a better response: meaningful accountability for the consequences of corporate data practices, which ultimately entails creating a new type of liability that recognizes the value of privacy.

Ignacio Cofone is the Canada Research Chair in AI Law & Data Governance at McGill University, Montreal, and an affiliated fellow at the Yale Law School Information Society Project. He writes about how the law should adapt to technological and economic change with a focus on privacy and AI.

The Privacy Fallacy

HARM AND POWER IN THE INFORMATION ECONOMY

IGNACIO COFONE
McGill University

CAMBRIDGE
UNIVERSITY PRESS

Shaftesbury Road, Cambridge CB2 8EA, United Kingdom

One Liberty Plaza, 20th Floor, New York, NY 10006, USA

477 Williamstown Road, Port Melbourne, VIC 3207, Australia

314–321, 3rd Floor, Plot 3, Splendor Forum, Jasola District Centre, New Delhi – 110025, India

103 Penang Road, #05–06/07, Visioncrest Commercial, Singapore 238467

Cambridge University Press is part of Cambridge University Press & Assessment, a department of the University of Cambridge.

We share the University's mission to contribute to society through the pursuit of education, learning and research at the highest international levels of excellence.

www.cambridge.org
Information on this title: www.cambridge.org/9781316518113

DOI: 10.1017/9781108995825

First published 2024

A catalogue record for this publication is available from the British Library

A Cataloging-in-Publication data record for this book is available from the Library of Congress

ISBN 978-1-316-51811-3 Hardback
ISBN 978-1-108-99544-3 Paperback

To my parents

Contents

Acknowledgments

One of the most wonderful aspects of being an academic is having the opportunity to spend time discussing ideas with brilliant people. I'm enormously grateful, first of all, for the feedback and comments from colleagues and friends who read all or parts of this book. Thank you Gilad Abiri, Jeremias Adams-Prassl, Nikita Aggarwal, BJ Ard, Lisa Austin, Jordan Axt, Rafael Bezerra Nunes, Jody Blanke, Johannes Buchheim, Miriam Buiten, Ryan Calo, Stefanie Carsley, Celine Castets-Renard, Rebecca Crootof, Isa Crosta, Luciana Debenedetti, Pierre-Luc Déziel, Jaye Ellis, Evan Fox-Decent, Vincent Gautrais, Fabien Gélinas, Nikolas Guggenberger, Sebastián Guidi, Claudia Haupt, Chris Hoofnagle, Yoel Inbar, Richard Janda, Lindsay Juarez, Thomas Kadri, Margot Kaminski, Prachi Khandekar, Ido Kilovaty, Adrian Kuenzler, Stephanie Leary, Asaf Lubin, Orla Lynskey, Miguel Ignacio Mamone, Marie Manikis, Kirsten Martin, Pierre-Emmanuel Moyse, Paul Ohm, Frank Pasquale, Przemyslaw Palka, Jen Raso, Yan Shvartzshnaider, Kristen Thomasen, Scott Skinner-Thomson, Andrea Slane, Rob Spear, Katherine Strandburg, Thomas Streinz, Nicolas Vermeys, Mark Verstraete, Ari Waldman, Daniel Weinstock, Felix Wu, and Angela Zorro Medina. Their reactions and challenges helped me improve this work significantly.

I'm lucky to work with fabulous colleagues and students at McGill. My colleague Evan Fox-Decent generously organized a manuscript workshop where I received invaluable feedback, much of it from people mentioned above. Students in the Privacy Law classes of 2020, 2021, and 2022 provided insightful comments and challenging questions. More broadly, I'm thankful to McGill University Faculty of Law, and its dean, Robert Leckey, for continued support and encouragement, and likewise to the Canada Research Chairs program of the Social Sciences and Humanities Research Council for providing research funding. I'm particularly thankful to twelve wonderful research assistants, Keira Chadwick, Henry Coomes, Ihsan Dalaban, Andie Hoang, Stephanie Kay, Adelise Lalande, Ana Qarri, Emma Sitland, Gajanan Velupillai, Aidan Wall, Jeremy Wiener, and Alessia Zornetta, who read and commented on the manuscript, helping me clarify and sharpen ideas. My Cambridge University Press editor, Matt Gallaway, provided valuable guidance throughout the process.

I could only write this because bright scholars have written a monumental body of work and created a vibrant conversation on privacy, data protection, and AI. It would be an omission not to thank this group of people from whom I continuously learn by listening and discussing early ideas, particularly at the yearly Privacy Law Scholars Conference. While members of this community are too many to name individually, Danielle Citron, Chris Hoofnagle, Daniel Solove, and Ari Waldman deserve a special mention.

The book has also benefited from people who offered their time providing perceptive feedback to the ideas that formed it, either after reading a paper I sent them or during talks at which I presented them. I benefited enormously from discussing the papers that formed this book's building blocks at workshops and conferences from 2016 to 2022. For every comment that was too deep, too complicated, or too comparative, I reassured myself by thinking "it'll go in a book." And some of them made it. Usual suspects for these extra-challenging points that help make my work better have been Ian Ayres, Jack Balkin, Woodrow Hartzog, Helen Nissenbaum, Neil Richards, Adriana Robertson, and Katherine Strandburg.

Finally, I'm grateful to my partner Rob and my family back in Buenos Aires for their unwavering support and enormous patience. And for all the coffee.

Abbreviations

AI	Artificial Intelligence
CCPA	California Consumer Privacy Act
CEO	Chief Executive Officer
EU	European Union
FCC	US Federal Communications Commission
FIPs	Fair Information Principles, or Fair Information Practice Principles
FTC	US Federal Trade Commission
GDPR	General Data Protection Regulation
ICO	UK Information Commissioner's Office
ISP	Internet Service Provider
OECD	Organisation for Economic Co-operation and Development
UK	United Kingdom
US	United States

Introduction

In September 2010, eighteen-year-old Tyler Clementi, a freshman at Rutgers University, was filmed secretly through his bedroom webcam while making out with another man. The video, taken by his roommate, was then distributed through Twitter and among students at his school. When Tyler had a second date, a group of students organized a viewing party to watch footage from a hidden camera.[1] Tyler was ridiculed. His sexuality was exploited for fun. After the incidents, he jumped to his death from a bridge into the Hudson River.

It's tempting to misconstrue the harm caused to Tyler as the result of an individual actor – his roommate. But it's inaccurate.[2] The harm was collective and it was enabled by a slew of digital services and devices we use daily, provided for profit. While blameworthy, Tyler's roommate and classmates were part of a digital ecosystem that, dismissing value in people's privacy, creates enormous tangible and intangible harm.[3] From 2010 to today, this system of unfettered collection and sharing only got larger, more sophisticated, more profitable, and more harmful.

All your interactions, movements, and decisions are collected in real time and attached to profiles used by advertisers to compete for your attention. Not because they think you're special or because they're interested in learning about you for the sake of getting to know you, but because, regardless of your age, gender, or country of origin, you're monetizable. When combined, these little pieces of ourselves fuel a trillion-dollar industry that threatens livelihoods, lives, and democratic institutions.

The worst part is not that we get little in exchange. It's that, much like companies that pollute the atmosphere or that offshore production to places where they can violate workers' human rights, every step of the data industry creates losses and harms that are opaque but real. Companies that collect, process, and sell our personal information create harms that are out of sight but have dire consequences for those affected.

Clara Sorrenti experienced firsthand the consequences of data harms. She received death threats, had her home address found and shared, saw intimate documents about her family revealed, and was "swatted" – the practice of falsely reporting a police emergency to send armed units to an innocent person's home,

an experience that for Clara ended up with an assault rifle pointed at her head.[4] Clara was a victim of Kiwi Farms, a platform that coordinates the gathering of information available online to target trans people.[5] For the law to consider that you harassed someone, you need to contact them several times. So, if a platform pools information and coordinates people who each contact a victim once, as was the case for Clara, it produces harassment while avoiding its legal definition. Describing her experience, Clara explained: "When you get your own thread on Kiwi Farms it means there are enough people who are interested in engaging in a long-term harassment campaign against you."[6] She left her home after the swatting incident, but Kiwi Farms found her by comparing hotel bedsheet patterns from a picture she took with information available online.[7] Clara fled the country to escape abuse and Kiwi Farms found her again.[8]

Viewing Clara's harassment as the work of a few bad individuals ignores a broader systemic problem. In our digital ecosystem, it's easy to obtain and use our data in ways that inflict harm on us – like a roommate exploiting a teenager's sexuality for entertainment or a website exploiting trans women's physical safety for dollars. Because Tyler and Clara's harms weren't just a result of individual trolls, but rather emblematic of an ecosystem that enables and magnifies data harms, Tyler and Clara's situations are not exceptional.[9] Part of what's shocking about their stories is that they faced enormous harm from something as common as webcams and blogs.

Data harms differ. Some are visible and affect people such as Clara on an individualized basis, with immediate consequences on their livelihood. Daily victims include women facing online harassment and abuse, racialized individuals experiencing magnified systemic discrimination, and anyone going through identity theft because their financial information was taken without their knowledge.[10] Most harms in the information economy, however, are opaque and widely dispersed. Examples are online manipulation to make personal and financial choices against our best interests (called "dark patterns") and the normalization of surveillance to constantly extract personal data (called "data mining").[11]

Tyler and Clara were pulled into the information economy – the trillion-dollar industry fueled by the collection, processing, and sharing of personal information to produce digital products and services.[12] When we look at data interactions, we sometimes forget that it's there. For example, in nonconsensual distribution of intimate images, there's a tendency to concentrate all blame on the first perpetrator. But when intimate photos go viral, that means hundreds of people reposted them and websites derived ad or subscription profit from them.[13] Victims are harmed because there's a data ecosystem that facilitates and encourages it. The information economy enables corporations and individuals to instrumentalize others for their own gain – and it amplifies them.[14] So cases of one perpetrator and one victim barely exist. We lack accountability over what happens with our data and what harms happen to us because of our data. By having a better picture of that data ecosystem, laws can better reduce and repair data harms.

This book builds on academic and policy critiques to privacy law, which is the body of law that governs the collection, processing, and sharing of personal information. It explores these critiques' consequences to explain where privacy laws fall short when it comes to the information economy and how their shortcomings relate. It then proposes what we could do about it.

The central problem is the following: privacy law across the world – including in the United States (US), the European Union (EU), and countries that modeled their privacy laws on either of them – is based on regulations designed for contract-like relationships. The foundations of privacy law therefore rest on two critical assumptions: that people can freely and rationally make data decisions that increase their wellbeing and that legislators can design rules that anticipate and prevent data harms. Neither of these assumptions is true. Further, privacy law fails us because it relies on false assumptions about how people behave and what people believe regarding their privacy.

Facebook serves as an example. In 2016, shortly before the Cambridge Analytica scandal, journalists uncovered that Facebook had been facilitating housing discrimination. Facebook's software made it possible for advertisers to filter who saw their ads by race, gender, nationality, and other protected characteristics. Marketers used this feature to avoid showing housing ads to racialized users and have whiter tenants.[15] The US National Fair Housing Alliance sued, supported by law enforcement.[16] After it did, Facebook agreed to remove its "ethnic affinity" filter.[17] But the information that Facebook has about its users is so detailed and nuanced that this hardly made a difference. For example, advertisers can't filter by who's Latinx, but they can filter by who likes Telemundo. Advertisers can't filter by who's gay, but they can filter by who likes gay tourism websites. And advertisers can filter by "multicultural affinity."[18] Facebook continues to classify its users by over 5,000 categories, some of which enable indirect discrimination.[19] The company didn't eliminate discrimination; it just hid it. Because of the host of information it collects and infers, the company has enough power to discriminate while complying with antidiscrimination and privacy law. The issue isn't unique to housing or to Facebook, but common to platforms that can weaponize information about us to selectively expose us to opportunities, turning our information against us.[20]

The international tendency to base privacy law on consent models from contract law is most extreme in the US. Omri Ben-Shahar and Lior Strahilevitz once described the tendency as "a quiet legal transformation whereby the entire area of data privacy law has been subsumed by consumer contract law."[21] In the EU and countries with EU-inspired data protection laws, similarly, laws hinge on individual consent and individual control – as if the relationships were in a market.[22] In both cases, laws' framework is founded on the notion of bilateral commercial relationships. The underlying dynamic for the contractual view is that there's a trade in which people agree to give up their personal information in exchange for a service. There's not.

In contrast to privacy law's assumptions, we mechanically click "I agree" on documents that would be unhelpful to us even if we read and understood them.[23] We do so for a wide range of corporations, such as websites, apps, and internet service providers (ISPs) that profit from our data. To supplement these agreements, governments make long checklists for corporations to tick to achieve legal compliance. But, as Facebook did when enabling discrimination, corporations cause enormous individual and social harm, often while remaining compliant.[24] Corporations obtain meaningless "I agree" clicks, performatively comply with checklists, and continue business as usual.[25]

This book's core premise is that, rather than grounding privacy law on concepts from contract law, which sets the rules for voluntary agreements, we need to ground it on concepts from tort law, which sets the rules for harms caused to others.[26] This premise may sound technical, but the reasons justifying it are intuitive because they respond to the social reality we all live in. Contract law works well for standard exchanges and agreements, like when we buy groceries or hire the services of a dry-cleaner. But the mutual understanding and agreement on the specifics of an interaction central to contract law (what legal scholars call a "meeting of the minds") doesn't exist in privacy. Privacy agreements' subject matter is opaque to the people they involve. We don't know what we give up in data interactions – like Clara couldn't predict being found from a nondescriptive picture.[27] And many companies that hold our data never interacted with us in the first place – like Tyler, who had no Twitter account.[28] By exerting power over people both within and beyond empty agreements, corporations do mass harms, including but not limited to their users.

The result of the mismatch between laws' assumptions and social reality is that corporations are free to exploit people whose information they collect, process, and share. They can do so by misusing their information for financial gain (data misconduct) and profiting from people's data without keeping it safe (lack of data security). Technologies that make it easier to analyze large amounts of data facilitate this type of exploitation. The increasing reliance on artificial intelligence (AI) for processing data and our increasing dependence on data-mediated social and economic interactions make exploitation a serious concern for what our society may soon become. The corollary is that solutions must involve substantive reform. We need to rethink the building blocks of privacy protections in the private sector.

Given the failure of the current model, the book proposes a program for building meaningful accountability into the information economy through liability for individual and group harms. Law's framework should move to one of compensating harms that occur outside mutually beneficial agreements. This program departs from existing laws and liability proposals, which focus liability on breaches of procedural rules or individual agreements. These breaches are too narrow to capture the different and unpredictable ways in which people can be harmed and exploited. To overcome these problems, the book proposes a theory of harm and exploitation that addresses common concerns with liability, such as standing, causation, class certification, and compensation.

The needed changes extend to regulatory reform. Regulations should complement harm-based liability regimes by focusing on systemic risks. Regulations must match the right type of underlying relationships and power dynamics. The changes this book proposes would depart from the current focus on individual rights for controlling personal information. Regulations that reinforce individual control are unhelpful because they implicitly rely on a contractual "meeting of the minds," and laws can't reinforce something when it doesn't exist. Individual choices and individual control rights that provide people with options can't meet this imperative because they elide an array of social harms.[29] Patching the current system with additions that uphold its underlying contractual logic, like the right to data portability or the right to be forgotten, is a band-aid solution, rather than a cure. Regulators are well positioned to reduce systemic risk and the magnitude of widespread harms, which requires looking into and moderating the power dynamics embedded in data practices' business models.[30]

The type of liability developed is crucial for achieving accountability. Liability proposals so far suggest compensation when corporations break a promise made in their terms of agreement or undertake an activity prohibited by a procedural rule. These forms of liability are contract-like, similar to liability arising from breach of contract or breach of a legislated mandatory contractual clause. They fail to reduce harm because they rely on similarly flawed assumptions over underlying dynamics. Data harms are different; they resemble mass harms addressed by modern tort law, such as environmental harms.[31] To address them, privacy law needs to hold corporations accountable through tort-type liability. Protection requires that corporations are held accountable for the consequences of their data practices – not for the checklists they complete or the notices they send.

The pervasive data harms that exist in the information economy show that this type of accountability needs to be at the center of the protection system, rather than an add-on to the system's enforcement. Recently, privacy scholars developed other calls for consequence-focused meaningful accountability, such as information fiduciaries, privacy by design, and relationships of trust.[32] This proposal builds on their motivations and is compatible with their implementation. They all respond to a social phenomenon that took off just under twenty years ago.

If you're old enough to remember one of the first-ever cases of viral information sharing, you may remember that it happened because hundreds of entities exploited and humiliated a woman for private gain. Twenty-four-year-old Monica Lewinsky found herself at the center of the news over her affair with President Bill Clinton. Lewinsky discovered the cost of artificially inflated shame for profit.[33] The more shame and scandal created, the more clicks they received. And the more clicks, the more ad revenue. Clinton's infidelity may have been newsworthy, but hundreds of memes, posts, photos, and commentaries made it about her. Lewinsky wasn't a public figure, but rather an intern in a relationship characterized by an exorbitant power differential. As she explains, people "plastered photos of me all over to sell newspapers, banners online, and to keep people plastered to

the tv … the attention and judgment I personally received was unprecedented."[34] Lewinsky, like Clara, was not harmed by a specific individual, but rather by an aggregation that the information economy's incentives structure enables and fosters. Back then, there was barely a name to designate what she went through. We now call what hundreds of individuals did to her "online harassment." We still lack a name for the systemic effect.

Traditionally, when laws and courts address privacy issues, they focus on tangible consequences. This is true whether the problem is a data breach, like when a company is hacked, or the violation of a data right, such as the right to know what information a company has about you. This important but insufficient conception contemplates financial harm such as loss of money, loss of reputation that damages one's employment relationships, and, in some cases, physical consequences, such as harm to one's health or safety. Privacy laws attempt to foresee and prevent these harms.

Modern data practices changed things. They introduced complicated power dynamics where corporations use people's information, often with the help of AI, to make decisions about their opportunities and experiences. Modern data practices also allow harms to arise between parties who never interacted with one another, such as harms from data brokers, who buy your data to aggregate it and sell a profile about you to others.[35] Through these power dynamics, modern data practices introduced and fuel informational exploitation, a different type of data harm that involves profiting from people's information with disregard for the harm that it causes them. Informational exploitation differs from other data harms in that it's systemic, it's opaque, and it facilitates, while simultaneously hiding, other harms. Informational exploitation is the systemic effect that Lewinsky was put through.

Surveillance that facilitates exploitation is easier, cheaper, more pervasive, and less evident than ever before. Practically every time you interact with a screen, your clicks are monitored, what you look at is recorded, your activity is surreptitiously linked to your identity, your information is traded, and all of it is aggregated with information from others. Most significantly, statistical inferences are constantly made about you and the groups you belong to. This dynamic gives hundreds of corporate entities power over you.

To address the systemic effects that new relationships of power produce, we must identify privacy-violating data practices by connecting them with the reasons for which we value privacy. Privacy is a social value, so it's about more than preventing negative tangible consequences.[36] Protecting privacy is important for building trust, preserving autonomy, and maintaining relationships. It protects us from emotional harm, such as distress and anxiety. Numerous theories of privacy explain what privacy is and why we protect it, underscoring its relationship with intimacy, autonomy, personhood, and trust. These theories show that privacy has intrinsic and instrumental value: it has independent social value and it protects people from other harms, such as financial fraud and physical violence.

This book doesn't advance a new concept of privacy. Rather, it builds on these concepts of privacy, together with lessons from behavioral science, economics, psychology, and sociology, to better design the system that protects people. Its proposals apply to different conceptions of privacy, which can be advantageous for advancing policy arguments in light of differing views.[37] The problems of the traditional protection system, as well as the need for accountability for data practices' consequences, apply across privacy theories because all those theories recognize that there's something in privacy worth protecting.[38] An accountability program based on privacy harm just requires recognizing that there's something valuable in privacy that can be subjected to systemic loss and harm.

The privacy fallacy causes us to miss that value. This fallacy refers to the disjuncture between a notion that privacy has value in and of itself and the conviction that, at the moment of protection, only tangible consequences – like physical or economic harm – are real, concluding that privacy can be sufficiently protected by preventing those outcomes. It contains a contradiction, because the idea that privacy has intrinsic value implies that there's a value in privacy that can be harmed, even absent physical or economic consequences. Opinion leaders succumb to the privacy fallacy when they solely address privacy's instrumental consequences in a particular issue and subsequently claim to have successfully protected privacy, dismissing the loss of privacy's social value. Thinking that preventing Tyler Clementi's suicide would have solved his invasion of privacy, for example, would be falling for the privacy fallacy. Regulators and industry members do so when they understand and endorse the value of privacy in theory, but forget about it in practice. Authorities fall into the fallacy when their protection regimes only recognize the tangible consequences of privacy losses, while politicians repeatedly remind people of the value of privacy. People fall into the fallacy when they say that, even though privacy is important in general, you shouldn't worry about it in a specific situation if you have "nothing to hide."

In its most popular and most dangerous form, the privacy fallacy is used to argue that each individual should protect themselves from those tangible consequences. It overlooks the loss of privacy's social value and how, in any information interaction, we affect each other. Traditional laws buy into the privacy fallacy by committing to the idea that it must treat people as hypothetically rational and perfectly informed entities and that, absent physical harm or financial fraud, their own choices will protect them from harm in the information economy. Public policy efforts buy into this fallacy by building on the mistaken belief that, by adding procedural requirements, people will at some point take control over their data. This approach pays lip service to privacy. It creates the illusion that we're moving forward and legislators are placing strict requirements on corporations that will, one day, achieve individual control. Though, even if regulators did provide individual control for people to prevent tangible consequences, the privacy values they claim to protect would remain unprotected.

* * *

The book develops this argument in seven chapters.

Chapter 1 ties together problems in central elements of privacy law: the individual choice-based system, the fair information principles that originated it, the view that privacy is about secrecy, and dichotomies such as public versus private. We don't have actual choices about our data beyond mechanically agreeing to privacy policies because we lack outside options and information, such as what each choice means and what risk we're taking on by agreeing. The choice-based approach creates a false binary of secret versus public information when, in reality, privacy is a spectrum. The idea that someone, at any given time, has either total privacy or no privacy at all is unfounded. Additionally, data are bundled: you can't reveal just one thing without letting companies learn other things. Reckoning with this reality defeats the popular "I have nothing to hide" argument, which traces back to Joseph Goebbels.

Chapter 2 shows the falseness of two ideas that underlie the central elements of privacy law: that people make fully rational privacy choices and that they don't care about their privacy. These notions create a dissonance between law and reality, which prevents laws from providing meaningful protection. Contrary to rationality, context has an outsized impact on our privacy decisions and we can't understand what risks are involved in our privacy "choices," particularly with AI inferences. The notion that we're apathetic is prevalent in popular discourse about how much people share online and the academic literature about "the privacy paradox." Dismantling the myth of apathy shows that there's no privacy paradox. People simply face uncertainty and unknowable risks. People make privacy choices in a context of anti-privacy design, such as dark patterns. In this process, we're manipulated by corporations, who are more aware of our biases than regulators are.

Chapter 3 shows why the contracts model doesn't work: consent in the information economy is an illusion. Inferences, relational data, and de-identified data aren't captured by consent provisions. Consent is unattainable in the information economy more broadly because the dynamic between corporations and users is plagued with uneven knowledge, inequality, and a lack of choices. Privacy harm can't be seen as a risk that people accept in exchange for a service. Data harms are collective and unknowable, making individual choices to reduce them impossible. Worse, privacy has a moral hazard problem: corporations have incentives to behave against our best interests, creating profitable harms after obtaining agreements. Privacy's moral hazard leads to informational exploitation. A manifestation of valid privacy consent is consent refusals among individuals. We can consider them by thinking of people's data as part of them, as their bodies are.

Chapter 4 delves into two modern efforts to reinforce individual consent: opt-in and informed choice. It illustrates why, in the information economy, they also fail. Power asymmetries enable systemic manipulation in the design of digital products and services. Manipulation by design thwarts improved consent provisions, interfering with people's decision-making. People's choices regarding their privacy are determined by the designs of the systems with which they interact. European and

American attempts to regulate manipulation by changing tracking from opt-out to opt-in and reinforcing information crash against the illusion of consent. Contract law doctrines that aim to reduce manipulation are unsuitable because they assume mutually beneficial agreements, and privacy policies are neither mutually beneficial or agreements. Best efforts to strengthen meaningful consent and choice, even where policies are specifically intended to protect users, are ultimately insufficient because of the environment in which privacy "decisions" take place.

Chapter 5 examines traditional data protection law's regulatory structure in light of these considerations. It shows why data protection rights and rules, while desirable, don't address the core problems of the contracts model and can't work well without the liability model. Data protection rights unintendedly impose administrative burdens on those they protect. Mandatory rules address power asymmetries and manipulation better than defaults. But our procedural rules overregulate while they underprotect: they benefit large players by adversely affecting new players and they allow companies to comply merely by following box-ticking exercises. Against this backdrop, laws legitimize exploitation that can be executed while remaining compliant. Risk-reduction approaches based on standards can reduce informational exploitation more effectively.

Chapter 6 explores a different path: building privacy law on liability. Liability for tangible and intangible privacy harm would improve our protection systems. To achieve meaningful liability, though, laws must compensate privacy harm, not just the tangible consequences that stem from it. Compensation for financial and physical harms produced by the collection, processing, or sharing of data is important but insufficient. The proposed liability framework would address informational exploitation by making companies internalize risk. It would deter and remedy socially detrimental data practices, rather than chasing elusive individual control aims. Applying it, courts and regulators can distinguish harmful losses from benign ones by examining them on the basis of contextual and normative social values. By focusing on harm, privacy liability would overcome its current problems of causation quagmires and frivolous lawsuits.

Chapter 7 proposes how the liability framework should be implemented. Harm liability can flow from a statutory standard or local tort law. This focus allows liability to complement, rather than replicate, public enforcement. The quantum of liability should depend on the harm incurred by the victim, rather than on the wrongfulness of the perpetrator's conduct or the consequences that the perpetrator foresaw. Because harms are often dispersed, privacy liability is most effective as part of a mechanism of collective redress, such as class actions. Considering privacy problems at scale, we need a framework recognizing mass privacy effects for regulators and courts. A robust notion of loss and intrinsic harm can address problems of insufficient compensation and uncertainties in class certification.

* * *

The information economy is formed by entities that profit from people's data and the people whose data those entities profit from. The corporate entities in the information economy are varied. They're websites, apps, advertising companies, product designers, social networks, data brokers, search engines, and manufacturers of Internet of Things devices, among others. Many, but not all, are tech giants. Often, I'll refer to a specific type of entity, but when discussing all of them I'll refer to "corporations" or "companies." Similarly, I'll refer to "users" as a shorthand when referring to those who use an app or platform. But the more accurate term would be "affected parties" because sometimes we're part of the information economy without using any service at all. Sometimes we engage in the information economy as "consumers," but we're not only affected while consuming something. For example, someone else can share data about us. EU law uses the term "data subjects" to stress that individuals are the key actors. But "data subjects" are seen in discrete ways, making it seem as if we're detached individuals with different interests, as opposed to an interrelated group whose actions affect each other because they're connected by data.[39] Because everyone's data is part of the information economy, most times I'll refer to "people."

The world changed significantly since 1973, when privacy law was conceptualized. Our new environment necessitates a different approach to privacy than what was conceived back then. Privacy law's challenge is no longer regulating individual choices, but rather regulating relationships of power.[40] And addressing power doesn't require presenting choices to the powerless. Addressing power requires holding the powerful accountable for the consequences of what they do.[41]

There's an old Silicon Valley mantra to "move fast and break things," encouraging disruption regardless of risk.[42] Privacy harms today are more pervasive and significant than those that took place back then. Data's central role in our economy and the increasing role of AI inferences in our daily lives will continue to accelerate this drift. The law needs a solution that allows for technological, economic, and social progress while protecting people from being turned into collateral damage. To move privacy law forward, we must abandon the old contractual paradigm and try something more difficult: holding corporations responsible for the things (and people) they break. Taking harm and exploitation in the information economy seriously is overdue.

1

The Traditionalist Approach to Privacy

Imagine you notice someone is following you on your way to work one morning. You find it concerning, but brush it off. Then another stranger follows you to the gym in the afternoon. You get worried, but carry on with your day. You eventually find out that the two share notes with each other, and become shocked. You finally become scared when you find out that everyone you spoke with that day also took notes about you during casual conversations and reported back to the strangers. This, essentially, already happens. Only it's devices like your phone, laptop, and smart home devices that do the tracking. And it's every written communication that gets recorded – unless you have devices with mics, and then it's the spoken ones too.

Privacy law emerged without the Internet or AI and evolved without revisiting its core assumptions. As a result, it's stuck in time. Core concepts in privacy law no longer correspond with daily social interactions in the information economy.

Privacy law across the world is grounded on ideas from nineteenth-century neoclassical economics of contracts – what I call "the traditionalist approach to privacy." Neoclassical economics makes assumptions about how people behave in market exchanges: it assumes people behave rationally, optimizing choices for their own wellbeing based on available information. These assumptions permeate how the law addresses commercial interactions. In many contexts, such as in mergers and acquisitions, the stock market, and most commercial contracts, these assumptions are helpful. In other contexts, such as in parent–child caregiving, less so. When the law uses the wrong assumptions, placing weight on them can impede it from protecting the vulnerable parties that it's meant to protect.

These assumptions don't reflect the reality of contemporary data interactions.[1] Yet the law places enormous weight on them. They dictate the law's worldview about how people make privacy choices (rationally, in an informed way), how people use their privacy (to keep secrets), what activities underly (bilateral commercial transactions), and how people's privacy ought to be protected (by providing more choices).

This book explores the myths that the neoclassical contracts conception creates and how privacy law can and should overcome their obstacles. It argues that the traditionalist approach led privacy law to ineffectively build on concepts from contract

law and shows how it can and should build on concepts from tort law instead. It attempts to chart how to change the foundations of privacy law to move toward a paradigm that protects real-life people in the twenty-first-century economy.

A FORCING PEOPLE TO CHOOSE

In their song "Freewill," rock band Rush says that "If you choose not to decide, you still have made a choice."[2] The idea comes from a famous quote from philosopher Jean-Paul Sartre, who emphasized that not choosing is, in itself, an important choice.[3] The information economy deprives us of this choice. Every day, we must make decisions about our personal information that we're not prepared to make.

Notices, Choices, and Self-management

As you diligently read the Amazon Web Services Terms & Conditions before agreeing to them, you probably noticed a curious clause in its gaming section. The clause indicates that a limitation won't apply "in the event of the occurrence (certified by the United States Centers for Disease Control or successor body) of a widespread viral infection transmitted via bites or contact with bodily fluids that causes human corpses to reanimate and seek to consume living human flesh, blood, brain or nerve tissue and is likely to result in the fall of organised civilization."[4] Technically, you consented to a way of certifying a zombie apocalypse.

The idea of valid consent (often called meaningful or informed consent) is pivotal in privacy law.[5] With limited exceptions, over the past fifty years individuals' consent has been the main basis to collect, process, or share their personal information, forming the bedrock of corporate privacy practices.[6]

Legislatures around the world are guided by the primacy of individual consent when establishing the default legal basis for collecting, processing, and sharing people's personal information. When discussing how to update data protection law, EU Justice Commissioner Julia Fioretti asserted that "[c]itizens should have more possibilities, more chances to be the masters of their personal data, to be informed on what somebody does with their personal data."[7] In 2012, the US Federal Trade Commission (FTC) proposed changes in US privacy law to give people "the ability to make decisions about their data at a relevant time and context."[8] A White House effort that year aimed for people to have "clear and simple choices, presented at times and in ways that enable consumers to make meaningful decisions about personal data collection, use, and disclosure."[9] As early as the 1990s, the Canadian government held that notice and consent "are the core values in any personal information code."[10]

Recent modernization efforts are also guided by individual consent as their gold standard. Press releases of the European Parliament state that people "should have full control over their data and be empowered to take decisions about it."[11] The interpretative authority for the EU Data Protection Directive repeatedly stated that

control over personal information is central to data protection, where control is achieved through consent.[12] In 2021, the Canadian government proposed to overhaul its private-sector privacy regime to "enhance consumer control by requiring organizations to get meaningful consent from Canadians."[13] The Australian Information Commissioner's website states that "Consumer consent for the collection, use, and disclosure of their data is the [law's] foundation … ensuring they can direct where their data goes to obtain the most value."[14]

The main way for companies to obtain our consent and for us to manage our privacy is through "privacy notices."[15] These notices are privacy policies or terms of service that corporations share with their users to explain how they collect, process, and disclose personal information, asking their users to agree to them. Privacy notices capture individual consent as the key to unlocking the data practices described in them.

Privacy notices, and the promises companies make in them, are central to privacy law globally. The global popularity of this practice may be linked to how it embraces a common regulatory approach: give people control (in this case, over their information) so they take care of themselves.[16] After all, that's how the law deals with most of our possessions, from apples to non-fungible tokens (NFTs). The history of how this practice took over our information dates back to 1973.

The Fair Information Principles

Every time you download a new app on your phone, you're asked to agree to its terms of service. The reason dates back to the early days when the world worried about the digitization of personal data and developed the 1973 Fair Information Principles (or Fair Information Practice Principles, usually referred to as the FIPs) to address it.

The FIPs have slowly become synonymous with privacy law. As their name indicates, the FIPs aim to make practices relating to peoples' personal information fairer.[17] They were initially principles developed in an American advisory committee report as guidelines for the private sector.[18] Rapidly growing out of that report, they became FTC guidelines, Organisation for Economic Co-operation and Development (OECD) international guidelines, and eventually law.[19] Today, they're the backbone of privacy and data protection legislation around the world.[20] They're the basis of privacy and data protection laws, for example, in Argentina, Australia, Canada, the EU, Japan, Malaysia, New Zealand, the Philippines, Singapore, South Korea, the United Kingdom (UK), and the US, among many others.[21]

The FIPs have many permutations and one commonality. For example, the FTC lists notice, choice, access, security, and enforcement as the principles the private sector should abide by.[22] Europe's General Data Protection Regulation (GDPR) lists eight.[23] The OECD proposes eight others.[24] The lists of principles go on.[25] Despite their differences, though, all FIPs permutations have one thing in common. They aim to increase people's control over their personal information.[26]

Apps ask you to agree to their terms of service because individual control is mainly afforded through opportunities to consent (or not) to the collection, processing, and distribution of your personal information.[27] And, according to the FIPs, consent requires two things: giving you notice and giving you a choice. For people to have notice, they must know how an organization will collect, use, and share their personal information. For people to have a choice, they must be able to decide whether to agree with the collection, use, or sharing by considering whether the benefits they may get from it outweigh the risks.[28]

The primacy of notice and choice is most marked in the US, where a regulatory peculiarity elevates privacy policies to a mainstay of privacy governance. The federal US agency tasked with regulating and enforcing privacy is the FTC. Established to protect consumers, the FTC's mandate is to investigate and pursue "unfair and deceptive" practices.[29] The agency ensures that corporate promises (if any) are fulfilled and sanctions companies when they fail to notify consumers of a practice – or, occasionally, for improper conduct, such as maintaining inadequate cybersecurity measures.[30] What corporations promise they'll do isn't the main object of scrutiny; whether they did what they promised is.[31]

The US emphasis on promises was part of a broader regulatory strategy. From the 1970s to the 1990s, Congress and US regulatory agencies prioritized disclosure schemes such as notices to achieve regulatory goals, rather than designing substantive regulation.[32] In privacy law, this strategy stuck.[33] Although in theory the FTC's privacy enforcement is guided by all FIPs, in practice it prioritizes the principle of notice.[34] The FTC refers to notice as the "most fundamental principle."[35] Ensuring proper description and adherence to data practices lies at the core of the FTC's role as a privacy regulator.[36] Functionally, the FTC mostly enforces private agreements.

The tech industry lobbies for notice-and-choice.[37] Mandating notices is a much lighter regulatory intervention than mandating or forbidding data practices. Mandating notices, rather than developing substantive regulation, reduces regulatory costs.[38] Notices take a market-style approach that intervenes without actually intervening: they're in line with the approach of regulating by giving "choices" to people and, instead of mandating or forbidding practices, letting people decide which ones they'll accept.[39]

Notices are also easy for agencies to enforce.[40] They're easier to develop than substantive regulation because they place the onus on each individual to decide what's OK and what's not.[41] In the face of different business practices, technologies, and processes that affect people's privacy, the easiest thing regulators can do is to verify that each corporation adequately describes its data practices and adheres to them. Privacy regulators bind corporations to their privacy policies by punishing them for breaking the promises made in them outside the US too.[42]

The FIPs' goal of individual control over information fails because we're not given the means to make those choices.[43] As Woodrow Hartzog puts it, "privacy law is in a bit of a pickle thanks to our love of the Fair Information Practice Principles."[44] The pickle is that the FIPs have become synonymous with privacy protection. Initially

designed as guiding principles and not specific provisions, they turned into provisions that regulate personal data around the world. Designed at a time before people had computers at home, let alone the Internet, the FIPs aimed to protect people in a vastly different environment than the current AI-driven information economy. Since then, privacy scholars have heavily criticized them.[45]

The FIPs' failure to protect people's privacy isn't their own doing. As this book explores, it's rather the failure of the paradigm on which they're developed and implemented. The appropriate solution isn't to just change the FIPs. It's to change the building blocks that support them.

Notices that Don't Inform

Privacy policies are in a predicament.

In the early 2000s, Aleecia McDonald and Lorrie Cranor had an unorthodox idea: to check how long it would take the average person to read the privacy policies of every website and app that she uses for a year. The answer was astonishing: 244 hours per year, or six full-time working weeks.[46] In the decade and a half since the study, this number can only have increased. Another study found that less than 5 percent of people read them, a result that may be optimistic.[47] Not even the sitting Chief Justice of the US Supreme Court reads them.[48]

The no-reading problem is only the tip of the iceberg of privacy policies' issues. Even when we read a privacy policy, we can't understand it.[49] Their meaning is lost to people navigating passages that are too detailed or ambiguous to be helpful.[50] The result is that readers trying to penetrate the obscure content of the one document that's supposed to explain how they're being surveilled are left with either a sense of confusion or a false sense of understanding.

Many call for more user notices to increase transparency so that people can make informed choices – doubling down on the traditionalist view.[51] But others suggest that privacy notices are ineffective at increasing user awareness.[52] Empirical evidence shows that simplifying their language doesn't make people understand them better, improve people's awareness of data practices, or lead people to make different choices.[53] These findings suggest that privacy notices haven't only been consistently ineffective, but they're also likely to continue being ineffective for the foreseeable future.[54]

Researchers at the University of Michigan developed an algorithm, called Polisis, that uses AI to visualize privacy policies.[55] If you go through the representations generated by the algorithm, though, you'll notice they're somewhat unhelpful to understand what's going on with your data. Their limitations illustrate that the real issue is not that you don't read your privacy policies. It's that they're uninformative – even after recruiting the help of AI.

Because no one reads them, people don't choose one product or service over another based on its privacy policy. So corporations have incentives to have privacy policies that are the most beneficial for them and the least beneficial for their users.

And what's most beneficial to a company changes from one to another. This reality leads to a peculiarity. Although privacy policies are unified in their unhelpfulness, they're dissimilar in their content.[56] Reading one or two of them won't provide insight into the content of the others to reduce the no-reading problem.

Privacy policies have a no-reading problem, a comprehension problem, and an indistinction problem. These problems make them uninformative: we learn close to nothing from them. Privacy policies' uninformativeness leads many experts to believe that they don't matter,[57] or that making them the target of regulatory efforts is a red herring.[58]

Choices with No Options

The information economy eviscerates the idea of people having choices over what happens with their information. Beyond the insufficient yet unfulfilled aim to inform people as the paramount means of protection, people are rarely afforded genuine choice to do anything other than agree with them.

Our notice and choice model, inspired by neoclassical contract theory, was conceived fifty years ago, when today's Internet was unimaginable.[59] The model emerged in a context where personal information transfers took place between few and easily identifiable parties, for discrete purposes as part of a business exchange, and in relatively predictable and transparent ways. Data transfers happened, for example, when stores requested customers' phone numbers to inform them of a product's arrival or when banks needed their clients' social security numbers to log their financial information. Back then, it was far easier to know with whom you were interacting, what information they collected about you, how it would be used, and whether it would be shared with anyone.

The information economy, defined by multiparty data exchanges, is fundamentally different.[60] Today, corporate use of personal information includes data sharing, data mining, data trading on the back end, and profiling based on inferred data. Even a simple interaction, like buying shoes at your favorite store, includes the possibility of the other party selling your information to data brokers, who aggregate it with other information about you and sell it.[61] Other parties, such as your bank, are obligated to report your information to credit reporting agencies, whose job is to aggregate information about you to probabilistically infer your trustworthiness as a borrower through your credit score.[62]

The information economy's paradigm shift makes it impossible for people to understand who has what information about them and what purpose they may use it for (let alone how it got there). Third parties collect and use an unprecedented amount of personal information beyond people's knowledge and understanding.[63] In this context, we don't know what we're saying yes to when we tick the "I agree" box.[64] The shift in the collection, use, and sharing of people's data from fifty years ago to today's information economy that makes notices difficult also makes choices impossible.

The rationale behind the choice model is that, in theory, it could allow people to manage their privacy risks.[65] Privacy self-management was thought of as a way to avoid paternalism by making each individual decide what data risks they find acceptable to incur, when, and with whom.[66] In theory, it accounts for the fact that people's privacy preferences may differ and their preferences may vary from one context to another.[67]

Choice assumes knowledge and understanding of risks. It's impossible to make a real choice if you don't know what the choice is and what its consequences can be – what risk you're taking on by agreeing. So the failed informativeness of privacy policies is key to the failure of choice.

Two Forms of Individual Agreement

Despite privacy policies' long history, legal scholars and courts disagree about what kind of legal document they are: notices or contracts.[68] I find this disagreement puzzling. Privacy policies are corporations' main vehicle for informing their users, so they have incentives to clarify what kind of document they are. And, particularly but not exclusively in the US, regulators use privacy policies to oversee corporate data practices, making privacy policies an important mechanism for protecting privacy. So regulators have incentives to clarify it too.

Legally speaking, a notice is a tool to convey to someone else what they can do based on your property rights. For example, "no shirt no service" notifies patrons that a business will exercise its right to refuse service to anyone who doesn't wear a shirt. "Entry beyond this point is trespass" aims to notify that an area is private and anyone who enters it is liable.

A notice can shift liability only when informing someone is relevant for determining liability. For example, a warning label on a product can free a manufacturer from liability if an injury results from an improper use that the label said to avoid. But notices can't expand the preexisting rights of the notice-giver.[69] For example, you can put a sign on your fence informing others that walking beyond the fence is trespass, but you can't decide the punishment for trespassing. Signs indicating that trespassers will be shot don't actually establish homeowners' right to shoot trespassers. A notice can allocate risks, but it can't give or take away rights. To allocate rights, one needs a contract.

Treating a description of data practices as a notice implies that the notifying corporation has the right to do whatever such notice contains – and is simply informing us of what it will do. Treating the document as a privacy contract implies that the corporation lacks the right to do what's in the document unless it obtains the consent of each user.

For many legal scholars and courts, privacy policies are more akin to "privacy contracts" than to "privacy notices."[70] For example, Facebook's Terms of Use include a forum selection clause indicating that any dispute will be resolved by California

courts, which is something only a contract can do.[71] Treating privacy policies as notices made sense when there were no restrictions about what corporations could do with our data. The contracts lens, rather than the notices lens, better reflects that corporations aren't free to do as they please with our data with a mere obligation to let us know. Instead, corporations must obtain agreement.

Privacy policies have further similarities with contracts. Some contracts, called standard form contracts, share a set of problems with privacy policies. They're written in complicated language that people must often agree to without someone to clarify the terms – and often without reading them. Consumers rarely know everything they're agreeing to, and there's no room for negotiation because it's a take-it-or-leave-it offer.[72] However, these are only a subset of the problems that privacy policies have.

The contracts model ultimately also fails to reflect twenty-first-century personal data interactions. In the information economy, privacy policies differ from contracts in that there's no "meeting of the minds": the mutual understanding and agreement on the specifics of an interaction that's essential in contract law.

Even in the most egregious contracts, consumer standard form contracts, there's a meeting of the minds. We may not read standard form contracts, but at least we know what their object is: we know what we're giving up and receiving in exchange. If you purchase a cellphone plan with AT&T, you know you're giving money in exchange for a cellphone service. But in privacy interactions, we don't know what we're giving up.[73] Standard form contracts can be valid, even if some of their terms are invalid, as long as there's a core agreement between parties, such as trading a good or service for a price.[74] This core agreement doesn't extend to data practices. Often, there's not even a trade involved. Standard form contracts must have sufficient notice and a chance to read and understand the terms before agreeing.[75] But privacy policies can even be changed unilaterally.[76] In standard form contracts, we can choose whether to complete a transaction, but many companies that hold our data are entities we never heard of. Treating privacy policies as contracts mistakenly situates them in relationships of mutually chosen trade – a more consequential misconception than believing people read them.

Ultimately, persuading courts to treat privacy policies as standard form contracts doesn't solve the problems posed by the notice-and-choice regime. In Canada, for example, where courts routinely treat privacy policies as consumer contracts, scholars critique its privacy law for characterizing privacy in market terms, thus placing disproportionate importance on business interests.[77] Notices- and contracts-based models equally reinforce the idea of privacy self-management, which mistakenly sees the relationship between corporations and their users as series of bilateral market transactions.

What are people managing when they self-manage their privacy, according to the traditionalist view? The next section addresses this question. The short answer is only the secrets that they want to hide from the entire world.

B THE BINARY BLINDERS

The law was deeply unfair to Pamela Anderson. She and Tommy Lee filed an invasion of privacy lawsuit against *Penthouse* magazine in 1997 for publishing intimate photos of the couple.[78] The photos were stills from a tape that had been stolen from their home and posted online without their knowledge.[79] *Penthouse*, Anderson explains, offered to pay the couple for the photos, but they refused and asked the magazine to destroy them, explaining they didn't want people to see them.[80] The magazine published them anyway, exploiting the couple's intimacy for profit.[81] The judge overseeing the case dismissed it, arguing that because intimate material of the couple had been previously published, they had forfeited their privacy.[82]

Thinking that Anderson lost all privacy over the pictures once someone shared them, and that she lost nothing by the subsequent publications, is a result of the binary blinders. It results from thinking that once someone's personal information is disclosed for the first time, all privacy interests over that information are gone. The binary approach misconstrues privacy's value because it disregards the context in which disclosures occur and that further disclosures generate new harm. Privacy isn't binary as this notion assumes. It sits on a spectrum. People's privacy can decrease by different magnitudes, depending on the informativeness and sensitivity of what other people learn or infer about them. Recognizing this spectrum is more important than ever.

Bracketed into a Binary

The traditionalist approach to the information economy is built on a worldview of bilateral commercial exchanges that leaves out people in situations like Anderson's. This binary worldview results in the notice-and-choice system that privacy laws across the globe incorporate. Under this view, you either have privacy or you don't – just like you either fulfill a contract or you don't, with no in-between.

In the age of algorithms, recidivist privacy invaders permeate daily social interactions in an unprecedented way. A binary conception of privacy may have been adequate (it probably wasn't) in a world of one-time bilateral intrusions. In that simplified world, a person could open only one of your letters (a single intrusion) and publicize its contents (a single disclosure), but it would be unlikely to go beyond that. That same person was unlikely to open and disclose many more of your letters because it would be difficult for them to have the resources to do so. By contrast, in the information economy we're involved in repeated and ongoing interactions with actors that reduce our privacy, from social networks we're too familiar with to data aggregators we never heard of. Getting stuck in the idea that one either "has privacy" over something or one doesn't prevents one from capturing this context.

The story of Holly Jacobs, who founded the Cyber Civil Rights Initiative, illustrates the pitfalls of reducing privacy to that dichotomy.[83] Dr. Jacobs had exchanged intimate

photos with her boyfriend while they were in a long-distance relationship. Eventually, he posted the pictures online, where multiple websites reposted them – most of them deriving ad or subscription profit.[84] Jacobs spent months sending takedown notices and, after monumental efforts, got them scrubbed. But they reappeared on about 300 more websites. The police told her there was nothing they could do.[85] Telling Jacobs that, once her ex-boyfriend posted the pictures, it didn't matter how many websites reposted them, like the court told Anderson, would have been detached from reality.

Courts and policymakers often engage in this type of poor privacy reasoning. In a case against the city of Petersburg, for example, employees were required to answer a questionnaire asking about the criminal histories of their family members, their complete marital history, their children, and their financial status. The court dismissed the claim that their privacy was violated, reasoning that there was no privacy interest in the information because it was already available in other records.[86] The binary view brackets courts like this one to only two possible readings of the world: a person either "lost" their privacy or they didn't. It leads to an unreasonably high bar for harm and makes privacy claims unfathomably difficult to prove in today's context of multiparty data exchanges.

A continuous concept of privacy loss is paramount for understanding the information economy. Recognizing that privacy exists on a spectrum captures intuitions about privacy better than binary views. When a company like Alphabet (Google) gains more knowledge about one of its users, it's false to say that the user no longer has *any* privacy – just as it's false to say that they had perfect privacy before. It's also incorrect to say that nothing happened to their privacy. Privacy loss is about the user's level of privacy dropping from one level to another.[87] Viewing people's privacy as a spectrum better captures the reality that they face regarding their privacy losses.

Determining any rights violation is a binary exercise in one broad sense: in a trial, courts have to rule whether there was a violation or there wasn't. Recognizing degrees of losses, however, is essential to identifying those privacy violations correctly. Likewise, when estimating "reasonable care," courts consider degrees of care and apply a cut-off. The estimation mistake is overlooking that privacy losses, like levels of care, exist in degrees.

Accounting for nuance in privacy through a spectrum of losses and gains is key because privacy violations that get to court involve grey areas: they involve different gradations of privacy losses.[88] Rejecting binary perspectives in favor of an understanding that privacy losses exist in a continuum is necessary for developing sensible laws for the information economy.

Counting Only Secrets

In its worst form, privacy viewed through the binary blinders is reduced to secrets. Under the secrecy view, once you reveal information to someone in any way that makes it possible for others to see or know it, you abandoned all privacy over it.

The shortcomings of the secrecy view are clear in the painfully frequent scenario of nonconsensual distribution of intimate material, such as Dr. Jacobs' story. It's eerily common to hear that, because a victim shared the material with someone, it wasn't a secret anymore and the victim assumed the risk of its distribution.[89] This misconception sometimes extends to courts.[90] For example, in 2015, a woman called Dana sent intimate pictures to an ex-boyfriend, and someone else who saw them on his computer plastered them over a public Facebook page. The Vermont Supreme Court said that Dana chose to abandon her privacy over the pictures when she sent them to someone with whom she wasn't in a relationship.[91] This type of dismissal occurs even when courts rule in the victim's favor, but still frame the victim's harm as a cautionary tale about their excessive or irresponsible risk-taking.[92]

Positing that people abandon privacy expectations over information whenever they share it with one person, as the secrecy view does, is mistaken. Dana retained some privacy over the images when she shared them with one person and lost significant privacy when they were shared with the world. So did Anderson. This view is worse than victim-blaming.[93] It also implies that the victim didn't have her rights breached at all – that she wasn't even a victim.[94]

The dynamic at play in these cases follows us into our daily lives. Their dynamic is replicated when corporations acquire massive amounts of information that are deemed public, such as taking pictures of us on the street or gathering our online profile photos to train facial recognition software that can identify us.[95] As a result, online interactions are plagued with surveillance, harassment, and risks of violence.[96]

Secrecy is a uniquely problematic aspect of the traditionalist approach because it further narrows privacy protections from privacy self-management's "let people make choices about their privacy" into one specific choice: hiding information about oneself from others. The flawed secrecy conception permeates the notice-and-choice principle, indicating that people chose to abandon privacy over information when they chose to disclose it. This fundamental error illustrates why notice and choice fails as a privacy framework and, worse, leads to people bearing the risks of corporate data practices.

From a secrecy perspective, privacy also disappears when a person moves from private to public spaces.[97] Those notions of public information and public spaces that nullify privacy are often defined too broadly or not defined at all.[98] Secrecy leads to the belief that, as Scott Skinner-Thomson puts it, "the right to privacy while in public is nearly nonexistent, that privacy is more or less 'dead' once you walk out of your front door."[99]

Maintaining a privacy claim under the secrecy paradigm means having to keep information to oneself.[100] However, keeping any digital record in absolute secrecy in the information economy is beyond impractical; it's impossible.[101] By requiring people to do so, this view of privacy inordinately disadvantages the disadvantaged: those without property, those without a home who need to use public spaces, and those who belong to communities that are disproportionately surveilled.[102]

Secrecy-based views of privacy require a binary conception because they zealously abandon privacy expectations and protections when information is revealed. But not all binary views of privacy are secrecy-based. One could (misguidedly) believe that a person either has complete control or absolute lack of control over their information – failing to capture that one usually controls some aspects of it but not others. Binary views, whether they're about secrecy or control, mistakenly pose that when we share something in one context we lose our privacy over it in all contexts.[103]

By inferring preferences solely from behavior (someone revealed information to a platform so they must not care about privacy), the traditionalist narrative weaponizes the binary blinders into deregulatory efforts. The most common consequence is the argument that, if you have nothing to hide, you have nothing to lose.[104]

"You Have Nothing to Hide"

Former Google chief executive officer (CEO) Eric Schmidt once famously said that "if you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place."[105] A strong statement for a data profiteer.

Schmidt's infamous statement is an example of the most widespread consequence of the secrecy conception: the "you have nothing to hide" argument, which myopically equates privacy with hiding terrible secrets.[106] The statement illustrates how viewing privacy as secrecy leads to a mistaken understanding of choices, even when making choices is possible. Often, the argument is used to present policymakers with a false all-or-nothing choice between privacy and another social value, such as national security or public health.[107]

The idea that only people with "something to hide" care about privacy is the most pervasive argument against privacy that one can find.[108] Anyone who has conversations about privacy has heard someone else indicate that if they have nothing (bad) to hide, they have nothing to lose. The argument gets repeated by industry members, regulators, and community members.[109] With the nothing to hide argument, the secrecy view reduces privacy to something merely instrumental. In this view, privacy exists solely for trickery.

Variations of this argument appear regularly in statements by politicians and government entities. A defense of the British public surveillance system by its Conservative Party was "if you've got nothing to hide, you've got nothing to fear" – a quote originally from Joseph Goebbels.[110] In the US, the argument harkens back to McCarthyism, when it was used to pressure witnesses to confess to endorsing communism.[111] Still today, the argument appears during legislative debates amid claims that only "criminals" should be concerned with their privacy.[112]

People accused of crimes aren't the only ones who find themselves on the wrong end of the nothing to hide argument. Everyone in the information economy does.[113] People are constantly surveilled in their digital lives to show them more accurate

ads.[114] The data harvested through this private surveillance system are the source of tremendous profits.[115] Given these economic incentives, it's unsurprising that the nothing to hide argument found its way into the information economy – and Google's CEO.

An influential version of the nothing to hide argument comes from Judge Richard Posner. Based on neoclassical economics, Judge Posner argues that people desire privacy because they "want more power to conceal information about themselves that others might use to their disadvantage."[116] In this view, privacy is the "right to conceal discreditable facts" about oneself.[117]

Judge Posner's argument begins with the premise that there are people with bad traits and people with good traits, and that people with bad traits want to hide them while people with good traits want to show them. Privacy, his argument proceeds, allows the bad types to hide their bad traits by reducing the information available in the market, making themselves indistinguishable from the good types.[118] From this market-based perspective, privacy creates an information asymmetry. This asymmetry, according to the argument, advantages bad types because others are more likely to engage with them if they can't see their bad traits. And it disadvantages the people examining information to choose whom to engage with (the "information receivers"). The notice-and-choice system, allowing people to waive privacy whenever they're asked, is its logical consequence because it doesn't see anything worth protecting beyond deceit.

The nothing to hide argument mischaracterizes what privacy is about. Resting on the secrecy conception, it views privacy as chicanery: it assumes the only valid reason to hold personal information private is to strategically deceive others. It's not.

Judge Posner presented the argument in the context of employment, which was an appropriate choice. Employers are part of the information economy when they profit, directly or indirectly, from their employees' personal data and not only from their work.[119] Uber, for example, gathers valuable information from its drivers when they don't have passengers.[120] Employment analogies, though, are more broadly illustrative of dynamics in the information economy. In both employment interactions and the information economy, corporations hold significant power to make decisions that impact people's lives based on their information.[121] It's clear that providing employees with a take-it-or-leave-it option under a power imbalance deprives them of real choices. Employees, like people in the information economy, have something to lose.[122]

When You Have Something to Lose

In 2000, economists Claudia Goldin and Cecilia Rouse developed a test for gender-biased hiring in symphony orchestra auditions.[123] They noticed a gap between the proportion of women in elite music schools and elite orchestras, so they held auditions behind a curtain, preventing those hosting auditions from knowing the

auditionee's gender. Female orchestra hires immediately increased by one-third.[124] The curtains increased the probability of each woman passing the initial round by 50 percent.[125] Imagine the value of this privacy protection for those women, who had absolutely nothing to hide.

Privacy protections often help prevent discrimination. The logic behind these protections is that decision-makers can't discriminate if they lack the information needed to do it.[126] With or without formal protections, people rely on privacy to avoid discrimination in interactions with their employers, landlords, healthcare providers, schools, and banks.[127] This protection is crucial in the information economy, where AI algorithms make decisions about us based on our data.[128]

This privacy protection wasn't afforded to Carter Brown, who was fired from his job in Texas in 2018 after a coworker outed him to management as trans.[129] Carter Brown didn't have anything nefarious to hide but, when his employer learned information that he would have liked to keep private, he lost his livelihood.[130] This protection wasn't afforded either to April Cox, who was refused by human resources giant Randstad when a drug test revealed her medicinal use of methadone to recover from a former addiction.[131] Brown and Cox aren't alone in their efforts to keep legitimate aspects of their life private.

The value of privacy protection extends to interactions without discriminatory intent.[132] To continue with the employment analogy, consider drug testing in the workplace, which illustrates dynamics of power and bundled information that extend to the information economy. Many workplaces employ random drug testing during employment relationships or as a condition for hiring.[133] Presumably, employers do it because they believe that it provides them with valuable information about their employees. Some employers might test if they don't care about recreational drug use itself but treat it as a proxy for something else. For example, they may mistakenly believe that people who use recreational drugs may experience more frequent health issues leading to higher absenteeism, that they're more likely to disobey other rules, or that they tend to be less conscientious or hard-working.[134]

General drug tests, which check for various substances, reveal other information besides what employers try to gauge based on drug use. They can reveal information irrelevant to employers about someone's health status by detecting prescribed drugs. They can reveal information about what someone does during weekends that's irrelevant to their productivity on weekdays. They can reveal methadone use, uncovering that someone is recovered or recovering from a former addiction, as was the case for April Cox. Or, if additional tests are run on the sample, they can reveal sex assigned at birth, the information that harmed Carter Brown.[135] What an employee seeks to keep private may be unrelated to what their employer wants or deserves to know.

One should consider privacy concerns over information attached to drug tests as evidence of harm that flows from revealing bundled information. This privacy harm can lead someone who doesn't use recreational drugs to avoid testing. Many who are

harmed by bundled information from mandatory drug testing (who have something to lose) aren't recreational drug users. They're harmed by the other information revealed by the test.

Because drug use data are bundled with other data, one can't infer drug use from test refusal. Contrary to the neoclassical economics of privacy and the nothing to hide argument, people like Brown and Cox may refuse the test not because of how nefarious what they're not revealing is, but despite it. Many who would have passed a test will either decline it, foregoing a job that they would be qualified for, or accept it and bear associated harm. Because employers can't know how much each employee is harmed by the bundled information, they can't distinguish between those who refuse because they use illegal drugs at work (those with something to hide) and those who refuse because it would reveal bundled information (those with nothing to hide, but something to lose).[136]

Bundled information justifies protecting people with nothing to hide from mandatory testing if there are other ways – beyond testing – for them to convey productivity information. These methods could include providing a list of contacts for recommendations or establishing a trial period. Allowing people to choose among means to convey information improves social welfare because it reduces privacy harm.[137] In the US, for example, three states allow for voluntary compliance with workplace drug testing.[138] Other jurisdictions should consider doing the same. In the meantime, employers in jurisdictions that don't would receive better employees by breaking away from the secrecy conception and understanding that resistance to testing doesn't mean that employees have anything to hide – they may just have something to lose.

Drug testing illustrates how the nothing to hide argument relies on the secrecy conception. From the perspective of the receiver, the information is binary: either an employee passes the test and gets the positive signal that their employer attaches to it, or they don't. Because employers believe that the test is informative about productivity (otherwise they wouldn't require it), they're likely to use it for promotion and retention decisions. They're wrong to believe that, because learning about productivity is legitimate, employees can't suffer privacy harm from how they learn about it.

Requiring people to disclose bundled personal information to obtain a benefit imposes social costs beyond employment.[139] Because information is bundled, people in the information economy often have to reveal irrelevant data to convey relevant ones, like when you need to provide your phone number to make an online purchase, hotels scan your passport to verify your identity at check-in, or you're recorded at a store for security purposes. The risks from those forced disclosures represent a social loss together with an individual one, as the consequences of surveillance constitute a social harm beyond individual harm. For example, people behave differently when they know they're under observation, regardless of whether they're trying to hide a wrongful activity.[140] Allowing people to keep bundles of information private, rather than forcing them to reveal them to access products and services, is beneficial to them and to society.[141]

Considering that people value their privacy for its own sake, and not just to deceive others, shows that the secrecy-based view of privacy is inadequate. Personal information is bundled by nature because disclosing anything to someone often implies disclosing other things too. Sometimes, we want to keep information private not because of the information itself, but because of everything that's bundled with it. For orchestra auditioners, their physical appearance was bundled with their gender. For Brown, his past appearance was bundled with his membership in the Queer community. For Cox, her nonuse of recreational drugs was bundled with former use prior to recovery. For everyone in the information economy, information about their online activity is bundled with information about their characteristics, behaviors, and preferences.

The neoclassical economics conception of privacy is one-dimensional. In this one-dimensional conception, the only reason someone would value their privacy is to hide something that should be relevant to someone else so they can deceive. This view has erroneous microfoundations, meant for bilateral commercial transactions in which, if I know less about you or can't speak about you, you're competitively advantaged toward me.

The nothing to hide argument makes it seem that privacy is about hiding nefarious secrets from others. The value of privacy, however, is social.[142] Recognizing privacy's intrinsic value means moving to a nuanced worldview where we recognize someone might want to keep information from others that is or should be irrelevant to them.

* * *

In 1987, President Ronald Regan nominated Robert Bork, a fierce opposer of privacy rights on traditionalist grounds, to the US Supreme Court. Unbeknownst to Bork, during the debate over his nomination, a reporter walked into his video rental store, asked for, obtained, and published Bork's entire videotape rental history – something that, in 1987, was quite informative about what one watched.[143] His viewing history turned out to be unremarkable and his nomination unsuccessful. But the process changed American law for decades because it led members of Congress to write and pass the Video Privacy Protection Act, forbidding video stores from disclosing rental histories, at record speed.[144] Possibly worried about their own viewing histories, members of Congress were similarly situated to millions of people in the information economy. Their choices about what video store to rent from alone didn't protect them, they would lose more privacy from having their whole rental history revealed than from the parts they revealed to others, and they most likely had nothing to hide in their perfectly legal rentals, but had something to lose.

The notice-and-choice principle and the privacy self-management system that it underpins share mistaken assumptions about privacy interactions. First, they assume privacy interactions exist in a context of trade, where parties to a contract have the opportunity to notify each other and make choices. Second, they assume privacy is

binary, as shown through the popular nothing to hide argument and the widespread notion of privacy as secrecy. Through the binary blinders, they pigeonhole people as hermitic or impassive. This privacy paradigm was designed for a simple commercial context that no longer aligns with reality. While the paradigm's concepts about privacy interactions may have been relevant at the time, today they're stretched into contexts where they no longer make sense.

The privacy fallacy, operating in this paradigm, reduces privacy to an instrumental dimension. It creates a blind spot. Just because people occasionally seek something instrumentally, such as privacy, that doesn't exclude that people also value it for its own sake.[145] This reduction makes secrecy-based arguments such as nothing to hide mistaken in their own terms. Privacy laws fail when they silo social effects into instrumental individual choices. The instrumentalist view overlooks distributional aspects that inform privacy's social value: people with fewer resources who lack power to say no and data from one person that conveys information about others.[146] Decision-makers who fall into the privacy fallacy fail to capture real privacy interactions. They leave out negative effects on oneself and others.[147] Most privacy protections, in theory and in practice, don't protect bad people's dark secrets.

There's a reason why serious cases of privacy invasions abound. The traditionalist approach is built on the idea that people make rational and informed choices about their privacy when they're given notice, similar to how they decide to buy apples, a shirt, or an apartment. In the next chapter, I call this the "myth of rationality."[148] The approach is also built on the idea that if someone "chooses" to give information to someone, that means they don't care about keeping that information private. In the next chapter, I call this the "myth of apathy."[149]

The first idea, that people make rational and informed choices about their privacy, is the bedrock of privacy self-management. It's the same foundation on which contract law rests. But there are good reasons to qualify and depart from it for the information economy. The second idea, that if someone "chooses" to give information away they don't care about keeping that information private, is specific to privacy. But anyone interested in privacy enough to open this book faces the idea routinely. You face these supposed choices every time you open a website in a rush and click "I agree to cookies" without looking for the hidden "read without agreeing to cookies," or open a website in Incognito mode not knowing that you're still giving your browsing information to the website, the browser, and your Internet service provider.

2

Privacy Myths

Rationality and Apathy

The traditionalist approach to privacy rests on two myths: the myth of rationality and the myth of apathy. Rationality refers to the mistaken idea that people always act in a rational way when making choices about their privacy, with preferences that are independent of context and unlimited capacity to process information. Apathy refers to the false conclusion that, for the most part, people don't care about their privacy. These myths form the mismatch between the law's assumptions and people's reality.

They obscure reality. People are imperfect actors who care about their privacy but sometimes act contrary to their interests because the online ecosystems they navigate are impossibly complex. This chapter shows the falseness of rationality and apathy in the information economy by referring to empirical evidence and to our daily online interactions. People don't act rationally or apathetically toward their data but, rather, choice ecosystems are designed to push them to agree to data practices.

Both myths are found in academic and popular discourse, adversely influencing policymaking and compromising laws' effectiveness. Rationality and apathy underpin the traditionalist approach to privacy that has been in place since the 1970s. The fact that rationality and apathy are myths was less consequential – and could go unnoticed – in pre-Internet times, when privacy was about regulating one-on-one exchanges of identifiable information points. But, today, our every move is an opportunity for hundreds of entities to mine data. Corporations assemble profiles about us and make inferences that are more valuable and dangerous than any information mined or released.

The privacy myths facilitate pervasive manipulation, by which we're made to act against our best interests. Every day, corporations "nudge" us to act in their best interest, not ours. Manipulation wouldn't be used if we were rational (because it wouldn't work) and it wouldn't be needed if we were apathetic (because we'd be eroding our privacy all on our own). Privacy law fails to address manipulation because it assumes that we're rationally immune to malicious nudges and that, if we act in corporations' best interest to our detriment, it's because we don't care. In this context, continuing to build privacy law on the shaky foundations of these two myths leads to the obsolescence of most protections people are afforded in the information economy.

A THE MYTH OF RATIONALITY

If you ever go to the Privacy Law Scholars Conference, you'll see how many of us have privacy stickers over our laptop cameras. But you won't see that almost none of us have the same sticker on our phone's camera, which we stare at way more than our laptop – or how many of us come home from the conference to smart home devices. It's unrealistic to expect people to behave perfectly rationally, and it's problematic for privacy law to draw conclusions from assumptions of hyperrational behavior that doesn't exist. When making complicated privacy decisions, we're influenced by various cognitive biases, usually without being aware of them.

Context Dependence

A key takeaway of behavioral economics is that context influences decisions in ways that rational choice theory can't anticipate. We're likely to exercise more if we live with a roommate who does the same. We snack less when snacks are in closed opaque jars versus open transparent ones. We're willing to stand in line to save $20 on a $50 purchase, but don't do it to save $20 on a $1,000 purchase.[1] A $500 TV seems cheaper to us when placed next to a $1,000 TV than when placed next to a $400 one. Our privacy behavior is influenced by our perceptions of the world around us – such as how much control we feel we have – as well as contextual influences such as our peers' behavior and even the physical environment.

When people perceive that they're given more control over their personal data (even when they're not), they become more likely to accept privacy risks.[2] Corporations know and exploit this. Facebook, for example, provided its users with illusory control over the use of data from third parties by showing targeted ads with the disclaimer stating: "you control whether we use data from partners to show you ads." But the actual control imparted to users was minimal.[3]

The physical environment's influence on people's privacy behavior has been documented all the way back to the 1970s. One study showed, for example, that the level of intimate disclosures is higher in warm, comfortable rooms with soft lighting than in cold rooms with bare cement and overhead fluorescent lighting.[4] In online interactions, the environment can be altered by design choices more easily than in physical spaces. Because bounded rationality renders us unable to exhaustively search for the best option, how privacy options are framed determines our choices.[5]

Our peers' behavior is another influential factor, affecting our privacy decisions through reciprocity. We're more willing to share personal information when our conversational partners also do so, even when our risks aren't changed by their disclosure.[6] People tend to reciprocate what others reveal about themselves even when such information concerns illegal or unethical behavior.[7] In an experiment, subjects' willingness to share personal information even increased to reciprocate disclosures from a computer agent.[8] People feel pressure to reciprocate how much

their peers share on social networks.[9] Companies can exploit pressure to reciprocate by curating what disclosures from others we see.

Another contextual factor impacting our privacy decisions is whether we trust the receiver of the information, even if this trust is undeserved.[10] Higher trust toward a corporation leads people to agree to more data collection – although this effect dissipates when people perceive risk.[11] Trusting the Internet itself increases people's likelihood to transact online, regardless of privacy beliefs and concerns over unauthorized use of personal data.[12] Even the presence of regulation reduces perceived risks and increases the likelihood of agreement to data practices.[13] Familiarity with online services reduces people's perceptions of risk, affecting their agreement to data practices.[14] Using services such as a social network frequently increases that feeling of familiarity.

Context, in sum, influences privacy decisions through framing, perceptions of control, reciprocity, and trust in a receiver, all of which are overlooked by assumptions of perfect rationality.

Inability to Understand Privacy Policies

Most of us don't read privacy policies, ever.[15] And we wouldn't understand them even if we did. Under current practices, most companies write privacy policies using inaccessible terms and sentence constructions.[16] Privacy policies and controls are difficult to understand given their length, linguistic jargon, and people's varying levels of digital literacy.[17] As a result, people are overwhelmed by privacy policies, hindering their ability to make informed decisions based on them.[18] It doesn't help that most people have limited knowledge of what actions they can take to protect their privacy and what means companies have to reduce it.[19]

Privacy policies' no-reading problem leads people to react in different ways to the existence of a privacy policy on an app or website. In 2009, more than half of Americans believed that the presence of a privacy policy means that corporations can't trade their data.[20] Although this misconception is likely less widespread now, newer studies show that most people wrongfully believe that the mere existence of a privacy policy protects them from privacy risks.[21] The majority of adults in one survey who simply encountered a label titled "privacy policy" on a website incorrectly assumed that the website would safeguard their information.[22] Others indicate that the mere presence of a privacy policy increases people's likelihood of agreeing to data practices based on those unfounded beliefs.[23] Another study, however, indicates that invoking the existence of a privacy policy reduces people's trust in a platform.[24] What is settled is that people aren't rational in their interpretations of privacy policies.

Impossibility to Estimate Data's Value

We have difficulties estimating the value of our personal information. For example, when people try to price a bundle of information (something that's difficult

to do and usually leads to an arbitrary number), their subsequent thinking usually remains tethered to this arbitrarily established value.[25] This tethering happens because we tend to overly rely on the first information we obtain – which behavioral scientists call anchoring. Someone pricing a piece of information at $5 and then being told that this is too low will usually only go up a bit, to $6, rather than restarting the estimation process. In that way, the first estimate becomes an anchor for later guesses.

There's a disconnect between people's (un)willingness to pay to protect their information and their willingness to accept small sums for it. The average person's willingness to accept money to allow information to become public is significantly higher than their willingness to pay to protect that information from becoming public.[26] In other words, people's valuation of their privacy depends on the direction of the cash-exchange: people value privacy more when they have it than when they don't. Participants in one study, for example, were willing to pay $5 per month to protect some information but demanded $80 per month to allow access to the same information.[27] The same discrepancy appears when the rewards are of little significance.[28] For example, in one experiment, people willing to give away relatively inconsequential information for 25 cents were unwilling to pay anything to protect the same information.[29] Low monetary rewards make people hold back and disclose less than if they had no monetary reward.[30]

These findings correspond to behavioral economics' endowment effect, according to which people irrationally place more value on the same thing when they own it than when they don't.[31] The endowment effect is much larger in privacy than in other contexts. In one experiment, willingness to accept was five times higher than willingness to pay, which almost doubles the average ratio in physical goods.[32] In another experiment, willingness to accept was sixteen times higher – over five times higher than for physical goods.[33]

Impossibility to Estimate Privacy Risks

If you ever did Crossfit, you may have heard that its founder Greg Glassman liked to say: "We sought to build a program that would best prepare trainees for any physical contingency – prepare them not only for the unknown but for the unknowable as well."[34] The unknown is what you don't know and the unknowable is what you can't know. The difference traces to what economists call risk and uncertainty. Risk is when you can estimate the chance that an outcome will happen and uncertainty is when you can't. Uncertainty, in other words, is a kind of risk that's impossible to estimate.[35]

People's inability to assess privacy risks impacts people's behavior toward privacy because it turns the risks into uncertainty. This inability leads people to perceive higher than real control over their information.[36] Overall, people are overwhelmed when identifying potential outcomes related to privacy threats and have difficulties

assigning the likelihood of those risks materializing.[37] People's inability to assess risk may explain why how much people post, how often they post, and what they say in their posts is independent of their declared privacy concerns.[38]

Properly protecting our privacy in the information economy requires technical skills that few people have.[39] Many social network users publicly share their birth date even though this increases the probability of identity fraud and identity theft. According to one study, 73 percent of people underestimate the probability of identity theft.[40] That's unsurprising, as most of us don't understand privacy policies or the workings of most privacy protection tools.[41] It's common for people to ignore basic privacy-protecting behavior, such as not responding to spam emails, not downloading files from nonsecured websites, and not clicking on pop-up ads.

The clarity of the information economy's convenience contrasts with the opaqueness of its risks. Most of us shop online even though it increases risks of credit card fraud.[42] Interviews with smartwatch users find that most participants didn't take privacy-enhancing precautions despite their awareness that privacy risks exist.[43] Users' decisions are affected more by the expected benefits of sharing data than by the expected risks even when they're aware that information leakage may happen.[44] Even technology-savvy users' concerns over privacy and security don't translate into decisions as well as other factors such as app functionality, usefulness, trust, price, ratings, and design.[45]

***

People are often accused of taking irresponsible risks in the information economy – an accusation based on narrow secrecy views of privacy. The so-called assumptions of risk that people are often described as taking aren't real. One can only assume risk when one actually understands the risk involved and can make choices that meaningfully change the risk levels. This understanding and freedom exist in some interpersonal situations, like when someone can choose to disclose something to their lawyer knowing the information will be bound by professional secrecy or, conversely, share it with a nosy coworker understanding that the whole office will find out. This isn't the case in the information economy, where we operate on notices that don't inform and, most of the time, have no real options. The impossibility of assessing risks takes us to the next myth: the myth of apathy.

B THE MYTH OF APATHY

The myth of apathy is the assumption that other people don't care about their privacy based on their behavior. It comes from two aspects of the traditionalist paradigm. First, it comes from seeing privacy as a binary, where people either care about it or don't, losing nuance over context, information receivers, and types of information. Second, it comes from reading too much into others' behavior as an external

observer – like neoclassical economists looking at whether people buy apples without caring about why they do – concluding that if people don't bargain for something, they must not care. The outsider perspective is appropriate for predicting people's behavior, but inappropriate for understanding their motivations.

We frequently see this myth in popular discourse, when people say things like: "Kids today don't care about their privacy: they're all on Tiktok."[46] It even makes it into mainstream popular science, such as Freakonomics.[47] The myth of apathy leads industry members and opinion leaders to argue that privacy shouldn't be a policy consideration because people show that they don't care about it.[48] A close examination exposes its problematic roots and implications.

The So-called Privacy Paradox

The myth of apathy, which erroneously assumes that other people don't care about privacy, is reflected most clearly in the so-called privacy paradox. The privacy paradox narrative suggests that people abandon their privacy in exchange for small perks, so they must not care about it very much.[49] It's built on seeing privacy behavior through the lens of binary individual choices.[50]

Privacy paradox studies claim to have found an inconsistency between people's declared concern for privacy and their actual behavior online.[51] An early study grouped participants according to their level of privacy concern (high or low) and discovered that, when in online shopping simulations, the groups revealed equivalent amounts of personal information.[52] Some experiments found that privacy concerns as stated prior to the experiment didn't match shopping behavior during the experiment.[53] In an experiment where almost 90 percent of respondents declared a high level of concern about their privacy, almost 90 percent agreed to provide their name and address in exchange for a loyalty card.[54] Other studies suggest that declared privacy preferences can't be trusted because they're unrelated to actual privacy decisions.[55]

People with high privacy concerns don't seem to use fewer social networks or post less information on them.[56] One of the first surveys of Facebook users found that even those who expressed the highest degree of concern for their privacy revealed sensitive information on the platform.[57] People don't seem to actively protect their privacy even when they report a strong motivation to do so.[58] In one study, the only significant predictors of sharing information on Facebook were the general tendency to disclose and desire for popularity.[59]

According to other experiments, people have a very low willingness to pay to protect their personal information. When experiment participants were shown stores that differ in the information requested (one sensitive and one nonsensitive), they bought from the cheapest store.[60] In one study, people disclosed sensitive personal information such as their monthly income for minimal discounts.[61] People's interest in low prices, low waiting times, high ratings, and exclusivity seem to obscure

privacy risks when choosing services.[62] Despite asserting that we value our privacy, the argument concludes, we're quick to surrender personal information.

Empirical privacy experts point to the problematic implications of the privacy paradox narrative. Kirsten Martin calls it "the most dangerous concept emanating from the privacy-as-concealment [secrecy] framework."[63] The privacy paradox narrative builds an unstable bridge connecting the myth that people don't care about privacy with deregulation. It weaponizes the binary view toward deregulatory efforts.

Context and Uncertainty Explain Our Behavior

Uncertainty is the one certain thing about the Internet. In a 2019 Pew Center survey, 74 percent of the Facebook users interviewed didn't know that the social media platform maintains a list of their interests and traits.[64] In another 2019 study, only 6 percent of people said they understand what corporations do with their personal data.[65]

People are uncertain about which corporations have data about them and what data they have. Corporations track us in ways we would never guess, such as our devices' battery levels.[66] The European Users Organization has said that "users are sleep-walking in a world without privacy."[67] Similarly, the popular objection against targeted ads is a visceral reaction that qualifies them as "creepy."[68] The empirical findings surveyed in the last section show the importance of even seemingly irrelevant aspects of context for privacy decisions – context we're rarely made aware of.

When people agree to information collection, they're uncertain about the possible outcomes, the magnitude of their consequences, the possible measures to protect themselves, the actions taken by those who desire their information, and other unforeseeable events.[69] In this context, there aren't knowable probabilities to formulate complete beliefs about what one should do.[70] The information economy is riddled with uncertainty about the set of negative consequences that could happen to us. Worse, these consequences change as technology advances. Not even the companies that collect your data know the uses and risks that it will have in the future.

The experimental evidence on the impossibility to estimate risk confirms this uncertainty. So does people's behavior. People respond to privacy changes when the decisions are less complex.[71] When information about privacy is visible, people often choose privacy protections.[72] Many use pseudonyms or nicknames on social media accounts to preserve some privacy.[73] In vignette studies with clear parameters, people respond differently to contextual changes such as the data collection's duration and location, the data's recipient, and the data's use.[74] People even respond differently to those contextual factors regarding information that's publicly accessible.[75] And people continue to have privacy expectations over information they allowed companies to collect.[76]

We often don't realize which of our digital "choices" undermine our goals because privacy policies are opaque and digital ecosystems are designed to extract

our agreement. For example, Facebook users have been shown to be unable to estimate the risks of different settings on the platform.[77] The risk estimation problem isn't unique to Facebook. People are unaware of how each data collection affects the probability of privacy harm in the future or the magnitude of the eventual harm. Information is combined to reveal other, new information, and it's impossible for anyone to know which pieces of information will be combined and what they will reveal.[78] It all seems as if we were making good, consistent choices because the consequences only materialize later.

When data collectors, intermediaries, and ad companies trade people's personal information, new unpredictable risks arise. As the information spreads, the likelihood of misuse and illegitimate disclosure increases. So every time someone's information is put in new hands, their risk of privacy harm increases. Transfers place personal information outside our control, yet leave us vulnerable to negative consequences. Since, as the next chapter explores, corporations don't face such a risk, they have incentives to misuse and excessively share the information.[79] These perverse incentives are exacerbated by our lack of awareness of uses and trades and our consequential lack of opportunity to discipline corporations.[80]

Even if people had full information about risks and benefits while making privacy decisions, they would have to base their decisions on uncertain risk. The risk of privacy harm isn't dependent on people's behavior alone but also on the subsequent behavior of corporations that acquire their data. The uncertainty makes it impossible to determine the optimal privacy decisions.

In addition to objective uncertainty, people have subjective uncertainty produced by levels of technical understanding, limited time, and limited attention. Uncertainty in the information economy isn't only determined by the unknowable data risks, but also by difficulties in learning about knowable ones. The result of it being too complicated to evaluate knowable risks due to subjective uncertainty is called "privacy fatigue." When people learn they can't manage their privacy effectively no matter how hard they try, they often stop trying.[81]

Constant uncertainty that leads people to stop trying can make them seem apathetic. In one study, an interviewee explained: "Over the great scheme of things I see that we are losing privacy every day. I feel we are not going to ever have it back.... And as a result, I am very like, oh well that's life!"[82] Negative experiences like this one matter: study participants who went through privacy-infringing experiences tended to become skeptical about the effectiveness of privacy protection and less protective of their privacy overall.[83] Privacy fatigue isn't apathy, but rather a consequence of the perceived futility of trying to keep pace with protecting our privacy.

Risk Matters

A second generation of privacy paradox studies separate the so-called paradox from the myth of rationality. They argue that people's agreement to data collection means

they discount their privacy hyperbolically. This version of the privacy paradox departs from neoclassical economics with a discussion on bias and temptation. But it remains traditionalist because it incorrectly infers apathy by assuming people have genuine and informed choices.

Economists explain that there are two reasons to discount future rewards: annoyance of waiting and risks. One reason is that we care more about present consequences than about future ones (the "waiting for a delivery is annoying" principle). The other reason is that, with time, rewards have the risk of disappearing or losing value (the "a bird in the hand is worth two in the bush" principle).

The second generation of privacy paradox studies rely on the "waiting for a delivery is annoying" principle to explain online behavior. They see people's privacy behavior as disproportionately valuing immediate rewards over future ones.[84] Showing that privacy-cautious people agree with data collection too, these studies indicate that people tend to maximize the immediate benefits of those collections.[85] They believe that people face data temptation: that they seek immediate data gratification and excessively discount future privacy consequences.[86] Behavioral scientists call this behavior "hyperbolic discounting."[87] Hyperbolic discounting explains, for example, why we sometimes make poor dietary choices disregarding future impacts on our health.[88]

They forget about the "a bird in the hand is worth two in the bush" principle. Think of a time when you rummaged through the kitchen in the middle of the night and picked the least healthy item available. You probably didn't plan to have it when you woke up that morning – you changed your mind later. Now think of a time when you played a card game, such as Texas Hold'em. You may have thought about an amount you'd bet and then changed your mind when a community card was flipped. In one case and the other, you changed your mind for different reasons: temptation in one and decreased uncertainty in the other. Both reasons to discount future consequences (annoyance of waiting and risk of losing the reward) can lead people to change their minds about their choices.[89] They do so for different reasons: temptation and uncertain risk.[90] Temptation describes people's behavior. Uncertain risk describes their context.

Temptation implies that people understand the risks involved.[91] When I choose between having cake or fruit for dessert at the law school cafeteria, I know that eating cake every day will negatively impact my health in the long run. If I still choose cake and then regret it, someone could say I was tempted because I knew about the risk – if I hadn't known the health effects, my decision would have been blissful ignorance. When people face daily-life situations in which they discount future consequences based on behavioral biases, they're aware of the risks' size and probability and make the suboptimal choice anyway.[92]

Uncertain risk implies a context with unknowable harms. The information economy's uncertain context described in the last few pages show the conditions for this second discounting mechanism. The negative outcomes of people's data choices, data harms, don't happen with knowable probabilities.

Inferring apathy out of observed privacy decisions inaccurately assumes one of the discounting mechanisms explains everything (the "waiting for a delivery is annoying" principle) while dismissing the other (the "a bird in the hand is worth two in the bush" principle). Seemingly puzzling privacy decisions (people "changing their mind" about their privacy) result from an uncertain risk of privacy harm, something not paradoxical at all.

There's No Privacy Paradox

Uncertainty explains people's privacy behavior. Imagine you open a vegan doughnut shop. Before opening, you don't know how many clients will come or what's the risk of the business not working out. You buy low-quality furniture for the shop that won't last long (cheap in the short run but expensive in the long run) because you're concerned that the shop won't either. The choice of low-quality furniture doesn't imply that you're present-biased or make poor furniture choices. It also doesn't imply that you don't care about quality. You're uncertain about how much risk there is, and there's a process during which you'll understand it better.[93] So you estimate the risk differently at the beginning than later.[94] People facing unknown risks, like people facing temptation, may seem impatient. But they're not disregarding future consequences.

Real-life privacy decisions differ from privacy paradox experiments in the outcomes' uncertainty. When we agree to data practices, we don't know the probability that data harms will occur, the timeline in which they may occur, or how to avoid them. Studies may suggest that people prioritize the immediate benefits of agreeing to data collection. But this conclusion implies the risks and benefits are comparable.

People's privacy behavior isn't apathetic as many privacy paradox studies present it to be. People react to privacy when it's visible. When Facebook was something that teenagers used, they engaged with its most visible settings, such as making their profile private.[95] And many do the same on Instagram. When information about privacy is available directly on search engines, people prefer websites with a perceived higher privacy protection, particularly for purchases that involve sensitive information.[96] People react to simple privacy scenarios.[97] When information about privacy is available and clear, many pay a premium to purchase from privacy-protective retailers.[98] People's privacy concerns often correlate with their choices over simple privacy settings.[99] Research on social media users finds that their privacy concerns correlate with the amount and type of information they share.[100] People's ability to deal with privacy issues changes with the choices' complexity.[101] People may appear unconcerned about privacy because few employ privacy-enhancing settings in social networks.[102] But that's because of difficulties in translating privacy preferences into social network settings.[103]

People value different types of personal information differently. They value information related to their medical history, financial status, and family more and

information about product and brand consumption less. People's privacy concerns respond not only to immediate harms – such as spam or fraud – but also long-term consequences, such as price discrimination, which vary by context.[104] If experiments on privacy concerns treat all personal information as equivalent and give people binary yes-or-no choices, their results will be inaccurate.[105]

The experimental evidence surveyed shows that people react to information about their privacy when it's understandable. People who face temptation aren't helped by more information because they already have it. People who face uncertainty, on the other hand, are. People's different valuations of different types of information, together with their reaction to context changes and to information accessibility, indicate that privacy decisions aren't irreflexive. They're just uncertain.

***

The privacy paradox narrative complements the "nothing to hide" argument: they're two sides of the same coin. The privacy paradox narrative suggests that people disregard privacy in their choices, so they must not care about it. The nothing to hide argument suggests that you shouldn't care about your privacy unless you're hiding something nefarious. These tropes get weaponized in favor of a contractual view of privacy, so that people who "don't care" about their privacy can waive it. They feed the privacy fallacy: why should laws, regulators, and courts protect people's privacy, absent negative tangible consequences, if they don't or shouldn't care about it?

C EXPLOITING THE PRIVACY MYTHS

Manipulating users works because perfect rationality is a myth. If we were perfectly rational, manipulation wouldn't work because we would be able to see through the tricks and we wouldn't let corporate tactics cloud our perception of value, risks, and rewards. And manipulating users is necessary in the first place because their apathy toward privacy is a myth. If we didn't care about our privacy, corporations wouldn't have to manipulate us into giving our privacy away because we would do that by ourselves. Explaining the pervasiveness of online manipulation requires recognizing that the privacy myths are real and influential.

Anti-privacy Choice Design

In 2018, you may have noticed a spike in the number of corporate emails you received. Dozens of companies (some of them you didn't know you interacted with) contacted you to let you know that they updated their privacy policy because they want to better protect your privacy. The reality is that companies around the world had to adjust their privacy policies to comply with Europe's newly arrived GDPR,

and they had a legal mandate to notify you that they did. Your relationship with those companies, though, didn't change much after they made those changes.

Anti-privacy design strategies present privacy notices and choices in a way that exploits people's biases. They "nudge" us, mostly against our interests and for companies' profits.[106] Design techniques aren't neutral, so they can be used to influence our decisions.[107] Real-world people in an uncertain data context can be and are exploited by corporations' design choices.[108]

When dealing with real people in the information economy, design holds power. As the Norwegian Consumer Council puts it, corporations "nudge users away from privacy-friendly choices."[109] We disregard privacy settings and terms and conditions not because we're lazy, but rather because service providers' designs push us toward disadvantageous choices.[110]

Examples of exploitative choice design aren't difficult to find: they're everywhere in our daily lives. Phone apps ask us if we'd like them to "connect" with Google or Instagram instead of making a new account, which sounds quite nice – they don't ask whether we want them to share our personal data with each other, which is what's happening. YouTube used to tell its users who wanted to turn off personalized ads that doing so meant they would lose the ability to mute the ads, which is problematic in offices and disruptive elsewhere.[111] Facebook asks you to consent to facial recognition because it can "help protect you from strangers using your photo" and "tell people with visual impairments who's in a photo or video,"[112] leaving out that facial recognition helps advertisers approach users based on perceived emotional states and identify them when doing so would be unwelcome. Digital products are deliberately designed to be addictive, from the type of font used to the frequency of popups.[113] The information economy provides incentives to design them that way because, the more that we use these products, the more ads we see and the more information is gathered about us.

Designers routinely shape choice architectures to get people to accept terms that benefit corporations. For example, they can endorse one alternative and highlight losses in the other or minimize privacy concerns, priming people into opting in.[114] Many companies use buttons of different sizes and colors for options they want their users to click. Others try to influence us by exploiting our aversion to losses. JC Penney highlights the number of people who viewed a product in the last day to develop a sense of urgency.[115] If you try to deactivate an account with language-learning app Duolingo, it will tell you: "Hooooooold up – are you sure you want to do this? Duolingo teaches you how to live, love, and speak another language. If you leave you might just never be able to reach your full potential in life."[116]

The design of privacy notices influences people despite the information shared in those notices. User-friendly privacy notice designs inspire trust in people regardless of whether the data practices they describe are privacy-protective, as the notifications from 2018 did.[117] People don't just respond to design; they respond to design despite the content of notices.

One way in which anti-privacy choice architecture contributes to our inability to understand privacy settings is what economists call the "framing effect." Framing privacy choice settings in convenient ways, such as labelling them as "app settings" rather than "privacy settings," increases the likelihood of people agreeing to data practices.[118] Moreover, nonuser-friendly designs obstruct perceived privacy controls.[119] Studies comparing widely used privacy policy formats with best practices – such as short overviews of the privacy policies and explanations in understandable language – found that participants couldn't reliably understand the best practices better.[120]

Anti-privacy design is often targeted. One technique, called "confirmshaming," is to shame people into acting favorably toward a corporation. Think of it as exploiting your fear of missing out. For example, when we decline an email newsletter, some websites shame us into changing our choice with banners that read something along the lines of: "Don't go! We'll miss you!"[121] Similarly, the "social proof" technique exploits the influence of our peers' privacy behavior over ours by highlighting how many chose the option that the corporation would like us to take. Social proof creates what behavioral scientists call a bandwagon effect. This effect operates when we do something after we see how many people around us are doing it, like when NBA teams get more fans as they progress in the season or Catholics become more religious when a pope of their nationality is elected.[122] Targeted techniques combine an unprecedented knowledge of our decision-making vulnerabilities with an unprecedented ability to reach millions of individuals with messages adjusted for them.[123] They press on our vulnerabilities to drive us into surveillance.

Targeted techniques undermine people's choices in a legal context where their agreement is the utmost protection mechanism.[124] By normalizing surveillance, they even distort our expectations and preferences.[125] They don't only interfere with individual autonomy, but also with the law's effectiveness at protecting us, because the assumption that we can freely decide what consequences we're willing to accept is essential to both.[126]

At their worst, designs hypertarget the most vulnerable, such as those with gambling addictions, medical issues, teenage depression, or a pending divorce. Until a controversy sparked in 2017, for example, Facebook allowed advertisers to target millions of teenagers who showed to be in psychologically vulnerable states, such as feeling "worthless," "insecure," and "defeated."[127] Hypertargeted designs steer vulnerable individuals toward surveillance.[128] Corporations with unprecedented access to knowledge about people's vulnerabilities can use those vulnerabilities to manipulate people at a low cost because they can do so at scale.[129]

Anti-privacy by Default

Anti-privacy by default hides privacy-protective choices or makes them more difficult to reach – a tactic that behavioral scientists call choice friction. Through choice

friction, they exacerbate the already asymmetric power dynamic between users and data companies. The combination of choice friction with self-interested bad intentions is what behavioral economist Richard Thaler calls "sludge," to differentiate it from beneficial nudges.[130]

What companies set as the default option in their design choices has enormous consequences. When it comes to design, as Ian Kerr puts it, the devil may be in the details, but it's often in the defaults.[131]

Defaults are powerful because they tend to be "sticky." When an option is preselected, parties deviate from it far less often than one would expect. Adherence to savings plans increases up to 50 percent when employees are enrolled automatically.[132] The number of organ donors increases dramatically in countries where being a donor is the default.[133] The effect is present in contexts as diverse as insurance and food choices.[134] It's present in marketing, where the number of people who agree to receive marketing emails increases up to 50 percent depending on the default setting.[135] Defaults are powerful even when the cost of switching away from them is negligible, such as ticking a box.[136]

The information economy is no exception. It even magnifies the effects of defaults present in other contexts. People rarely examine defaults because privacy settings (or "app settings") are complicated and time-consuming to read, as was found for Facebook users.[137] And people almost never change them.[138]

Anti-privacy defaults exploit our status quo bias. This bias indicates that, when offered a choice, people tend to remain in the current state of affairs.[139] The status quo bias is ubiquitous, which makes it easy prey for choice designers to nudge us into the options they want us to take. Through default settings, designers steer people toward less privacy due to the appealing simplicity of preselected options.[140] Defaults also create an endowment effect.[141] The endowment effect indicates that people typically seek higher compensation to change the status quo than they would have offered to acquire it.[142] They exploit the disproportionate asymmetry between willingness to pay and to accept payments for privacy discussed above. Defaults also stick because people perceive them as silent recommendations of a state of affairs that would work well.[143] This mechanism exploits trust and familiarity.

Exploiting our biases through anti-privacy defaults is a common way to nudge (or "sludge") us into surveillance. Corporations use default choice architectures to steer people toward the "options" that corporations want them to reach.[144] With time, companies get better at carefully articulating the promises in their privacy policies, such as those they announced in 2018 due to the GDPR. But they weaponize design to circumvent these promises by complexifying privacy features and simplifying information disclosures.[145] For example, social networks such as Facebook have made increasingly more information public by default.[146] In a seven-year longitudinal study, even when people seemed to adopt privacy-seeking behaviors, changes in privacy policies and interfaces countered those behaviors.[147]

Design tactics that exploit people's biases, such as anti-privacy default settings, make choice architecture as important as the existence of choices themselves.[148] Digital products are designed down to the engineering level to undermine our privacy.[149] Responding to economic incentives for ever-increasing data collection, products are engineered to increase data-driven profit at any surveillance cost.[150] As such, design needs to be subject to better standards and better laws.[151]

Dark Patterns

Dark patterns are the ultimate form of design manipulation. They're strategies meant to manipulate people into agreeing to data practices through deception.[152] Dark patterns interfere with people's decision-making, making them act in the interests of online services and, potentially, to their own detriment.[153] They go beyond nudging designs and surveillance by default. Interface designer Harry Brignull, who coined the term, defined them as strategies that are "carefully crafted to trick users into doing things […] with a solid understanding of human psychology, and they do not have the user's interests in mind."[154] Empirical evidence finds them strikingly effective.[155]

The strategies are varied. Some types of dark patterns, known as obstruction, are designed to trick people into picking a specific option by presenting options asymmetrically.[156] For example, if you try to cancel a subscription with the *Financial Times*, you'll find a preselected option to change the subscription to a different (sometimes more expensive) one; to find the "cancel subscription" button you'd have to scroll to the bottom of the webpage and find it in smaller font.[157] The *New York Times*, for a while, made it difficult for subscribers to cancel: after easily subscribing online, subscribers had to call or use a chat with long waiting times to cancel.[158] Google assures people that they can easily delete their data in a dashboard, but makes the dashboard containing those options unnecessarily difficult to navigate and the options difficult to exercise.[159]

Some types of dark patterns involve trick questions with intentional ambiguity.[160] LinkedIn sometimes asks its users yes/no questions but, instead of allowing the user to answer "no," the alternative to "yes" is "No, show me more."[161] Barclays, among many other companies, makes you "[t]ick the box if you *don't* want marketing messages" (emphasis added).[162] A related type of dark pattern involves hiding useful information, making it difficult for people to make choices that the designer disfavors, such as deleting a profile.[163] Booking.com, for example, pretends to have a greyed-out button to delete your account, but the account deletion process requires you to check your email instead.[164] Facebook used to have several steps on its website to refuse cookies that included having to click on the button "accept cookies."[165] Bumble's explanation of how to delete your profile directs you to its "disable date mode" and "snooze" features instead.[166] Obstruction, trick questions, and hidden information have been found to be highly effective for companies to manipulate their users.[167]

Default settings or preselected options that benefit corporations turn into dark patterns when they're hidden or deceptive – like some systems of tracking.[168] If you registered with eBay using the "sign in with Google" feature, for example, you automatically opted into marketing emails.[169] In Google's ad settings, it's impossible to know whether "ads personalization across the web" is turned on or off by default.[170] In one experiment, preselection combined with clicking through another window more than doubled the number of people who were left with the pro-corporation option.[171]

Other tactics leverage deception to exploit our limited bandwidth to process information. Urgency tactics, such as false low stock messages, shortly expiring offers, or countdown timers, do this.[172] To trick people into resubscribing, *The New Yorker* sends a pretend final demand letter that reads "statement of account: FINAL NOTICE," but is just a request to renew the subscription, which would otherwise expire.[173] "Nagging" dark patterns are repeated or invasive requests to act in the interests of the service provider.[174] Duolingo's push notifications are so insistent that they've been the object of parody.[175]

Dark patterns, as these examples show, are widespread. You can find them throughout the information economy. One study identified them in 95 percent of the free Android apps in the Google Play Store.[176]

The GDPR, and privacy laws outside the EU modeled after it, create a framework that attempts to limit manipulation practices such as dark patterns. The GDPR, for example, requires that services be designed with data protection by default.[177] This default includes the principles of transparency and data minimization.[178] Arguably, most of the examples mentioned here breach these principles as they purposefully obscure beneficial options for people and aim to collect data that the service doesn't need to function.

These legal frameworks have been largely ineffective at protecting people from dark patterns.[179] Most dark patterns I mentioned proliferated after the GDPR came into force. In one broad study of pop-up banners after the GDPR, only 11.8 percent of websites were found compliant with minimum requirements so as not to be considered as deploying dark patterns.[180] If any of the dark patterns described here sound familiar to you from your online interactions with different corporations, then you already know that the law has been ineffective at preventing them.

Responding to these challenges, researchers propose a variety of legal strategies to address the consent problems dark patterns produce. Most of these strategies fit within the traditionalist paradigm. Some believe that more effective enforcement of existing laws is all we need.[181] Traditionalist laws, however, are oblivious to manipulation because they rely on the myth of apathy.[182] Others suggest antitrust legislation, arguing that a more competitive market would work well.[183] Antitrust proposals, though, don't address the deep consent flaws involved in dark patterns because they rely on the fictitious idea that people behave rationally with full information – and that more corporate alternatives would enable people to change the ecosystem. Some

suggest using the contract law doctrine of undue influence.[184] But the doctrine is more suitable for individual cases within bilateral contractual relationships than it is for systemic problems among numerous parties, some of which never interacted before.[185] Other proposals promisingly shift the focus toward extracontractual accountability. Some privacy researchers propose fiduciary duties, which mandate you to act in the best interest of someone else.[186] Those fiduciary duties imply imposing duties of care, confidentiality, and loyalty on corporations.[187] In a later chapter, I argue that a properly executed duty not to exploit is enough.[188]

Dark patterns aren't the disease. They're a symptom of law's focus on individual control, which is ineffective in an environment plagued with manipulation tactics that undermine people's autonomy by impairing real choices.[189] Dark patterns' pervasiveness poses difficult questions about the validity of individual agreements for the information economy overall. Navigating the necessary context-dependent nuances to distinguish valid from invalid agreements under dark patterns is a herculean task for any regulator or judge.[190] And if no one can identify which agreements are invalid, how can we justify relying on them?

* * *

Privacy laws around the world largely rely on two myths. One is that people behave perfectly rationally with regard to their information. The other is that people don't care about their privacy even if they claim to. The reality is that people who participate in the information economy are manipulated into situations that they wouldn't opt for if they could make informed choices that reflect their preferences. While people care about their privacy and the harms it protects them from, they aren't able to act according to that concern.

The rationality and apathy myths join in the worldview of the traditionalist paradigm. In this hypothetical world, people engage in bilateral agreements with the corporations that hold their data, make informed choices in those bilateral relationships, and take actions that result in an optimal level of privacy. Traditionalist privacy laws use these myths as building blocks. For example, notice and choice efforts, seen in the previous chapter, fail because they're based on the myth of rationality. The nothing to hide argument, similarly, fails because it's based on the myth of apathy. The overlap of rationality and apathy assumptions explains laws' consistent failure to address anti-privacy design.

The privacy myths weaken privacy laws that rely on them. The challenge is that, as the rest of this book shows, privacy laws across the globe incorporate them in some capacity. Current law reform proposals pivot on the mistaken idea of giving people enough information and options, trusting that those who care will choose correctly.[191] Even the most protective mechanisms of the last decade, such as the right to be forgotten, only work as intended if people use them to make rational and informed decisions about their personal information.[192]

Many modern laws and law reform proposals for the information economy have elements that escape these myths, such as privacy by design, data minimization, and information fiduciaries.[193] Those few and scattered parts of privacy laws represent meaningful progress. But they're few and they're scattered. If laws recognized that rationality and apathy are myths, they could focus on protection mechanisms that aren't undermined by the pervasive manipulation of individual choices.

In the meantime, people are overwhelmed by uncertainty and overstretched in an ocean of microchoices that change very little. Privacy law's paradigmatic subject – the one it aims to protect – is far from the hyperrational, fully informed machine that laws assume it to be. To be useful, privacy laws must account for the fact that their paradigmatic subject is swayed by powerful corporate actors every day.

Privacy laws' reliance on these two myths determines how much each of them makes individual agreements the distinguishing factor between legitimate and illegitimate data practices. The role of agreements in the information economy, as the next chapter explores, is inflated by these faulty assumptions about people's behavior, overlooking the central importance of context for people's privacy.

3

The Consent Illusion

A few years ago, Jordan Stein opened an OKCupid account and uploaded five pictures of herself to meet new people. She didn't expect to later discover, together with other OKCupid users, that her pictures were sold to another company, called Clarifi.[1] Clarifi uses these pictures to train facial recognition algorithms, learning about the biometrics of Stein and other OKCupid users and improving its ability to identify people from their facial features. Clarifi confirmed that it would use them to train autonomous weapons.[2] Led by Stein, users sued the company, but failed for lack of jurisdiction.

OKCupid's misuse of its users' data represents a troubling trend stemming from a lack of corporate accountability once users' agreement is secured. Why did OKCupid users consent to the policies that authorized sharing practices even though they would be hurt by them? They didn't really. Despite clicking "I agree," their consent was an illusion. But consent provisions in privacy laws globally stipulate that, if people agree to the collection, processing, or sharing of their data, the resulting data practices are legitimate.

Privacy laws that assume rational and informed people making choices in a functional data market stipulate that information should be acquired, processed, and distributed whenever people agree to it. While consent in privacy has been defined in different ways, these definitions are akin to consent in contract law, where consent is linked to agreement. In the EU, for example, the GDPR defines consent as "any freely given, specific, informed and unambiguous indication … [that] signifies agreement."[3]

This chapter explains why expecting individual agreements to protect privacy and reduce harm is a dead end. Individual agreements leave out inferences made about us, large anonymized datasets that affect us, and information about us that other people agreed to disclose. They fail at protecting us from the little they leave in because we must give agreement with no information, no real choices, and no bargaining possibilities. Such limited individual agreement is unable to shield people from data harms.

It gets worse. Users and corporations have a dynamic that philosophers and economists call "moral hazard." Privacy's moral hazard is the misalignment of incentives between corporations, who want to maximize profit from data, and their users, who

wish to participate in the information economy without exposing themselves to harm. In other kinds of relationships, the law worries about solving this deep misalignment of incentives that leads to exploitation. In privacy law, the misalignment persists. As a result, corporate actors are free to exploit people based on their personal information.

Consent provisions' mechanism is binary: you can, in theory, not agree to the collection of a piece of information but, once you agree, consent provisions don't protect you. Consent provisions only exist at the moment people are shown the terms and conditions, which one can call "I agree" moments.[4] But data harms happen later. People can't anticipate at "I agree" moments all considerations needed to make decisions. The relevant risks to making any privacy choice in the information economy aren't only unknown, but unknowable. In this context, granting impunity for consequences that happen after agreement is secured unshackles perverse corporate incentives. The incentive misalignment exposes people to pervasive harm.

A YOUR PRIVACY IS NOT AN ISLAND

About a decade ago, people began to fear that our phones are listening to us. Countless stories populated the web about personal conversations followed by an eerie closely related ad. Many concluded that we're being listened to by apps surreptitiously.

We're not. Our phones aren't listening to us because they don't need to. Instead, all the information we provide through them is pieced together to identify and predict patterns in a way that's cheaper and more effective than illegally tapping our microphones. Individual agreements don't cover all relevant personal data. They leave out inferred and de-identified data and, more importantly, can't address relational data. Their oversight makes consent provisions an ineffective protection tool.

Inferences and Aggregations: Information You Didn't Agree To

What we listen to on Spotify can be used to infer our ethnicity.[5] The type of coffee we order can be used to infer our political convictions.[6] Our text messages can be used to infer our income bracket.[7] These are just some of the thousands of ways companies know a lot more about us than we think they do.[8] Not only can this information harm us individually, but aggregation also causes social harms because identifying patterns uncovers group insights, such as shared preferences and identifying features.

Data brokers gather information about you from everywhere – every credit or debit card purchase, every discount code at an online store, and every loyalty card at your grocery store or hotel, among others. Acxiom, for example, has data about 2.5 billion people across sixty-two countries including age, gender, ethnicity, education, occupation, number and ages of children, income ranges, net worth, economic stability, purchases, payment methods, leisure activities, community activities, sports,

entertainment consumed, pets, marriage, divorces, and location.[9] Data brokers can match all of these with information from your social networks and your phone number because, when you clicked "I agree" to the respective privacy policies and terms of service, you agreed to data sharing. Because corporations trade data with each other, whom you disclosed information to doesn't matter very much.

Think of the amount of information each app on your phone has about you – your demographics, device ID, and location, to name a few. Every time you spend time with someone else, your phones know that you were together, for how long, when, and where. That allows corporations to cross-reference your browsing history, interests, and behavior with that of anyone you spend time with to show you ads based on the interests and behavior of those around you too. You may even have had a conversation about some things just before a related ad popped up, and ads may prompt you to have a conversation about others.

You may have thought, if that happened, that corporations surveilled you without your consent. The reality is that they didn't have to. Instead, they aggregated information that you "chose" to disclose, used it to infer more information about what you may be interested in, and weaponized information others disclosed to learn more about you.

Solon Barocas and Helen Nissenbaum warned us a decade ago that consent's problem "is not only that [it's] difficult to achieve; it is that, even if [it was] achievable, [it] would be ineffective against the novel threats to privacy posed by big data."[10] The issue is that large datasets run through AI reveal patterns. Different types of information, perhaps given to different corporations at different times, are compiled because people don't have a real choice over data practices.[11]

Two American cases illustrate this dynamic. In one, Jeremy Meyers sued Nicolet Restaurant because it illegally printed the expiration date of credit cards on sales receipts.[12] In the other one, Eric Kirchein sued Pet Supermarket because it illegally printed more than five digits of credit card numbers on receipts.[13] Meyers and Kirchein claimed that the stores had increased the risk that their credit cards would be copied. Both cases were dismissed. Printing a full credit card number instead of its last four digits or printing its expiration date together with the last four digits seems harmless in isolation. An expiration date alone is unlikely to lead to credit card fraud. So is exposing a few additional digits of a credit card number. Yet these practices facilitate malicious actors to aggregate data. External actors piecing together harmless financial data lead people to be rejected from loans, evicted, or have their utilities cut off.[14]

These cases underscore a central policy consideration about privacy: it's infrequent that a single piece of collected personal information is what leads to people being harmed.[15] In most cases, personal information becomes harmful when it's aggregated with other pieces of data.[16] Jordan Stein's loss, for example, wasn't so much the pictures themselves, but that the resulting facial recognition algorithm can identify her anywhere.

Aggregation creates privacy risks by unlocking inferences, particularly with the help of AI. Inferences exponentially increase the risk of harm because they collate meaningless pieces of information into meaningful individual profiles and group trends. Inferences lead to privacy-decreasing outcomes and, regardless of their accuracy, they enable harmful data practices. For example, they lead to price discrimination when a corporation determines that a user is willing to pay more than average for a product and charges them more than it charges others.[17] Or to actual discrimination when corporations profit from allowing advertisers to treat people differently based on their race, as in the Facebook ads example discussed earlier in the book.[18]

Decisions are nodal, contributing to a network that provides corporations more information about us. People are asked to disclose each piece of information to each single corporation. But they don't agree to the inferences made from this information. Although taken individually, each piece of information that corporations collect from us isn't particularly meaningful; their combination is.[19]

Inferences are invisible. We don't know what piece of information will be the one that completes an inferential sequence that leads to new information.[20] Risks posed by inferences are impossible to anticipate because the information inferred is disproportionate to the sum of the information disclosed.[21] This means that, in the information economy, we mistake the implications of the information collected about us, constantly underestimating how much privacy we cede.[22] People often mistakenly believe that a corporation's knowledge about them doesn't change much with new information, such as audio from a smart home device. But, at the margins, it usually does.[23]

Laws increasingly recognize inferences as personal information – something that it took them a while to do. In California, the Attorney General recently did so for access requests – when you ask a corporation what information it has about you.[24] European courts, similarly, include some inferences in these requests, such as comments on examinations.[25] Once one recognizes the importance of inferred information, it becomes apparent that there's no legal or conceptual reason to stop at access requests. Amendments to the California Consumer Privacy Act (CCPA), for example, expand protections over inferred information to other duties.[26] In Australia and Canada, privacy commissioners go further, stating that inferences are personal information for all purposes – although they lack interpretive authority over their laws.

However, even when acknowledged, inferences escape consent provisions. Requiring individual agreement for each inference would be unworkable, drowning us in an ocean of notifications that we don't understand.[27] Inferred information isn't protected by people's choices of whether to agree to corporate practices even under the most sophisticated privacy laws – it's personal data that no one agreed to companies having. Embracing the pervasiveness of inferred data marks the importance of not hanging privacy protections on the weak pegs of individual agreements. The inclusion of inferences isn't a sign that we could worry less about consent provisions, but a sign of reckoning with their unhelpfulness.

Privacy law, in sum, builds a back door for corporate harm if it doesn't protect people against inferences created by assembling collected information. And consent provisions can't protect against them.

Consenting for Others: Personal Information Is Relational

Under the information economy's consent models, each person is a prisoner of other people's choices.

Social networks often prompt you to "share with your friends," giving the impression that sharing is a two-way exchange. When they do so, companies are exploiting a heuristic.[28] Appearing to promote bilateral information exchanges, they're profiting from the reciprocity bias discussed in the previous chapter.[29] The information exchange isn't bilateral. You're not just sharing information with your friends. Rather, you're sharing information with your friends, the company, sometimes other people in the network, and anyone the company decides to give it to. More than information about yourself, you're also sharing information about others and tools to infer new information about them.

Information is relational in that it often describes interactions between people more than it describes discrete individuals.[30] Data are almost always about more than one person.[31] Imagine a holiday family photo that one family member uploads to social media. Does the platform need consent from every person in the photo to avoid violating their privacy? If it doesn't, there's a tension: each family member can't choose what to do with their information because they can't stop others from sharing it. If it does, there's a tension too: each family member can't choose what to do with their information because they can't share it without everyone else's endorsement. Because most data involve others, consent provisions create simultaneous and incompatible control-based claims. Their incompatibility curtails people's consent-based protection when people come to different decisions.

The impossibility of individual control would be a minor problem if what laws were trying to do was restrict data collection, processing, and sharing to nonharmful and socially valuable activities (as they perhaps should). But consent provisions are tied to providing individual control over data.[32] So relational data is a fatal problem for their effectiveness. A consequence of the reality that our data are informative about others is that, if laws aim to provide people with individual claims over their information, those claims become impossible to allocate. Individual control is simply impossible in the face of relational information.

The detrimental consequences of overlooking that personal data are relational extend to more significant situations than a family photo. Every individual decision about personal data has spillover effects on others.[33] Think of genetic information databases, where data from anyone with whom you share part of your genetic code are informative about you: if your sibling or your cousin sends a sample to 23andMe, the company will have genetic information about you even though you

didn't agree to anything.[34] People are exposed to harms stemming from data practices that depend not only on information about themselves but also on information about others over which they have no say.

Personal information's relational character leads some to see personal data as common goods, which are goods shared by members of a community.[35] This notion captures that any information has external effects.[36] It acknowledges, therefore, that individual agreements to collect, process, or share one's personal information affect others.[37] Those others are negatively impacted by data practices we agree to in ways that aren't captured by individual consent provisions.[38] Seeing information as the opposite (a private good) means treating it as a normal commodity, like apples, where one person's consent is enough. It neglects that personal information, unlike fruit, affects third parties. Besides, while most things we can sell can be replaced, one can't "replace" personal data once they're disclosed.[39]

Inferences are also relational. Companies run AI algorithms to infer information about you based on databases of information provided by (or taken from) others.[40] Your information is assembled with that of others to make probabilistic assessments about your social identities.[41] These assessments are then imposed on others who share those identities. Any well-meaning agreement to an app collecting your data, combined with others' agreement, can be used to inflict inferential harm on third parties – and vice versa. Because companies add people to datasets and infer information about each of them based on information collected from others, individual consent becomes increasingly meaningless as any dataset reaches more people.[42]

This reality creates a distributional problem. When members of socially privileged groups volunteer their data, the resulting data practices can benefit them while harming disadvantaged groups.[43] For example, many people install smart cameras on their front door as a safety measure, monitoring who walks by their house. However, they do so to the potential detriment of disadvantaged neighbors who are more likely to suffer any negative consequences from police surveillance over public spaces that the cameras provide.[44] The traditionalist reaction to the distributional concern is to blame those individuals and say they're apathetic toward privacy. A better response would be to address the perverse incentive structure that leaves others to be harmed when someone consents to an activity.

The personal data game, in short, is a group inferences game. Corporations obtain, process, and share personal data about one that not even a hypothetical fully rational and informed person would have had a chance to agree with, and perhaps wouldn't have.[45] The relationality of personal data isn't incidental to, but is part of, business models in the information economy.[46]

Overlooking data's relational character similarly leads to dismissing data's beneficial uses for others. The focus on individual consent and control prioritizes each individual's ability to decide what information they want to share and with whom over all else.[47] It insufficiently addresses legitimate countervailing interests.[48] Sometimes, privacy interests over low-risk data should yield to public interests, such as containing

a pandemic.[49] Privacy laws often address competing public interests by formulating exceptions for them, such as public interest exceptions.[50] But obligations on corporations to obtain individual agreements fail to adequately recognize interests beyond those of the specific individual who's asked for agreement.[51] Data's relational character is a broader, more significant permutation of the countervailing interest problem.

Privacy law fails to acknowledge relational data because it's hyperfocused on each individual. Law, as a consequence, allows companies to use one person's agreement to justify data practices about others. Providing consent for others, as we do in the information economy, is illegitimate under the parameters of any substantive consent model.

De-identified Data: Data No One Consented To

A related problem is the under-protection of so-called "anonymous" or de-identified data.[52] These are personal information that's harder to trace back to any particular person. Often, information is categorized this way because its identifiers, such as names or social security numbers, were removed.

In 2021, a Catholic news outlet used de-identified data that Grindr sold to third parties to identify and out Monsignor Jeffrey Burrill, a priest who promptly resigned after he was compared with pedophiles purely based on his sexual orientation.[53] He lacked protection over that data because, when acquired, the data lacked personal identifiers. In most legal regimes, anonymous data aren't considered personal data.[54]

The label of "anonymous" can be deceiving because data can often be re-identified with enough effort, depending on what other information is out there to match it with.[55] Sometimes, data can be re-identified quite easily.[56] Location data, like that of former Monsignor Burrill, are frequently re-identified. In one study, just four location points throughout a year were enough to re-identify 95 percent of 1.5 million Belgian cellphone users.[57] This means you could be located, for example, at an abortion clinic or a protest.

Re-identified data are individually dangerous in two ways: the privacy loss that re-identification involves in itself and the consequential harms that can accrue from it.[58] This combination of harms takes place, for example, when de-identified social security numbers are re-identified. Consent provisions fail to protect us against re-identification because re-identification is impossible to monitor after we click "I agree."

More importantly, group harms arise from large de-identified datasets through inferences. Data that are kept de-identified leak information because they uncover group trends. De-identified data provide inferences about preferences, behavior, population mobility, urban dynamics, and more.[59] People are harmed by aggregated de-identified information because it produces inferences about the groups they belong to and, by extension, group members.[60] For example, if a corporation has data about its users' sexual orientation and aggregates probabilistic information about the preferences and behavior of Queer individuals, then it knows more about

each Queer user than if it only had the former. Privacy laws overlook possibilities to harm without re-identification because they over-focus on each individual and ignore group harms.

The group harms of de-identified data illustrate another shortcoming of the "nothing to hide" argument, discussed earlier in the book.[61] These inferences expose people to harassment, discrimination, and human rights abuses, especially against members of vulnerable groups. Someone might think that they individually have "nothing to hide" and should be uninterested in keeping information private. But the more information corporations collect, the more accurately they can target a group with personalized ads or algorithmic decision-making, producing group harm. Other people in their community thus have something to lose. These group harms can't be reduced by addressing privacy through individual choices.[62] When viewed from this social perspective, the nothing to hide argument becomes even more evidently inadequate.

Laws must move away from the dichotomy of identified versus de-identified information. This false dichotomy results from the binary view, under which information either eliminates people's privacy or doesn't affect it. Moving past it implies acknowledging that de-identification is a spectrum of security over information, that information throughout that spectrum is personal, and that social harm exists regardless of re-identification. The focus of regulation should be setting standards for reasonable levels of de-identification to minimize risk, rather than creating false dichotomies within the spectrum.[63] Such a change would enable legislators and enforcement authorities to develop reasonable security standards.

With or without appropriate regulation, de-identified data poses a twofold reason to avoid relying on individual consent provisions. First, these provisions leave out data obtained as de-identified that can be re-identified. Second, they don't protect from group harms triggered by data that remain de-identified. The processing and sharing of de-identified information escape consent requirements despite their potential to harm.

***

Individual consent models have three crucial blind spots: inferred, relational, and de-identified data.

A privacy traditionalist would have a quick solution to the issue. If the problem is that consent provisions don't ask for permission to infer information, from the multiple people information relates to, and from anyone for de-identified information, they would propose that we simply require consent for that too. Problem solved. For example, while there's disagreement, many believe that the GDPR covers inferences. But the problem runs deeper than that. Even if it were possible to ask for agreement for inferences, relational data, and large anonymized databases in a workable way (it isn't), people can't provide genuine consent to this information because, as the next section explores, it's impossible to know how it will be used and what its risks are.

B UNATTAINABLE CONSENT IN THE INFORMATION ECONOMY

Criticizing consent in privacy isn't new. Privacy scholars showed that information asymmetries between users and corporations pose a significant barrier to the consent model.[64] They indicated that consent and privacy self-management fail because they require managing a vast amount of information and decisions, which the protection system doesn't equip people to do.[65] They convincingly showed that meaningful consent to facial recognition, like Jordan Stein and other OKCupid users provided in theory, is impossible.[66] Their work uncovering why consent provisions are flawed shows that these provisions' limitations are systemic. It indicates that context-specific fixes can't address the problem.

Agreement to terms of use has three deficiencies that make it not synonymous with consent. First, consent is impeded by information asymmetries. Second, it's impeded because we often have no alternative. Third, because we have no possibility to negotiate. Underlying these problems that lead to meaningful consent being unattainable in the information economy are relationships of unequal power. Consent provisions, due to these problems, are unable to do what they're designed to do in the first place, which is capturing consent.

No Information

Corporations have a lot more information than their users do about the interactions between them. Economists call this situation "information asymmetry." People can't understand privacy policies, estimate the value of their personal information, or gauge the risks that they face from its collection.[67] This asymmetry puts people in a vulnerable position because they lack enough information to choose whether to agree to the different things that corporations ask them to.[68]

In the US, privacy's information asymmetry has been referred to by the FTC, coupled with the language of market failures, to promote regulatory interventions independent of consent provisions.[69] This effort is a step forward, but it still mistakenly assumes the existence of a market with failures one can fix. Functioning markets require prices, which reflect consumers' preferences for products and services. By contrast, as Katherine Strandburg explains, "Data collection would serve as 'payment' in that critical sense only if its transfer from users to collectors adequately signaled user preferences for online goods and services."[70] It doesn't.

In the information economy, it's impossible for people to assess the risks involved in disclosing their personal information.[71] Privacy law's assumption that people can calculate risks appropriately when agreeing to data practices is mistaken. People don't know how their information will be used and what exactly can and will be done with it.[72] The information economy forms an opaque system where we even ignore how much information was collected from us.[73] The time and information required to assess risks when providing agreement are insurmountable. The

clear signaling of user preferences, which Katherine Strandburg explains would be needed for a market, doesn't exist for personal data.

Making matters worse, corporations have economic incentives to mislead their users. Whistleblower Frances Haugen revealed proof of this reality at Facebook, which was accused of driving engagement at the cost of harming teens and spreading misinformation harmful to democracy.[74] But perverse economic incentives are by no means exclusive to Facebook. Because people can't sufficiently understand privacy terms and conditions, corporations can engage in manipulation and exploit the limits of people's information-processing ability in pursuit of corporate interests.[75] People would need an unreasonable amount of time and effort to understand each mechanism of manipulation.[76]

Policymakers, legislators, and academics often call for corporations to improve privacy notices to increase transparency.[77] However, we now know that notices are ineffective at increasing users' understanding of how their personal information is collected, processed, and shared.[78] They lead us to mechanically click "I agree."[79] One reason why privacy notices are ineffective is that there are too many cognitive steps between the information disclosed (for example, location tracking) and the risk of the information (for example, where you went, when, and whom you spend time with).[80] This is true regardless of how simply privacy notices are formulated or how visible they are. Numerous transparency efforts are undermined by their reliance on rationality.

For consent provisions to work, people would have to understand the risk of their information in advance. They never do. So it's difficult to believe that people can ever truly make informed and welfare-enhancing decisions regarding their privacy in the information economy.

No Choices

Privacy laws across the globe are undermined by their reliance on individual choices. Elena Gonzalez and Paul De Hert write that individual consent, which has become a "cornerstone of data protection" in the EU (among many jurisdictions), "is only appropriate if the controller can offer genuine choice, control and responsibility to individuals over the use of their personal data."[81] But, in the multi-party information economy, this doesn't happen.

The necessity of online life renders countless choices obsolete. There are often no surveillance-free alternatives to services that are necessary to meaningfully participate in society.[82] This situation puts service providers in a position of power over their users, who have no choice but to accept their terms. As FTC Chair Lina Khan recognizes, "[w]hen faced with technologies that are increasingly critical for navigating modern life, users often lack a real set of alternatives and cannot reasonably forego using these tools."[83] People are placed every day in take-it-or-leave-it situations between using a product or service and giving away personal information or

not using the product and limiting their social participation.[84] To participate in the information society, you need to agree to be surveilled.

A high schooler, for example, might think they're missing out on valuable social opportunities if they're not a member of the same social media platforms as their peers. Someone concerned with COVID-19 might consider it inviable not to have a contact tracing app. Someone looking for a job may have to use LinkedIn. As I write this, accepting the Microsoft Office and Outlook privacy policies is a requirement of my job. Products and services like email, cellphones, and even some social networks are a core part of our daily interactions, so opting out of them is disruptive. We periodically agree to more data practices than we otherwise would because the consequence of not doing so is social or economic exclusion.

Income inequality adds a distributional concern. Those who are economically disadvantaged have the least ability to make choices over their data, as they have fewer options and fewer means to protect themselves. Consent provisions are especially unhelpful to them. Precarious financial positions limit access to paid, privacy-protective services to replace free, surveillance-intensive ones.[85] People need to accept loaned laptops from work or school when they can't afford their own, ending up with an added layer of surveillance from their work or school. In the case of devices that are sponsored and dependent on an internet connection, such as Chromebooks, they end up with added surveillance from Alphabet too.

The entrenched imbalance between corporations and people is aggravated when people must use free services at the cost of their privacy. Because of the lack of options that results from financial constraints, those who need the most protection are precisely those who, under contract-law-inspired consent provisions, have the least. This doesn't mean that there's something wrong with providing free services or devices that include surveillance. It means that we can't rely on consent provisions to prevent harms that result from that surveillance.

We need to accept whatever terms services put before us because we need them to participate in the economy and social life. Agreement to them isn't given freely. Therefore, it doesn't amount to consent.

No Bargaining

Consent provisions are also ineffective when information is available and outside alternatives exist.

A former Privacy Commissioner of Canada once told me that, one time that she was buying an item at a mall while in office, the store clerk required her phone number and email to complete the purchase. She explained to the clerk that the request was illegal under Canadian law. But there was nothing the store clerk could do, and she ultimately relinquished the information to be able to leave with the item she needed. Not even the most powerful user in the most innocuous privacy interaction has leverage.

What's left for the rest of us? We can either give blanket agreement to terms and conditions or avoid digital products and services.[86] The intermediate option, to choose what's collected or how, is removed, not contemplating that some form of collection may bring a smaller privacy loss while allowing for functionality and profit. The lack of bargaining means that consent is worse off.[87]

Privacy laws expect us to bargain for our data while failing to equip us with the tools to do so. We're expected to manage our own privacy by deciding when, how, and to whom we give our information.[88] The bargaining expectation is fed by the regulatory model of privacy self-management.[89] This model is built on the false assumptions that individuals are rational and informed, and will thus make optimal decisions regarding their data.[90] The bargaining expectation overlooks the real dynamics between users and corporations, which are so unequal that they evaporate any semblance of mutual agreement. Consent provisions pile, on top of the unfulfilled promise of informed choices, the impossible-to-meet burden to make those choices anyway.

Even reaching the relevant parties with whom to bargain over our data is hopeless. Many corporations, such as data brokers, come into contact with someone's information only after a different corporation collected it. This detachment makes bargaining with them impossible. Jordan Stein's experience with Clarifi, for example, illustrates how we have little to no recourse to third parties that acquire and use our data under the contracts worldview of privacy. Further, harm often results from the combined actions of several corporations that are impossible to identify ahead of time. Harm is usually a product of inferred information about us, often partly inferred from information collected from others.

Lack of information and lack of choices make the lack of bargaining for our data worse than other take-it-or-leave-it situations. First, our lack of information produces uncertainty. People can't negotiate over data practices because they can't estimate the harmful effects that each of them can have.[91] Unequal bargaining power between corporations and their users is magnified by information asymmetries because users can't rationally assess the risks involved in the take-it-or-leave-it alternative. People can't bargain over something if they don't know what they're bargaining over, whom they should try to bargain with, what alternatives they have, or the risks at play. Second, people have no choices, so they must accept any terms, such as those of a social network they must use to find a job or room to sublet, or an app they must use to trace COVID-19. The alternative is social or economic exclusion, so there's no take-it-or-leave-it because they can't threaten to walk away. There's just taking it. This burden is compounded for socioeconomically disadvantaged people.

Glossing over people's lack of bargaining power perpetuates the myth of apathy. Not even someone with privacy expertise in the simplest bilateral scenario, like the privacy commissioner in her story, is in a position to bargain in the information economy. That doesn't mean they don't care.

The Result: No Power

The original GDPR draft had a curious provision: "Consent shall not provide a legal basis for the processing where there is a significant imbalance between the position of the data subject and the controller."[92] But the provision was struck from the amended versions.[93] A possible reason is that those circumstances are ever-present in the information economy. Leaving that provision, and taking it seriously, would have been equivalent to stripping consent out of the GDPR. Believers in the traditionalist paradigm in industry and government wouldn't allow for that.

A uniquely problematic aspect of surveillance is the unequal power dynamic between the people who are surveilled and the corporations that surveil them.[94] The corporations that require our agreement for digital products and services also control the digital ecosystem through those same products and services. Even if information asymmetries could be evened out, users would remain at a disadvantage.[95] Because of the power imbalance in how users and corporations interact, regulators can't reinforce consent and improve users' relative position simply by mandating notices that reduce information asymmetries, using competition law to break up giants and give us alternatives, or banning take-it-or-leave-it consent. People have far less power, which leads to a lopsided dynamic that persistently favors corporate interests.

Consent provisions can't overcome the injustices caused by this power imbalance. Privacy law's reliance on consent and control as mechanisms of self-protection exacerbates those power imbalances, extending the problems of privacy self-management from law in theory to law in action.[96]

The roadblocks of no information, no choices, and no bargaining in a context of differential power lead to exceptions to the primacy of individual consent in other areas of the law. But they don't in privacy. Workers can't contract for pay under the minimum wage and construction workers can't contract out of the need to wear hard hats.[97] Most countries regulate pesticides, denying people the ability to waive those regulations.[98] Under product liability law, you can't consent to harms that are extravagant.[99] In privacy law, you can.

The use of AI to make decisions about us, such as our credit scores and employability, exacerbates the power imbalance between people and those who hold their information. Privacy law can address this imbalance if it distributes power instead of assuming users already have it. As Daniel Solove puts it: "Privacy involves the ability to avoid the powerlessness of having others control information that can affect whether an individual gets a job, becomes licensed to practice in a profession, or obtains a critical loan … [and] the power to refuse to be treated with bureaucratic indifference."[100] That's only possible, however, if privacy law moves beyond mechanisms that allow those with power to act with impunity as long as they extract agreements.

***

Consent provisions don't capture consent. Our consent is undermined by asymmetries of information, lack of choices, and absence of bargaining. For individual agreements to equate with consent, people must be able to imagine potential harms (so that choices are conscious), have alternatives (so that choices are real), and choose seriously (so that choices are meaningful).[101] Agreements in the information economy can't meet these conditions.[102]

C INFORMATIONAL EXPLOITATION

In January 2021, queer dating app Grindr faced a historic fine of 10 percent of its global annual revenue.[103] The fine arose from Grindr sharing information about its users to third parties, like the one used to identify Burrill, while having inadequate consent provisions. The shared information included users' sexual orientation and their HIV status.[104] The Norwegian Data Protection Authority ruled that the take-it-or-leave-it option in Grindr's privacy policy, which asked people for blanket agreement to its data practices, was insufficient due to the information's sensitivity. According to some sources, Grindr's user data had been available for sale since 2017.[105]

The experience of Grindr users, like those of Jordan Stein and other OKCupid users, illustrates how in-advance individual agreement is unhelpful to prevent harms that stem from data. Technically, users agreed to the data transfer and uses in advance through the app's privacy policy. Broadly, their experience uncovers the obsolete character of our protection system. Even for the Norwegian authority, while protecting users, the problem wasn't the data practice; it was the consent provision.

Consent provisions can't help us prevent harms related to surveillance due to informational exploitation. Because corporations don't face the consequences of the risks that they create for people, and reap more rewards the more risks they create, they have incentives to collect, process, and disclose personal data in risky ways. Since consent provisions don't survive "I agree" moments, they fail to create incentives or obligations for corporations to take care of users' data after this point. Informational exploitation makes relying on individual agreements counterproductive for reducing harm.

Privacy's Moral Hazard

Moral hazard refers to the idea that organizations take too many risks if they're not fully responsible for the negative consequences of their actions. Moral hazards happen when there's impunity for those consequences. For example, if a bank knows that the government will bail it out if it makes risky investments, it may be more likely to take those risks, knowing that it won't bear the full cost of eventual losses. That situation encourages risky behavior that leads to negative social consequences. Moral hazards happen, in particular, when someone's behavior affects someone else's wellbeing, and the second person can't control the first person's risky behavior.

So the first person has incentives to minimize care and maximize their benefits at the expense of the second person.[106]

Moral hazards are enabled by information asymmetry. They happen because one of the parties can't monitor what the other party does, but what the other party does continues to affect the first. A mechanic, for example, knows more about cars than a car owner, so they could exploit the owner's lack of knowledge and overcharge for repairs. In the information economy, people have far less information about what corporations do with their personal information than the corporations do. This information asymmetry makes it difficult to monitor corporate behavior. Without proper monitoring, corporations can take excessive risks with personal data to increase profits, given that people will ultimately bear any risk.[107]

Uses and disclosures of data continue to affect users' interests and wellbeing after the moment of agreement, as the OKCupid and Grindr examples illustrate. They do so because personal information inevitably retains a connection to the person, even after they no longer control it.[108] Conversely, over-collection, irresponsible processing, and risky disclosures are profitable for the entities engaging in them.

Because people don't know when a corporation engages in risky behavior, corporations have incentives to take more risks than people would agree to. Corporations are in a position to reduce the amount of harm. But, given that such a reduction would be costly and they aren't liable for the harm in question, there are minimal incentives for them to protect their users and others.[109] As a consequence, corporations' risk-taking after they obtain agreement proliferates harm, negatively affecting people's wellbeing.

Aligning incentives is central to attenuating moral hazards, especially when the affected individuals continue to be affected by the other's actions indefinitely. In other areas of the law where parties are affected after their interaction, scholars and policymakers consider structural lack of incentives to take care as a significant drawback of relying on consent. This happens, for instance, in environmental law, regarding carbon dioxide emissions.[110] When there's a lack of restrictions and monitoring, corporations have incentives to take environmental risks to minimize private costs, such as those created by environment-preserving measures. Costs are then externalized to the general population, for example in the form of pollution. Algorithmic harm is analogous.[111]

If people could know in advance how much risk each corporation will take and they could monitor each corporation's data practices as they happen, the contracts paradigm would have a solution: parties could add a contractual clause that internalizes the risk.[112] But people are unable to do so because of information asymmetry, lack of choices, and inability to bargain with the countless parties that collect, process, and share their data. Because users can't anticipate the magnitude of risk associated with any data practice, it's impossible to factor it into agreements. In light of moral hazard, our agreements can't set adequate incentives for any moment after the moment that we agree. That would remain true even if they covered inferred, relational, and de-identified data.

Moral hazards, in sum, are about perverse incentives. Corporations in the information economy have incentives to increase the risk for people because they don't bear the cost of such a risk increase. This incentive misalignment leads to perverse risk-taking and harm.

Moral Hazard's Exploitative Outcome

When privacy law came about, before anyone could predict we would all carry internet-connected computers in our pockets, let alone AI inferences, it was difficult to predict the inadequacy of contracts-based privacy laws for inferences and multiparty data flows across borders. This obsolete character results because our protection system allows corporations to collect, process, and share anyone's personal information by securing far-reaching and unconditional agreements. The consequence is informational exploitation.

Corporations in the information economy, as a result of their moral hazard, have incentives to exploit people in two ways: extracting benefits and affording little protection. These track to what economists call "expropriate" and "shirk."

The first mechanism is exploitation through data misuse. Corporations have incentives to use personal data in risky ways that can be harmful, including sharing user data with third parties. Corporations have incentives to aggregate de-identified information to a point where it can be easily re-identified. They have incentives to give it away for profit, as OKCupid and Grindr did. They have incentives to collect as much as possible and infer as much as possible, even though this creates new risks. Some of these data practices may increase expected harm for people more than they increase expected profit for companies. But corporations have incentives to engage in such socially harmful behavior anyway because they can externalize that risk to others.

This first mechanism extends to (lack of) beneficial data practices. When there are measures that could benefit people, corporations are disincentivized to implement them in our regulatory landscape because they bear their cost and don't benefit from their risk reduction. Beneficial measures would involve avoiding risky or harmful uses of de-identified data, such as re-identifying them. Other beneficial data practices would be collecting as little information as possible or not sharing information with third parties if not needed.

The second mechanism is exploitation through lack of safeguards. Profiting from someone's data while placing insufficient security for it is one way of exploiting it. Corporations have incentives to minimally comply with data security obligations to prevent data breaches.[113] For example, when encrypting your data, they have incentives to use minimal encryption that's easier and cheaper to implement, but also easier and cheaper to override.[114] Cybersecurity regulations, which determine sufficient data security practices, must mandate specific protections because privacy law fails to encourage corporations to establish high thresholds. Many data breaches are carried out by another private actor (a hacker), but are enabled by corporate

actors' unlimited data collection. Another form of exploitation under this second mechanism is enabling intimate harms such as nonconsensual distribution of intimate material by platforming and amplifying them for profit. Many websites that hosted nonconsented material about Dr. Jacobs, whose story is discussed earlier in the book, engaged in this form of exploitation.[115]

Business models temper the second mechanism's incentive misalignment only slightly. Some corporations receive a reputational gain from data security that provides economic incentives, but the size of those incentives depends on each business model.[116] Apple and Microsoft have better incentives to provide privacy protections than Alphabet and Meta do because their business model doesn't rely on targeted ads, so they can advertise those protections to improve their competitive position.[117] But these are exceptions. And even corporations that market their privacy protections have an underlying moral hazard dynamic with their users, so informational exploitation persists. There's no economic reason for most corporations to implement these safeguards other than compliance with regulations or a tenuous benefit over competitors from a reputation standpoint.[118] Grindr's privacy policy, for example, says: "Grindr cannot guarantee the security of your Personal Information. Our security, safety, and privacy features are provided on an 'as-is' basis."[119]

If the entities profiting from our data and deciding over its safeguards bore the benefits and risks of their data practices, they would have incentives to engage with the data responsibly and implement adequate safeguards.[120] In a context of no information, no choices, and no bargaining power, weakened consent provisions can't align these incentives. Even if they did, the misalignment would remain for all-important inferred, de-identified, and relational data. Informational exploitation isn't the result of poor user choices. Rather, it results from a structural lack of incentives for corporations to consider their users' interests and wellbeing.

Informational exploitation persists because the law relies on individuals foreseeing all possible harms at "I agree" moments to protect their own privacy. Personal data affect our wellbeing post-agreement. And they do so forever. But we only get a chance to agree once, later on impaired from understanding what's going on by moral hazard. This dynamic allows data profiteers to disregard any negative effects on us. Consent provisions condense the little protection they provide on people's shoulders at that moment. They're contrasted by accountability mechanisms that govern data practices throughout their duration.

The Search for Autonomy in Refusals

In 2019, thousands of Facebook users posted different permutations of a lengthy message on their profiles that started with "Facebook does not have my permission to share photos or messages." Instructed by friends and acquaintances to copy and paste it into their profiles, users did so in an attempt to stop the company from giving their data new uses that had been falsely announced.[121] None of those messages on

user profiles work.[122] Facebook users had already agreed to the privacy policy and, for the law, that's what matters. Their agreement withdrawal didn't count.

The proposal to rid the information economy of consent provisions faces an autonomy-based objection. People may want to control the information that companies have about them.[123] People may want to choose what kinds of data they give up, when they do so, and to whom.[124] Consent provisions allow us to feel as if we have a say in our privacy, even if we don't.

The limit of the autonomy objection is that the changes in corporation–user interactions needed to turn agreements in the information economy into true consent are so colossal that consent provisions lack autonomy value. The fact that we can't understand what we agree to or its consequences deprives agreements of this value. So does exploitation.

Capturing privacy consent is attainable in some situations. These situations are when (a) there are no unconsented inferences or data about us taken from others and (b) we understand the consequences, have alternatives, and can agree to part of it. It's just that these situations don't exist in the information economy.

Agreement equals autonomy-enhancing consent, by contrast, in most privacy interactions between individuals. For example, recording an intimate encounter is appropriate only if those recorded expressed informed consent (knew its potential consequences), held power (no duress or pressure), and could dictate the terms of the recording (what was OK to record).[125] Consent also requires, though, that the person recording doesn't have a blank check to do what they want with it after their interaction.[126] Imagine someone consensually records an encounter and later harms someone by using the material in ways that the person technically authorized but couldn't foresee. We would consider those actions to fall outside what was consented to because we can only consent to foreseeable things we're taken to understand. Unforeseeable harms that enable exploitation such as that one, which preclude autonomy value, may be exceptional in one-to-one interactions, but they're the rule in the information economy. If one cares about autonomy, no data in the information economy can be left at the mercy of individual agreements.

For those who are unpersuaded of the need to eliminate individual consent provisions in the information economy, there's a moderate alternative: treating agreement as a necessary but insufficient condition for legitimate data practices. This alternative retains the little autonomy value our agreements have. It matches with individual-to-individual interactions, where agreement isn't the only distinguishing factor for legitimacy (as many laws for the information economy make it into) but a necessary yet insufficient condition for it. Although it overlooks the problems outlined in the first part of this chapter, it captures exploitation. For this moderate path, Facebook users' withdrawal should have counted because treating consent as a necessary but insufficient condition prevents data practices when agreement is refused. Consent provisions' unhelpfulness to protect from harm, one could argue, doesn't imply that refusals to agree shouldn't be considered.

There are few times when we can refuse a data practice in the information economy. Apple provided space for this with third-party tracking for iPhones, and over 90 percent of users exercised it in one way or another.[127] Android users sometimes deny permissions when they're clear and they have a choice, particularly when apps ask for access to their microphone or calendar.[128] A moderate alternative could discard provided agreements while contemplating refusals to agree, as rare as they are. If this direction were followed, it would constitute a "right to refuse" data practices, which would group and broaden two narrower rights in the GDPR: the right to withdraw and the right to object. We just can't depend on it; we otherwise risk building a back door into the few protections people are granted.

Consent's Social Norms

Refusals to data practices can't be determinative in all circumstances. In some situations, it's unreasonable not to provide data. For example, it would be unreasonable to borrow a library book and refuse to give any information for the library to track its return. Implementing refusals to agree independent of circumstances would impede socially beneficial uses of low-risk data, such as for medical advances or public health. These uses have positive externalities to others and society that may not be appreciated by each individual.[129] They can be prevented if each individual has an unqualified power to stop data practices.

Laws could contemplate refusals to agree when there's no overriding public good – making the mechanism in accordance with social norms and values. More specific alternatives, like carving out exceptions from refusals for all de-identified data and inferences, rather undermine protection.[130] When there's a public good involved, systemic regulations that focus on reducing surveillance while allowing for functionality are more protective than relying on individual refusals to agree or misleadingly presenting issues as a conflict between privacy (consent) and public health.[131]

The limit of refusals to agree comes from the realization that consent shouldn't be the main mechanism to legitimize data practices. When individual agreement is the only mechanism for a corporation to acquire, process, or share information about us, it gets enshrined as a universal valve to determine legitimate information flows. Helen Nissenbaum calls this valve a "transmission principle."[132]

Think of a time when you considered whether revealing something about someone was appropriate, and what made it so. The "what made it so" changes depending on the information and who it's about: the answer depends on the social value of specific actions.[133] To determine the social appropriateness of an information flow, one needs to identify what makes it so, and there's no universal transmission principle for people's information.[134] So if the law aims to reflect shared social norms and values on privacy, it needs to employ the correct transmission principle too.

Most privacy laws around the world, with the exception of the GDPR, apply one transmission principle (consent) across the board, using it as the default way to

legitimize data practices.[135] But the reality is that social transmission principles vary according to context.[136] Universal consent provisions are at odds with the idea that privacy is about context-dependent appropriate flows of information.[137]

One way to add precision to the context-informed role that refusals to agree could take in the information economy is by tracing an analogy with the role of consent for our physical integrity with the tort of battery. A tort is a noncontractual act or omission that results in injury for which those who committed it are liable. The tort of battery, at least according to one view, prohibits touching others in a socially inappropriate way. If you tell someone not to touch you on the shoulder and they do anyway, that constitutes battery. It's not that it's battery *because* you told them not to, but because telling them not to made it inappropriate to do it.[138]

One could argue refusals matter in battery for similar reasons they did for third-party tracking with Apple and they should have for Facebook users. Information about us is inevitably linked to us, like our bodies are.[139] Data, like our bodies, are part of us, and what people do with them after an agreement impacts us, unlike what people do with commodities we give them.[140] In both battery and privacy, refusals act as a proxy for interference with the social value of autonomy, given this prolonged impact. But an activity can also be inappropriate because it breaches another social value, such as intimacy.[141] How the law addresses the body may provide better analogies for data than how the law addresses objects that become irrelevant to us after we give them away.

At a minimum, the information economy requires the treatment of individual-to-individual privacy interactions, where agreement is a necessary but insufficient condition for legitimacy. This treatment would make refusals to agree determinative, rather than making agreements so. However, refusals to agree face two limits for privacy protection: they're a proxy for autonomy value, not a synthesis of social values, and the consent illusion makes them extremely rare. The best way out of the consent illusion may be to stop dreaming of individual consent.

* * *

Consent's primacy derives from contracts theory. Laws widely recognize people's ability to voluntarily bind themselves into obligations by agreeing to them. Individual consent-based mechanisms from contracts theory are a suitable legal solution for an enormous number of contexts. They're just the wrong mechanism for protecting personal data in the information economy. Individual agreements leave out important types of personal data, consent is unattainable for the types of data that the agreements do cover, and relying on these agreements is counterproductive for reducing harm.

The reality that corporations leverage people's data for profit, carrying inevitable risks, is understandable. In some contexts, it may even be desirable. However, data practices' profitability shouldn't provide immunity to abuse the power of holding people's data. Neither should individual agreements to those practices.

Privacy consent is an illusion. Consent-based privacy protections allow corporations to do as they please with people's data as long as they're able to extract superficial agreement. We routinely experience this (lack of) protection when we mechanically click "I agree" to websites' and apps' terms of service. Individual consent provisions fail to address the harms produced by aggregated, inferred, and relational data. They ignore information asymmetry, lack of choices, and unequal bargaining.

Consent-based protections have a deeper problem: they bolster the wrong protection mechanism. Circumscribing protection to them unshackles informational exploitation. Unless otherwise constrained, corporations lack incentives to minimize processing and disclosure harms to people who can't predict or monitor their behavior. Data entities lack incentives to incur the costs of caring for this information or to moderate their data practices to avoid risks. The cost of data practices is borne by people through increased risk of harm, while their profit is captured by corporate entities, leading to excessive collection and excessively risky uses and disclosures. This dynamic is mirrored regarding data safeguards, where corporations bear the costs of safeguards and the benefits accrue to users, resulting in few safeguards. People are exposed to harm, such as financial, reputational, physical, or discriminatory, as a result of corporations' lack of incentives to avoid risk.

If consent provisions are meant to be a mechanism to help people manage their data risks to prevent harm from taking place, they have failed. If the opposite is true, and consent provisions are a mechanism to allow corporations to profit while harming people by complying with checkboxes, then what's the point of requiring them to collect agreements?

Privacy law must transcend the consent illusion that defines the prevailing and ineffective approach to preventing data harms. Abandoning harm prevention to individual self-management, as consent provisions do, is equivalent to deregulating the information economy. Overcoming laws' ineffectiveness at curbing informational exploitation requires new accountability mechanisms that mitigate harms regardless of whether these harms accrued through data practices that people agreed to. Privacy law must focus on establishing duties that pair with those harms.

The next chapter explores how these problems translate into improved consent provisions. The real choice in privacy law reform isn't between individual control and harm prevention. It's between harm prevention and a mirage of individual control that, given how the information economy is structured, will never exist.

4

Manipulation by Design

Improvements on consent provisions hit a wall because dark patterns are just one instantiation of a broader problem of power to manipulate.

Think of all the shopping websites that have fake timers for their discounts to get you to buy fast, even though the timer restarts and the offer continues.[1] Or apps that pressure you to sign up for a no-strings-attached "free" trial by labeling it as a limited time offer even when it's not.[2] Think of websites that shame you for not providing your email for a discount, using pop-up messages that say: "No thanks, I like paying full price," or "No thanks, I hate saving money," instead of a simple decline button.[3] Digital manipulation is such a pervasive feature of the information economy that we grew accustomed to it, and sometimes we barely notice it anymore.

The design of the systems we interact with impacts our privacy. Choice architects hold significant power in shaping people's behavior.[4] Despite people not reading privacy policies, the information conveyed through design choices affects their decisions.[5] It's not new that people, particularly when acting as consumers, don't behave according to hypothetical rational choice models. Corporations have always designed choices to influence people, such as through product placement or payment methods. But the extent and scale of this influence in the information economy, and its resulting exploitation, is unprecedented. In the information economy, those who design our choices also design how we communicate with each other and have power to use our personal data against us.[6] Influence is exerted over everyone, every day.

Product designers introduce strategic friction, which makes some choices easy and others difficult, to the detriment of their users. Amazon makes it easy to sign up for a Prime membership, but to cancel it you need to find your way through six layers of menus repeating your intention to cancel in each one of them. The menus have buttons that change content to make them difficult to find, such as "end membership," "cancel my benefits," "continue to cancel," and "end now."[7] When you miss a day of language practice on Duolingo, you'll see a teary owl cartoon with the caption "11 day streak lost! Do you want to repair your streak? This helps us keep education free" and a button for "repair for $3.49."[8] The information economy gives companies endless possibilities to introduce friction by designing the choice mechanisms that people go

through. Yet existing law is oblivious to manipulation because it relies on the myth of rationality – the idea that we're immune to it – and the myth of apathy – the idea that if we "chose" to reduce our privacy, we must be OK with it.

Manipulation causes improved consent provisions often lauded as best practices, such as opt-in consent and informed consent, to fail at protecting us. The way opt-in privacy options are designed determines our choices. It's impossible for us to estimate the risks of data practices even when we're informed. The large power asymmetry between us and the designers of the services we access combines these two problems. The outcome is that it's impossible for us to know which interactions with digital services are beneficial to us.

This chapter explores two stories: the opt-in/opt-out catastrophe of tracking laws in the EU and the fiasco of regulating ISPs in the US, through the lens of behavioral science. These stories illustrate how power imbalances make it easy to exploit people's biases. They show how aggregation and inferences make it unreasonably difficult for people to understand what's going on, obfuscating the privacy risks associated with broad and superficial agreements. And they reveal why the most robust versions of consent provisions are ineffective: these efforts still rely on us making choices we're unequipped to make. This chapter then explores regulatory designs that may thwart some of these issues, with a recognition that a comprehensive solution would require major reform, such as the one advocated in the chapters that follow.

A MANIPULATIVE CHOICE DESIGN ON BOTH SIDES OF THE ATLANTIC

Traditionally, individual consent is manifested by opting out of a data practice, such as tracking. Many modern attempts to strengthen people's choices flip this dynamic, establishing that instead of having people tracked until they opt out, they shouldn't be tracked unless they opt-in. The opt-in versus opt-out dichotomy, as Helen Nissenbaum and Solon Barocas explain, is "hegemonic across a range of online practices."[9] The objective is familiar: improving consent and increasing control.[10]

At first glance, it may seem as if opt-in consent departs from the traditionalist, neoclassical paradigm: it considers the behavioral science insight that people tend to stick to default options. This departure, though, is a red herring because opt-in rules still rely on the flawed notion of contracts-like choice. These rules assume that people will avoid opting in if they care about their privacy and, if they do opt-in, they must not care about it.

Tracking in the EU

The EU experience with online tracking sheds light on the limitations of opt-in and opt-out systems. European efforts to regulate tracking failed because they overlooked insights from behavioral science and design in an environment of entrenched power.

A lot of tracking happens through cookies. Cookies are bundles of information installed on our devices that store data about us. They allow websites to identify a device when it visits them, remembering information from prior interactions.[11] They present enormous possibilities for profitable surveillance.

Data protection law provided Europeans with a right to refuse tracking since the 1990s, including cookies.[12] This right was implemented through an opt-out system, where people were considered to have consented to cookies unless they indicated otherwise.[13] The choice to opt-out left data collectors with two obligations: to inform people about the purposes of data collection (notice) and to give them the right to refuse it (choice).

The EU then implemented the Cookies Directive.[14] With the objective of enhancing individual control, the directive changed tracking through cookies from an opt-out system to an opt-in. Moving from an option to opt-out of tracking to one to opt into tracking (or vice-versa) is a way of changing the default. The opt-in system, unlike opt-outs, required consent to be given before any tracking. This prior consent, according to the interpretive authority at the time, could be obtained either explicitly by people agreeing to cookies or implicitly.[15] People who continued to use a website after being warned about the site's cookie policy were deemed to have consented implicitly.[16]

All EU countries but one initially allowed for implicit opt-in consent. Simply clicking somewhere on a website constituted (implicit) consent. The Netherlands, by contrast, required explicit consent. As a response, websites stopped installing cookies in visitors' devices automatically and began to display banners asking whether the visitor would allow the installation of cookies.

We've all encountered cookie banners, a type of privacy notice popping up to tell us about cookies when we open a website. This happens because the GDPR later changed the consent requirement in the EU: user inactivity is no longer sufficient consent.[17] Based on this new provision, the Court of Justice of the EU indicated that opt-out systems in general, and continuous browsing in particular (opt-in with implicit consent), aren't valid consent under the GDPR.[18] Now, European cookie banners must follow the Dutch rule: you need to click "I agree." As a consequence, the Dutch experience is informative of what is now the broader European experience with tracking.

The Way the Cookies Crumbled

Dutch regulators interpreted the demand for prior and specific consent as requiring explicit consent for cookies.[19] But corporations responsible for implementing the Dutch regulation found ways to make their countervailing interests prevail. Websites implemented the consent model by presenting banners and pop-ups when people entered a website.[20] To get people to accept cookies, some websites used banners that occupied most of the screen and only allowed access to the website

after agreeing, which was known as a "cookie wall."[21] As a result, the rule was considered a regulatory failure by the media, the people it was supposed to protect, and the political parties that developed it.

There were several complaints about the regulation. For members of the industry, the regulation "doesn't help anybody and makes it more complicated for both us and for the consumer."[22] Stakeholders, including media companies, complained that the requirement was disproportionate to the aim of increasing individual control.[23]

People were also dissatisfied with the rule. People reported that it led them to mindlessly click to allow cookies every time they entered a website, thwarting its purpose.[24] They said that the law was impractical and it missed the point.[25] Consumer associations complained that privacy protection should be implemented with user friendliness in mind.[26] Dutch academics called the regulation a "policy fiasco of impressive dimensions."[27] Dutch data protection scholars claimed that the regulation's main effect was making it more difficult to offer services, hindering commerce.[28]

Making matters worse, compliance with the regulation was low. Many websites installed prohibited cookies on their visitors' computers.[29] These rogue sites included the websites of political parties that had voted in favor of it and the Dutch government itself.[30] When faced with these results, political parties who originally voted in favor of the regulation stated that it was unworkable and had to be put to an end.[31]

Compare the Dutch regulation with the most influential example of the opt-in with implicit consent: the British regulation, which was then part of the EU. Like the Netherlands, the UK departed from prior norms that only required an opt-out option.[32] Unlike the Netherlands, the UK adopted the minimum protection by implementing an opt-in system with implicit consent, deeming explicit consent too burdensome when applied to all cookies.[33] The British Information Commissioner's Office (ICO) set a low bar for implicit consent, which included visiting a website without blocking cookies. Its guidelines required consent to be prior to tracking only "wherever possible."[34] The British government further stated that consent isn't time-bound, so it doesn't have to be acquired prior to tracking when doing so is impractical.[35]

Implicit consent rendered the change of default imperceptible. If any user who visits a website without blocking cookies is considered to be implicitly opting in, the distinction between opt-in and opt-out systems fades.[36] In practice, the user behavior needed to install cookies is the same: accessing the website. While the Dutch regulation became the strictest legal system in the world regarding cookies, all others stayed eerily close to an opt-out system. What they had in common is that neither of them provided meaningful protection.

Pushback eventually led the Dutch government to relax the regulation.[37] The revision allowed websites to let people show consent by clicking on any part of the website if it's clearly shown to them that doing so signifies agreement. In doing so, the Dutch also moved to a system of implicit consent that rendered its opt-in characterization questionable.

Since the Dutch fiasco, the European Data Protection Board ruled that cookie walls, which block website content until cookies are accepted, are illegal.[38] National authorities, accordingly, sanction companies when they don't provide an easy method to refuse cookies.[39] But manipulation and exploitation prevail, such as through dark patterns.[40] Many cookie banners have "accept all" highlighted and "personalize choices" shadowed.[41] Others go further and have hidden preselected options. A 2022 study shows that 60 percent of privacy notices with defaults in a sample from European websites have at least one dark pattern.[42] Prohibiting specific manipulation tactics, such as preselected options or cookie walls, is bound to be insufficient because of the countless ways choice architects can nudge and manipulate us.[43] The problem wasn't solved because these new regulations focus on a technology (cookie walls) rather than an activity (manipulation). They attempt to reinforce individual consent while overlooking its systemic problems. As a result, the EU is back to where the Dutch regulation was.

Defaults and Informative Notices in the US

The US has traditionally relied on opt-out consent, similar to the British tracking regulation. The CCPA, for example, became known for giving people the right to opt out from most forms of third-party sharing, including inferences.[44] There was one point in time, however, when the US got close to the GDPR's opt-in model.

In 2016, the Federal Communications Commission (FCC) tried to help people protect themselves from the prying eyes of their ISPs. A document called the Privacy Order required ISPs to obtain consent to collect (and, by extension, use or share) their users' personal information.[45] ISPs would have been required to obtain explicit opt-in consent for most types of personal information and opt-out consent for the rest.[46] Congress disapproved this protection, also banning other federal agencies from passing similar regulations.[47] But the Privacy Order brings broader lessons for privacy regulation.

ISPs have virtually unrestricted access to their customers' personal information through their IP addresses. For example, data giant Alphabet can gather information while people use its products, such as its search engine Google, its email service Gmail, and its web browser Chrome. ISPs can see everything people do on their Wi-Fi: every website visited, every video and song streamed, and every file downloaded. As Paul Ohm explains, "an ISP can always access even more because it owns and operates a privileged network bottleneck, the only point on the network that sits between a user and the rest of the Internet … the greatest point of control and surveillance."[48] However, in the US, ISPs face overall less privacy regulation than other corporations such as Alphabet (Google) and Meta (Facebook).

Although, in theory, people can opt out of ISP tracking through self-protection, this is easier said than done. Doing so requires circumventing ISPs' tracking efforts. Most privacy enhancing technologies are ineffective against tracking by ISPs because

their benefits only appear after one connects to the ISP server. Other means, like free virtual private networks (VPN) and the encrypted browser Tor, while effective at masking from an ISP, come at the cost of usability and speed. Privacy tools also require people to be familiar with their specific functions and limitations. People are thus expected to bargain with their ISPs for privacy protection as a hypothetically rational and informed being would. This model doesn't conform with reality. People lack information, outside options, and bargaining power.[49] And they can't monitor what their ISPs do after agreement, which provides ISPs room to exploit them while abiding by any promises.[50]

The disapproved FCC rule, which aimed to solve this regulatory void, paralleled current EU cookie regulations. For most information accessible to ISPs, by requiring explicit consent, the rules would have shifted the tracking default to an opt-in similar to the Dutch regulation and the current EU model. Default's stickiness would support the idea that ISPs should restrict the data collection by default. If the default setting is do-not-track and ISPs need clients' agreement to track them, the contracts worldview tells us that a change to opt-in consent should provide meaningful protection.

It doesn't. These disallowed FCC rules would have experienced equivalent issues as cookie banners. As we learned from the Dutch experience, it would have likely fallen prey to exploitative design. Notably, information overload, discussed in the next section, leaves people equally vulnerable under opt-ins and opt-outs because it prevents them from understanding how much privacy they're losing when they agree.

The Power of Designing Choices

Behavioral scientists distinguish two ways to set nudging defaults, called policy defaults and penalty defaults. Legislators use policy defaults when they set by default an option that they would like people to keep, such as countries that make people organ donors unless they opt out.[51] These defaults rely on inertia and the status-quo bias to increase the number of people who stick to the regulator's preferred option.[52]

Legislators use penalty defaults when a more informed party in a contract withholds information from their counterpart, creating an information asymmetry. Sometimes, parties withhold information to obtain a larger portion of the benefit resulting from a transaction, which economists call surplus.[53] Penalty defaults counteract incentives to withhold information strategically.[54] They work in three steps. First, legislators set as the default an option that's costly for the more informed party.[55] Second, the more informed party bargains with the less informed party to get them to agree to a different option.[56] Third, through bargaining, the more informed party provides information to other parties, reducing the information asymmetry.[57] The appeal of penalty defaults stems from their information-inducing properties: compelling the informed party to reveal information mitigates their value-destroying behavior.[58]

The answer to which default rule the Cookies Directive and the FCC Privacy Order used depends on what their aim was. If their aim was to reduce the overall amount of tracking by nudging people to stay under do-not-track, they implemented a policy default. If their aim was to ensure informed consent by nudging websites and ISPs to disclose information, they implemented a penalty default.

Penalty defaults, at first glance, seem to have a strong case in favor of an opt-in system for cookies, as platforms are more informed than their users about the cookies they install. What determines penalty defaults' success is whether they leave less-informed parties better informed – a crucial element of consent. Do-not-track defaults can be seen as penalty defaults that aim to increase transparency by counteracting incentives to withhold information.[59] Arguably, their hope is that a burdensome default option (do not track), encourages websites (and ISPs) to give people more information when attempting to persuade people to switch away from the default.[60] Ideally, they would leave people better informed of cookies' functions, advantages, and disadvantages. This didn't happen.

Do-not-track defaults haven't been effective at inducing helpful disclosures that reduce the asymmetric information between websites and their visitors about data practices. They haven't been effective at reducing the overall amount of tracking either. The defaults, instead, make websites disclose that they use cookies, sometimes providing information about cookies' functions aimed at convincing us that they're important and we should accept them. Although European countries continue to apply opt-in for tracking, people don't become informed about what's most relevant: the privacy loss that follows after they click away cookie banners.

***

Cookie banners are one of the most common ways to strategically introduce choice friction. Some cookie banners have hidden preselected options, making them into dark patterns.[61] Some are just defaults. Both of them, from users' experience, are a nuisance.

Cookies might soon be a thing of the past, but their lessons won't be. Alphabet and Apple, among other companies, propose moving away from tracking based on cookies.[62] Alphabet, for example, proposes to substitute cookies with analyses of browser history to identify topics people are interested in.[63] Others propose that companies just ask people about their preferences and habits instead of inferring them.[64] The significance of this change for business models and power dynamics invites skepticism. Surrounded by promises of better individual control as default changes were, the tracking methods being entertained would channel existing dynamics of power, manipulation by design, and informational exploitation into surveillance through different technical means.

Companies can exploit their users' biases and inability to anticipate inferential harms with little to no safeguards. Imagine a hypothetical provision that prohibited

deception and perfectly captured individual consent – where people had complete information and real choices to use products without surveillance. One might think that this protection would put a halt to many companies' business models. But corporations have enough design leeway to reconfigure their products so that their core features are only accessible with agreement. Reconfiguration would again push agreement away from consent. The perfect consent provisions that the law systematically fails to create would be futile because of power-enabled exploitation in the information economy.

B THE LIMITS OF TRADITIONALIST SOLUTIONS

Companies can infer your gender, ethnicity, political views, religion, and sexual orientation just from your Facebook likes.[65] Without knowing your likes, they can infer your sexual orientation just from your public list of Facebook friends.[66] With some more data, such as your browsing history, companies can infer your age, gender, occupation, education level, and general personality traits using technology from over ten years ago.[67] As AI keeps taking over data processing, the amount of information that can be extracted from each data point increases. The sheer amount of data inferred in the information economy is hard to fathom.

Consequently, people can't understand how informative each data point collected from them is. They face an information overload, which prevents people from grasping how each piece of information puts together the puzzle of their digital identity.

Information Overload

Opt-in efforts try to overcome consent problems by changing the default from "tracking" to "no tracking." But consent problems run deeper than that. Two biases discussed earlier in the book undermine changes from opt-out to opt-in: the influence of context on our choices and our inability to estimate the risks of each data collection.[68] They're captured by the idea of information overload.

Information overload is a special bias in the information economy because it undermines a key aspect of decision-making: it prevents us from understanding what information we're giving away. Information overload happens when people have to process so much information that their decision-making ability is negatively impacted.[69] In the face of inferences and relational data, people struggle to estimate the informativeness of each data point. When people provide a corporation with a piece of information, they often mistakenly believe that the corporation's knowledge about them doesn't change much. This leads people to underestimate the amount of privacy that they cede to corporations.[70] The bias benefits data companies: it contributes to unrestricted data collection by extracting agreement more easily than they otherwise would.

Information overload makes understanding how different types of data fit together particularly difficult.[71] Data combine into inferences that are impossible to predict.[72] Companies leverage seemingly innocuous collected information to infer activities and habits, including those we intended to keep private.[73] For example, if you use a smartwatch that measures your heart rate data and can access your cellphone app usage, you're also revealing stress levels, mood, smoking habits, progression of Parkinson's disease, sleep patterns, levels of exercise, and types of physical activity.[74]

Information overload is a growing problem in the information economy. The amount of data collected and inferred is exponentially larger than in the pre-AI world that most privacy laws were designed for. AI inferences worsen information overload. By being unpredictable, they increase estimation difficulties. Further, we don't know what information about us is out there for corporations to aggregate or what means they have to aggregate it. Because these calculations are impossible to make, risks are unforeseeable. As AI inferences continue to grow, so will the insufficiency of our processing ability to estimate our losses.

A daily-life example can illustrate our challenges to appreciate how the size of a data pool exponentially increases the precision of inferences that can be determined based on that pool. Imagine someone called Brooklyn is deciding whether to get an audiobook app. Brooklyn knows that, in doing so, they grant a corporation access to app use data. Imagine they get Audible, owned by Amazon. Although they realize that Amazon can learn about them through the app, they underestimate how much Amazon can infer because adding all data points and figuring out inferences require computational power that no human has.[75] Brooklyn's underestimation of their privacy loss worsens when Amazon and other corporations that collect Brooklyn's data combine the information they have, making more unpredictable inferences. Further, corporations don't consider anyone's data in isolation – information is relational. By aggregating Brooklyn's information with others', Amazon makes more inferences. For example, Amazon will make inferences about Brooklyn by examining the shopping patterns of people nearby.[76] As a consequence of underestimating losses, Brooklyn may even allow Amazon future data collections that they otherwise wouldn't have, such as their apartment floorplan if they buy an Amazon-owned Roomba.

While we realize that, the more data corporations have about us, the more accurate their inferences are, we can't identify how quickly the precision of these inferences increases or the direction they take.[77] When Brooklyn accepts Audible's terms of service, they realize that they're granting Amazon access to their location data. But they miss how much Amazon can learn from that information. For example, the app would record where Brooklyn goes on weekday mornings and evenings. Based on this alone, Amazon can infer where Brooklyn lives, works, and how they commute. Brooklyn's location around midday reveals their lunch routine and their evening location reveals where they like to have dinner. In this way, the app effortlessly

collects data that it can use to learn about Brooklyn's shopping habits, hobbies, and social network. Similar inferences take place when people use the Amazon website. Information has synergies, and the risk of a bundle is more than of the sum of its parts.

Despite reading and understanding the terms of service, Brooklyn didn't realize what outcome they agreed to. Regulating Amazon to mandate plain language in its notices, a popular approach in privacy legislation, wouldn't help.[78] The GDPR, for example, indicates that these notices should be "concise, easily accessible and easy to understand" and written in "clear and plain language."[79] Brooklyn's lack of knowledge, though, isn't because they didn't read the policy or didn't understand the words used. The cause of the misunderstanding is that Brooklyn systematically underestimates how much is inferred.

By making us underestimate our privacy losses, information overload prevents us from realizing how much risk our information involves.[80] One may think that Brooklyn's priorities might differ from everyone else's, they know their best interests, and don't care about privacy – they're apathetic. But, in the information economy, we're all Brooklyn.

Expecting people to estimate the risk of their information before deciding to agree is unfeasible because the risk of information isn't linear. Disclosing all sixteen digits of your credit card, for example, is exponentially riskier than disclosing only four digits. The risk of any data point changes depending on the combination of the other data points. And, in addition to information overload, people have no way of knowing what information is already known about them, ready to be combined.[81] The increased risk of each data point, such as an additional credit card digit, is impossible to estimate.[82]

People are also unlikely to understand how data collection will affect their lives in the future. People also have no way of knowing what information about them will be acquired later to combine with what's collected today. People can't anticipate the ripple effect of information trades because, after corporations collect their personal data, they share information with each other and make further inferences about them. Underestimation also happens when data is anonymized because, as discussed in the previous chapter, they enable inferences about those who belong to a group.[83] For example, if a neighborhood is classified as one where many people with high blood pressure live, an insurance company could increase rates based on zip codes.[84]

Policy discussions of tracking defaults depart from the myth of rationality. But only by considering one bias: defaults' stickiness. Information overload demolishes our safeguards against those specific biases because it causes disadvantageous agreements for everyone on the Internet. If all of us have difficulties identifying what data we're giving away, it's easy to see how society ends up with monumental amounts of data in the hands of entities that can use it against our best interest.

Like Brooklyn, we're often manipulated into giving away tools to build inferences about us for profit. Brooklyn's example might seem like a defect in need of repair,

but a closer look reveals a deeper systemic problem. This model of exploitation, enabled in part by consent-reinforcing policies such as defaults, is a built-in feature of the information economy, not a bug.

Can Defaults Solve It?

The behavioral science of defaults explains why opt-in efforts don't work to protect us from tracking. Websites wanted people to switch away from the default, but the most effective way to achieve this wasn't to carefully inform them about the risks of tracking. It was to manipulate them. What people faced wasn't a real do-not-track default, but the illusion of choice. The Dutch story illustrates what can go wrong when regulators make protections conditional on choices while overlooking the power of choice architects.

Legislated defaults don't always yield their expected outcome.[85] Choice architecture can be effective when regulators design the choices but, when corporations do it, they can circumvent legislative intentions.[86] Legislative defaults are ineffective when they allow the exploitation of people's biases.[87] This limitation is prevalent in penalty defaults, which seek to use the threat of lost profit to leverage companies to inform their users.

Corporations in the information economy can skirt opt-in regulations by manipulating choice architectures, nudging us into switching away from the default.[88] Dutch websites, for example, manipulated their visitors in their presentation of choices without breaching the regulation. Consent-enhancing regulations like this one are undermined when legislators fail to anticipate the multiple ways behaviorally informed corporations can circumvent them. Their ineffectiveness is acute in the information economy due to privacy's moral hazard, which leaves countervailing incentives unchecked. Entities with a vested interest in people agreeing to tracking are poor candidates for receiving the power to shape how choices are presented.

For a change of default to yield its expected result, people must be treated similarly regardless of their choice.[89] A do-not-track default only works if people under the do-not-track regime and the track-me regime are treated the same. Otherwise, most of the policy's benefits are lost.[90] People under the Dutch regulation were often unable to access the website, facing a "cookie wall" that put pressure on choice.[91] Dutch users' choice wasn't whether to be tracked, but whether they still wanted to visit a website seconds after typing its URL. When they could access a website without cookies, these often malfunctioned because the negative choice meant that cookies necessary for some features weren't installed. Regulations can limit differential treatments, but those limits are difficult to determine in advance and even more difficult to enforce.[92]

Websites can (and did) reframe tracking choices. Designers can exploit how context influences our decisions, using framing tactics so people pick options that are better for corporations.[93] Many websites still frame their visitors' choices by presenting

cookies as necessary for websites' functioning. Framing from Dutch websites when they placed a banner that included only the "yes" option, so people who wanted to choose "no" had to leave the website since they had nowhere to manifest their choice, was stronger – an early example of what we would now call a dark pattern.[94]

Cookie walls that block website content, and cookie banners that don't, lead people to auto-accept and develop consent fatigue, where people automatically dismiss any options in their path to access the content they were looking for.[95] Anti-privacy design techniques for increased surveillance continue to exist. They're particularly powerful when combined, like when notices have ambiguous language and preselected options.[96]

Information asymmetry is part of a multifaceted problem. It's true that websites know more than their visitors about the cookies they install and people don't know enough about them to provide informed consent. People's lack of information, however, isn't the main problem. If it were, one could solve it by educating people about tracking technicalities. Similarly, people don't fail to opt out of tracking just because of inertia. Inertia can only go so far and, although the costs for opting in or out of tracking defaults is low (just a click), few opt out of tracking and many opt into it. Information asymmetry and inertia pile onto the uncertainty problem that unshackles moral hazard: the risks of agreeing aren't just unknown to us, they're unknowable.

The implementation of EU tracking regulations illustrates opt-ins' limited helpfulness for people facing power imbalances and multifaceted information problems in the information economy. The switch of default had little effect. The resulting massive opt-in agreements are something that people wouldn't have chosen in a position of rationality and power. Their choices weren't real.

Can Contract Law Solve It?

The traditionalist paradigm sees people's personal information as a commodity that gets traded in a market.[97] Under that view, it's natural to look at contract law mechanisms to address the information economy's problems, as courts increasingly have.[98]

Contract law has different ways to address consumer biases in standard form contracts, written in advance by one of the parties (like those we sign with our gyms and banks). Chiefly, it does so through the doctrine of unconscionability.[99] Courts use unconscionability to invalidate a contract, or a clause within an otherwise valid contract, if it's an improvident bargain resulting from unequal bargaining power.[100] Consumers use the doctrine to invalidate abusive clauses, sometimes scaling-up the lawsuit to a class action.

The doctrine of unconscionability has been criticized as insufficient to deal with many biases in standard form contracts.[101] Its insufficiency even leads some contract law scholars to argue that cognitive errors should be ignored in unconscionability determinations, as evaluating biases requires evidence of mental processes that

courts lack.[102] Information overload is one of those biases that unconscionability doctrine can't solve. Unlike narrower biases that consumer contracts aim to address, information overload operates even when people have all information.[103]

Information overload places a hurdle on unconscionability determinations. For unconscionability to address information overload, judges would have to make individual assessments, since the risk of each data point about a person depends on the other information already known about them. And the bias is ever-present. If judges believe information overload impairs consent for some and not for others, the individual analysis of each decision by each person in the information economy would be practically impossible. Judges would lack the bandwidth to analyze whether the consequences of each choice were comprehensible to each person or whether the amount of personal data inferred was too large relative to the benefit that each one received. If, instead, judges believe information overload impairs everyone's consent, it follows that it's a systemic problem for which individual contract law solutions such as unconscionability are inadequate. In that case, expecting each user to go through a court to obtain a separate unconscionability ruling is unreasonable. Rectifying at-scale online manipulation requires holding those in a position to manipulate accountable for their practices, instead of attempting to identify whether each individual succumbed to the manipulation.[104]

Even if these issues could be addressed, a problem unique to the information economy remains: once a user's data have been used to learn more about that person, it's virtually impossible to force the other party to "unlearn" it. Unconscionability is concerned with nullifying a clause (or, at best, a contract) after data transfers happen, and nullification is poorly placed to address privacy because companies cannot "unlearn" what they learned from a user's data, particularly after inferences. Harms would remain.

Countries without the doctrine of unconscionability would also struggle with using contract law to address the problem. Contract law in civil law jurisdictions, such as most European and Latin American countries, doesn't include unconscionability. Instead, it has concepts such as abuse of rights and lesion. These concepts are also used to invalidate clauses – or, occasionally, contracts – based on individual determinations. These concepts suffer from unconscionability's shortcomings: they require agreed-upon contracts to be in place to evaluate when to void a particular agreement. They presuppose a mutual agreement with valid consent over a core set of contractual provisions. But manipulative data practices and informational exploitation exist in the absence of agreements. Therefore, they can't be addressed through contractual remedies in civil law countries either.

A third contract law approach to reinforcing consent in light of errors is the doctrine of unilateral mistake. As a traditional casebook explains, someone can void a contract "if the material mistake of one party was caused by the other … [or] the other had reason to know of it."[105] The doctrine is well reflected in a classic case in which the US government purchased furniture for a hospital from Frank Hume at 60 cents per pound.[106] This was a clerical error: they meant 0.6 cents per pound.

According to the court, if Hume knew about the error (or if he should have noticed), the contract should be set aside.[107] While cognitive errors are distinct from clerical ones, it isn't obvious that the law should treat them differently. Corporations are or should be well aware that their users can't properly estimate their privacy losses, just as Hume should have known about the clerical error.

Despite its appeal, the doctrine of unilateral mistake faces equivalent limitations to the doctrine of unconscionability. Courts, after all, sometimes interpret the doctrine of unilateral mistake as a manifestation of unconscionability.[108] Courts, once again, are poorly placed to evaluate the sufficiency and clarity of each privacy notice for each person in the context of the other information available about them, which must be aggregated to evaluate the mistake. Even if they were well placed, nullifying an agreement once the information was collected and the privacy lost is far from an ideal solution, as the inferred data can't be unlearned. And they would probably have to apply the doctrine to everyone, rendering all agreements null.

Faced with information overload, we can't estimate how much privacy we lose toward the corporations we interact with – let alone the ones we don't. Contract law doctrines such as unconscionability, unilateral mistake, abuse of rights, and lesion assume that there's a core, mutually understood agreement from which one can separate invalid clauses. Although standard form contracts may have that agreement over core elements, privacy interactions lack it because of information overload. Information overload is a systemic problem, yet any determination borrowed from contract law depends on individual assessments. These individual assessments are at least insufficient and at most inadequate.

***

Contracts-based approaches are inappropriate because contracts are assumed, at least in principle, to be mutually beneficial, resulting in surplus to distribute between the parties that leaves them both better off than before. Privacy interactions aren't. In the information economy, there's no reason to believe that all privacy interactions produce mutual value. Some do. But, because consent isn't working to distinguish value-creating interactions from the rest (even when improved by opt-in), there's no contractual mechanism left to differentiate them. In other words, without a mechanism external to the will of the parties, there's no way to ensure surplus-creating data interactions while preventing non-surplus-creating ones. Especially since, in the information economy, these interactions happen at a large scale.

C IMPROVING TRACKING REGULATIONS WITH BEHAVIORAL SCIENCE

Invisible tracking goes beyond cookies. In a 2019 US Supreme Court case, Paloma Gaos sued Google representing a group of users. Google had been giving websites

information about people's search terms that led them to the sites by including this information in the header.[109] This data practice wouldn't have been caught by the EU cookie regulations or the US ISP regulation, which focused on a type of technology – cookies and IP addresses respectively. Similarly, Meta provides websites with a line of code to track you across online activities, called the Meta Pixel.[110] It works whether you have a Facebook or Instagram account or not, and without installing new cookies. To be effective, regulations must focus on the underlying relationship intermediated by technology (surveillance), not the specific type of technology (cookies).

Can Notices Be Improved?

Privacy policies are ineffective by design – not by accident. After seeing their ineffectiveness through behavioral science, one could ask if behavioral science provides a way to improve them. In the sense of making them better at informing people, it does. But the failures of opt-in defaults and contract law mechanisms to rescue privacy's consent provisions uncover that information improvements don't address the deeper problem at hand. Improved privacy policies would still be impaired by informational exploitation.

Any regulation with the modest aim of informing users should include provisions that reduce information overload. Changing a default isn't enough. The information problem isn't just that people have limited attention and defaults are "sticky." Nor is it just that people don't know what information is out there. Rather, the information problem is behavioral: people's inability to estimate their incremental privacy losses. To make informed choices, people would need to know how information fits together.

The effectiveness of transparency duties hinges on people's ability to process information. A disclosure that considers information overload must help users understand what the information actually means in the context of other information being collected. Legislators can design better privacy notices to limit the effects of information overload by mandating notices that consider the effects of information collection, rather than their technical aspects. They can do so in three steps.

The first step is for notices to explain the informativeness of collected data, rather than data collection methods, in a way that's easy to interpret. Empirical studies show that simplifying how data collection methods are described doesn't improve people's understanding of what happens with their data.[111] For notifications to be useful, they must address the information's significance. Being told "we track headers" wouldn't have helped Paloma Gaos and other Google users understand the data's significance as much as "when you click on a link, the website will know where you navigated from." One way to explain significance is through examples. Transparency's bottleneck isn't the amount of information people receive but their ability to process it correctly. Examples are essentially pre-processed information,

so they can mitigate information overload.[112] The notifications mandated in the Cookie Directive and the FCC Privacy Order didn't achieve this enhanced form of notice. The cookie banners informed people that a website used cookies and the Privacy Order would have, at best, required ISPs to disclose collected data to their users. These rules overlooked information-processing limitations.

The second step is explaining how the information aggregates with other information. A central aspect of information overload involves inferences: how a user's data combines with other data to learn more about the user.[113] Reading "we collect location data" is less informative than reading "we collect location data; this can be combined with location data from your other devices and publicly available information to tell us when you are at home, at work, or at a store." The first text addresses information asymmetries about collection methods. The second text also explains the privacy loss caused by typical inferences. With the first text, users would know that their location data are being tracked. But they might not realize how easy it is to aggregate this with their home and work address to infer, for example, how much time they spend at the office. This step includes explaining how different types of data fit together. Paloma Gaos' header data could be aggregated with countless other data Google had about her, such as her location and others' location, that one can't expect users to anticipate when clicking "I agree."

The third step is indicating how the information combines with future information. To be complete, disclosures should help people understand how the next collected data point changes things – not just what's already known.[114] I used to schedule my office hours with Calendy, which integrates with the Meta pixel.[115] Even if, when prompted to integrate them, I knew everything that Meta knows about me prior to collecting my schedule data (I don't), I wouldn't be able to estimate my privacy loss without knowing what Meta will collect, including from others, later. A complete disclosure would have to help people understand how the company will make inferences by pooling the collected data with other data it expects to receive.

Improved notice mandates, as limited as they are, can and should combine these three steps. Legislators and regulatory authorities have an opportunity to catch up with the knowledge of people's biases that private actors in the information economy already have and employ. People would benefit if, rather than receiving mandated disclosures with long, technical details on data collection, sometimes plagued with technical jargon and legalese, they received clear and simple information about the significance of collected data and the inferences they unlock.[116] This might sound like new information, but it isn't: it just takes people one step closer to understanding their privacy loss.

These behaviorally enhanced privacy notices can only act as a partial remedy. Design manipulation isn't unique to defaults. The reality of designers nudging users to accept designers' preferred choices applies to enhanced privacy notices too. For

example, corporations could make these notices long, leading people to accept them without reading, as many do with terms and conditions.

Can Cookies Be Reduced?

Tracking regulations would improve with two changes: reconsidering choice designers based on their power and differentiating between types of tracking based on their losses. First, whenever possible, regulations should target entities that don't profit from tracking directly – and therefore have fewer incentives to undermine the policy. In the case of cookies, these entities are web browsers instead of websites. Second, regulations should better differentiate between types of tracking to reflect the different privacy losses that they involve and their relationship with information overload. In the case of cookies, regulations should distinguish between session cookies, which expire when the browser is closed without being stored, and persistent or permanent cookies, which remain in storage until deleted.

The first change that would improve tracking regulations is giving the power to design choices to entities with fewer incentives to undermine them – even if they still have some. Many of tracking regulations' problems would have been moderated by targeting web browsers instead of websites. Browsers can operate as gatekeepers and choose whether to let cookies through, websites' intentions notwithstanding. Like regulations called on websites to apply a do-not-track default, they can call on browsers to block cookies sent by websites by default.

Browsers have fewer incentives than websites do to manipulate the default, while they have the technical ability to block cookies.[117] Browsers' business models are less dependent on cookies, so they would lose less profit by having fewer of them. Profits would be reduced – particularly for Chrome, owned by Alphabet – but less than websites that depend on cookies to place targeted ads.

Browsers are also easier to monitor than websites. The Internet has millions of websites but five browsers through which most traffic passes. Requesting them to block cookies would establish a do-not-track default that's easier to enforce. Under the GDPR, each website has to design a banner for the opt-in mechanism. Monitoring five banners to ensure they aren't manipulative is a lot easier than monitoring thousands.

Browsers can implement a tracking policy better. They can ask whether to navigate with cookies in a more relevant context than that of websites – even when well intentioned.[118] When websites ask whether you agree to cookies being installed, you're asked every time you change websites. People find these interruptions bothersome.[119] If browsers posed this question instead, people could be asked when they open their browser. This change would avoid interrupting navigation. It would allow people to switch more seamlessly from tracking to no-tracking by opening a new window. Requesting browsers to block cookies thus allows for a more user-friendly way of knowing whether a user wants to browse with or without them.[120]

This change fits better with the aims of tracking regulations, such as the Cookies Directive, of requesting consent in a way that's as user-friendly as possible within technical limitations.[121]

Most privacy-enhancing technologies – especially those that are more sophisticated – have usability issues.[122] A function embedded in browsers would be simpler to use. This change would align with broader efforts to hold companies accountable for embedding privacy as functionally as possible within the design specifications of the data-fueled products that people use, called privacy by design.[123]

The second change to improve tracking regulations is differentiating between types of tracking based on their privacy loss. Do-not-track regulations would become more effective by allowing for session cookies while preventing permanent cookies from being installed. Differentiating cookies helps address choice overload and sets better incentives for corporations, which is crucial in a context of informational exploitation.

Different cookies produce different levels of privacy loss. Among other distinctions (strictly necessary, functional, stats, marketing, etc.), session cookies disappear after the browser is closed while permanent cookies remain in storage until the user deletes them.[124] Permanent cookies – which can last for years – present a higher risk than session cookies – which usually last for a few hours. Permanent cookies facilitate data aggregation by different websites, worsening information overload. Most cookies that enable websites' useful functions, such as a shopping cart, are session cookies.[125]

Regulations that treat permanent cookies and session cookies differently better respond to websites' incentives. Permanent cookies involve more profit for websites and advertisers, as they facilitate assembling user profiles. Regulations that treat all cookies equally reduce the benefits of diversification because they incentivize websites to install the most profitable cookies, which are also the most invasive.[126] It's unlikely that websites under a regulation that treats all cookies equally would decide to install only the least invasive and least profitable alternatives. On the other hand, if less privacy-invasive cookies could be installed more easily than invasive ones, websites would have reasons to diversify, leading to enhanced privacy.

Differentiation responds to consent fatigue. Under regulations that don't differentiate between types of cookies, people entering a website are asked to agree to its use of cookies (or notified that it uses them). It's costly for visitors to know, however, the proportion to which those are session or permanent cookies, categories to which they could react differently. Perceived privacy risk, as well as annoyance during browsing, is determined by each banner. Regulations requiring agreement for permanent cookies, thus providing incentives to use more session cookies, would reduce the number of times people receive a banner.[127] The shift would make the presence of banners more informative, giving people a better sense of what kind of privacy loss a banner means. Fewer and more meaningful banners would make people less prone to automatically accepting them.

One should develop skepticism about whether websites don't extract data from session cookies stored after the tracking device expires. One study found websites cloak third-party analytics as regular subdomains of their own websites, finding that "27 out of 90 highly sensitive web services (e.g., banks) that we analyzed expose session cookies to the web analytics services."[128] That said, a tracking device that expires with some information being kept is better than a tracking device that doesn't expire. It makes the aggregation not built-in but rather dependent on another layer of processing that will have some cost and a success rate dependent on each company's data infrastructure.

The European opt-in problem was caused by trusting choice design to entities with incentives to undermine our choices and by focusing on technical specifications over function. Relying on web browsers instead of a vast array of websites to design choices and considering degrees of privacy losses would improve regulatory outcomes. This approach would facilitate enforcement and avoid overinclusion.

Tracking in the Information Economy

Online tracking regulations in Europe, which faced implementation difficulties, and the Privacy Order in the US, which left the main issue unresolved, shared a limitation. They both overlooked the role of power in the information economy, which enables exploitation and undermines consent.

Opt-in tracking regulations, although sometimes considered to be tough on companies, aren't. The only precedent of a real opt-in system for cookies (the Dutch regulation) was such a resounding failure that it backtracked to implicit consent. The EU now incorporated the explicit consent system that failed in the Netherlands, with narrow differences such as prohibiting cookie walls, without evidence of success. ISP tracking shows the extent to which people are unable to accurately estimate how much companies can infer about them, undermining efforts to overcome consent provisions' problems. Together, these stories illustrate that policymakers must consider power dynamics, manifested in manipulative choice architecture and exploitation of biases such as information overload, when designing privacy laws for the information economy.

Other best practices go down the wrong path when legislators focus on asymmetric information, such as turning consent requirements into informed consent requirements. Notices could give detailed information about data practices, with long forms for people to complete. For example, they could do so whenever people enter a website, specifying the cookies they prefer to allow, their purpose, for how long they prefer to allow them, and for the use of whom. Such a requirement is similar to what the CCPA mandates, requiring websites to inform visitors about their cookies, their source, their purposes, and whom they share the data with.[129] Similarly, to comply with the regulations governing cookies under the GDPR, websites must provide accurate and specific information about the data each cookie

tracks and its purpose – and must do so in clear and plain language.[130] This path offers limited benefit because people have to decide whether to agree to too many options in a context of uncertainty and information overload. It ignores manipulation mechanisms that nudge us into disadvantageous choices and dark patterns that, exploiting biases through innovative deception methods, turn a nudge into a push.

Treating privacy policies as standard form contracts provides minimal improvements. Unequal information and take-it-or-leave it agreements limit the scope of allowed consent in standard form contracts.[131] But these are only a subset of privacy's consent provisions problems. Standard form contracts can be improved with defaults,[132] doctrines such as unconscionability,[133] and clearer drafting and disclosures for agreement to be specific.[134] But these best efforts are insufficient for personal data in the information economy because their problem is systemic – not specific to some bilateral commercial transactions. The application of solutions developed for these contracts to privacy rests on mistaken constructions about the underlying interactions.

I proposed here how to design notices in light of information overload, which would improve current best practices of detailed notices in plain language and contracts-based approaches. These enhanced privacy notices face a significant hurdle too. Most people can't read long disclosures; notices need to be short.[135] Even if notices clarified typical inferences, they wouldn't eliminate information overload because they can't capture all potential risks without becoming incomprehensible. To be complete, enhanced notices would need to address how information can produce a wide array of data harms.[136] Since companies often learn about AI inferences later, and they often share data with third parties, it's even difficult for them to anticipate how aggregation will occur and the consequences it can have down the line. While difficult in general, doing so in a short banner on a browser is impossible. Enhanced notices would be an improvement over existing ones, but they wouldn't address all hurdles stemming from individual consent provisions. Because it's impossible to understand in advance how informative each data point is, there's no consent regime that can overcome the problem.

I also proposed how to improve tracking regulations based on lessons from behavioral science. While an improvement, these enhanced regulations would also leave unsolved the root problem of entities with power unilaterally producing harm for profit. Even if an improved notice free of dark patterns appeared when people opened their browser, that wouldn't be enough. Most people mechanically accept data collection to access a service because they can't protect themselves.[137] It's unlikely they'll gain the ability to consider different forms of tracking and their consequences every time they open their browser. Agreement to improved tracking notices will continue to lack as a guarantee of protection.

The law must, instead, regulate companies that are in a position to exploit their users through their personal information because they know their users' vulnerabilities.[138] It should do so in a way that incentivizes companies to care for the interests of

their users. They're the ones who hold the power and information to determine how doing so is possible in each situation. These stories' central takeaway is that even the best versions of disclosure regimes and consent provisions are insufficient to address privacy harms created and exacerbated by manipulative design and exploitative surveillance.

* * *

The stories of Brussels trying to regulate cookies and Washington trying to regulate ISPs' surveillance illustrate a systemic problem. They show that the problem hasn't been the modes of consent. The problem has been the object of consent.

People can't make perfectly rational privacy choices because they aren't equipped to anticipate the consequences of their inferred data. This fact is relevant for any policy that attempts to protect people's privacy in relation to corporations. Opt-in consent requirements and plain language requirements miss the information overload mark just as applying contract law principles does.

Ultimately, moving privacy consent from an opt-out to an opt-in model, establishing contract law mechanisms, and reinforcing privacy notices are desirable improvements. The issue is that these improvements are marginal. They don't solve the root problem of power and harm because they rely on individual choices. They fall into the trap of believing that the problem with privacy is that it's not close enough to a market. As a consequence, they work as palliative solutions that are helpful only as long as they don't distract from meaningful ones. Cookie banners are a reminder that we don't have real choices in the information economy; they're not the reason why we don't.

These examples tie to the myths of rationality and apathy. The law fails because it assumes that people willingly trade their personal information and are relatively indifferent to those privacy losses (apathy), and they do so after understanding and considering all costs and benefits (rationality). The efforts of the EU cookie regulation and the FCC were influenced by these myths, creating an unstable policy foundation that led to their unhelpfulness.

Because exploitation, such as through manipulative design, is a prime feature of the digital ecosystem, individual consent is a false promise. Laws for the information economy can and should engage in efforts to prohibit specific forms of manipulation, but they can't eliminate it because new forms will show up. The chapters that follow explore what the law should do instead.[139] A better way forward is through laws that establish power-aware accountability mechanisms. This approach would increase people's wellbeing while maintaining profitable business practices.

5

Traditionalist Data Protection Rules

Victims of data harms don't get the affordances that victims of other harms get.

During the 1970s, Ford knowingly endangered the lives of Pinto car owners by ignoring a defect in the car's gas tank. Ford dismissed preventive safety measures because a cost-benefit analysis determined that these measures would be costlier than the lawsuits the company would encounter.[1] After one Pinto owner was severely injured when his car burst into flames, Ford had to pay $125 million in punitive damages – the equivalent of $400 million today.[2]

The law doesn't allow companies to ask consumers: "do you accept the risk that your car engine may combust?" It just requires companies to sell safe engines. Similarly, the law doesn't allow amusement parks to build rollercoasters with varying safety levels to let consumers choose whether to go on an expensive safe ride or a cheap unsafe one. It just mandates amusement parks to build in safety measures. Risk-prevention standards are set by governments and industry, both of which have better access to information and resources to evaluate risks than the average person. These standards are limits on consumer choice in the sense that, in our range of options, we can't choose to buy a car without a seatbelt or to buy drugs that will poison us. It's not left up to us to choose whether to use a dangerous product and hope for the best.

The law, however, has so far let us boundlessly choose how much risk to assume when it comes to our data in the digital economy. Processing people's personal data, by the nature of the activity, creates risks for them. Some of these risks are inevitable, but most of them can be reduced. Because corporations that process personal data create risks for others, substantive limits and outcome-connected duties to reduce risk independently of individual agreements and mandated procedures would be a legal response that treats it equivalently to other risk-producing activities.

The several-billion-dollars question is how laws can curb those risks while preserving the information economy. To depart from a free market system, data protection law became too focused on individual control and individual rights to exert control. It also became too focused on procedure. Modern data protection law has useful elements aimed at reducing risk, such as data minimization and privacy by design. Yet they're few and not well enforced.

A better approach is to combine substantive prohibitions aimed at reducing risk and liability when risk materializes. Data protection law must embrace corporate accountability for data practices' consequences, rather than for rule-compliance, as the cornerstone of protection. Without this change, reforms will fall short of protecting people from data harms. Ideally, data protection law would abandon consent provisions, make data protection rights independent of individual control, shift from procedural mandates into substantive ones, and expand its systemic provisions. As the next chapters explore, it also needs civil liability.[3]

Ford's eagerness to ignore the potential for harm to thousands of their customers because it was cheaper to let them be harmed than to prevent it resembles the information economy's lack of, and need for, more meaningful accountability. Ultimately, Ford was held accountable. But the data giants that make cost-benefit analyses about their profits and our harms still aren't.

A RULES FOR CONTROL

Data giants can freely behave like Ford did with its Pinto car.

In 2021, the congressional testimony of Frances Haugen, a Facebook (now Meta) employee turned whistle-blower, described how Meta sacrifices user safety and well-being to further its financial interests. Haugen's words were powerful: "I'm here today because I believe Facebook's products harm children, stoke division, and weaken our democracy. The company's leadership knows how to make Facebook and Instagram safer, but won't make the necessary changes because they have put their astronomical profits before people."[4] She explained that Meta is well aware that its platforms exacerbate body-image issues in teenage girls, facilitate the spread of misinformation and hate speech, and even enable human trafficking and armed violence, but has done little to fix it.

Consent in Individual Control

The EU responded to potentially harmful data practices like Meta's by focusing on the right to data protection, which protects people's personal data.[5] The EU's data protection system influenced jurisdictions worldwide, such as Argentina, California, Canada, Japan, Israel, and New Zealand.[6] Data protection may be the most internationally influential aspect of EU law.[7]

Data protection law is an effort to move away from a market-based, notice-and-choice ecosystem into a regulated one.[8] But data protection systems are strongly influenced by the preexisting market-based system.[9] After all, they're based on the FIPs.[10]

Most jurisdictions around the world implemented the FIPs, with their principle of *lawful, fair, and transparent processing*, through a pivotal provision in their data protection statutes that requires individual consent for processing data. For example, consent is the primary legitimizing basis for processing data in Andorra, Argentina,

Brazil, Canada, Faroe Islands, Guernsey, Japan, Korea, Mexico, Singapore, and Uruguay.[11] Consent is key to data protection law everywhere, particularly outside of Europe.[12] The US, similarly, historically focused on (consent-based) opt-in and opt-out rights to protect privacy.[13] The American system relies on a contracts-based regime that aims to produce a market for personal information.[14] Its sector-specific federal privacy laws and state privacy laws are similarly based on consent.[15]

In the GDPR, on the other hand, data practices are lawful if undertaken based on any of six grounds: performance of a contract, protection of vital interests, compliance with a legal obligation, public interest, legitimate interests, and consent.[16] Each of these grounds is only sometimes applicable. Performance of a contract is appropriate when processing to provide an estimate of the costs of a service, but it's narrow and it might be an inappropriate ground to develop AI.[17] The vital interest justification applies in exceptional cases such as emergency medical diagnoses of unconscious patients. Compliance with a legal obligation applies when a legal obligation mandates processing someone's data.[18] The public interest justification is for public entities under a specific set of conditions.[19] The legitimate interest justification is broader; it applies when corporations "use data in ways that people would reasonably expect and that have a minimal privacy impact."[20] Ultimately, although processing can be lawful absent consent, consent is a widespread ground for private sector data practices in Europe.[21]

The GDPR may be the data protection legislation in the world that places the least weight on consent.[22] But that's a low bar. People's agreement is key to the GDPR beyond consent as a legitimizing basis.[23] By a simple count, the GDPR has seventy-two references to consent. The Charter of Fundamental Rights of the EU, which establishes data protection as a fundamental right, indicates that data must be processed "on the basis of the consent of the person concerned or some other legitimate basis laid down by law."[24] Agreement broadly considered, as detailed below, permeates mechanisms of individual control.

The permissive attitude toward individual agreements that these laws give data practices in the presence of pervasive harms is exceptional in comparison with other regulated areas. The fact that people can be forced into tradeoffs doesn't imply that those tradeoffs are inevitable or fair.[25] Imagine legislators replaced food safety laws with clear notices. Some people would tolerate hazards, risking consuming contaminated food for lower prices. The mere fact that an agreement would exist doesn't mean laws should allow the transaction.[26] Laws protecting personal data in the information economy should make protections independent of agreements.

Where consent is not at the forefront, control is, due to the FIPs. Both American-style privacy law and European-style data protection law are based on the FIPs.[27] The GDPR, like its American counterparts, aims to protect people while ensuring free movement of data by giving each individual control over their personal information.[28] The individual control effort is central in EU-inspired data protection laws in other parts of the world.[29] What sets the American and European approaches

apart is that American privacy law embraces consent explicitly through opt-in/opt-out efforts, while European data protection law embraces it implicitly by focusing on individual control as a protection mechanism.[30]

Building on the FIPs, laws extend consent problems beyond notice-and-choice and consent as a legitimizing basis. They extend them into the mechanisms that are supposed to pull our data away from problems such as those outlined in the last two chapters. Emphasizing individual control reinforces the most troubling aspects of the preregulatory, free-market system:[31] the focus on individual binary choices, the rationality and apathy myths, and the consent illusion.

The narrative that values increasing individual control over personal information emerges from a focus on privacy self-management.[32] Politicians using control as a narrative to deregulate isn't unique to privacy. Politicians who oppose minimum wage, for example, believe that people should have the right to consent to less pay, so employees and their employers should freely determine wages. Those who oppose price controls on monopolies and oligopolies usually say that we should instead reinforce consumers' control, which consumers can exercise by choosing whether to use the service. Individual personal information control is a similar trap.

Data protection rights are the most significant departure from notice-and-choice since 1973. Systems of data rights across the globe, however, have control (and therefore, indirectly, consent) embedded in those rights. Policymakers know consent is a problem for the notice and choice system. The Australian authority, for example, acknowledged that "overreliance on consent shifts the burden to individuals to critically analyse and decide whether they should disclose their personal information in return for a service or benefit."[33] But they underestimate the importance of the consent illusion for the effectiveness of data rights. The problem's extension to data rights is highly consequential for determining how one can and should reform protections.

It's Not Right, But It's OK

The EU, and countries that modeled their data protection law after the EU, depart from notice and choice by granting data rights, such as the right to rectification and the right to object. Recently, US states have also taken a step toward this approach by including data rights in comprehensive privacy laws that started in California and followed in Colorado, Connecticut, Utah, and Virginia.[34]

Although this second wave of privacy laws provide people with the ability to correct, access, and delete information about themselves, they subscribe to a long history of privacy laws that prioritize, as Ari Waldman puts it, "atomistic personal autonomy and choice."[35] Further, besides prioritizing individual control, traditionalist protection mechanisms depend on it. Their reliance on the very notion of control they reinforce is why some of the most robust data protection regimes don't solve informational exploitation.

Data rights, like opt-ins and opt-outs, rely on users exercising them. The problem with this regulatory choice is that it turns data rights into mechanisms of individual control.[36] And individual control mechanisms put the onus on people.[37] Data rights end up affording possibilities to exert individual options. But if individuals don't or can't exercise these options, the rights are of little use. Because data rights place the onus on people, they place people in a fight against corporate power that they can't win.[38]

Consider the key data rights of the GDPR, one of the strongest data protection legislations in the world. The GDPR grants a series of individual rights that come from the prior Data Protection Directive.[39] These rights are the right to information, rectification, erasure, object, and restrict processing. Buying into the myth of rational, informed users, they replicate the problems of the illusion of consent.

The right to information grants people the ability to know what personal information about them is held by a corporation. Referred to as "the right to know" in the US, it's people's right to ask a company what data it has about them.[40] People can ask for specific information such as a confirmation of ongoing processing, what personal data are being used, and details of their processing, including risks and safeguards.[41] The right to know is of low cost for companies and allows people to access information about themselves. The issue is that truly informing people is impossible. People can't always ascertain which corporations are processing their data to exercise their right to information toward them.[42] Further, providing real people with bounded rationality and limited power to process information with more information isn't the same as helping them know.[43] In reality, people can exercise a right to receive information from some companies but they can't really know what happens with their data. Relying on it, as other data rights do, can be counterproductive.[44]

If you ever downloaded your Facebook information, you probably didn't find it very useful beyond an anecdote or two. This option is granted by the right to access your records. The rights to access and to know are treated together in most jurisdictions but bifurcated in the GDPR.[45] The right to access, used for obtaining direct access to specific records, exists around the world.[46] Having the option to access records is better than lacking it. But these records tell us little about all-important forms of data processing and their implications. As technology journalist Kashmir Hill explains, "most of these companies are just showing you the data they used to make decisions about you, not how they analyzed that data or what their decision was."[47] The right also leaves out inferences in most jurisdictions, where they aren't considered personal information.[48] And you can request information from one or two data giants, but requesting access from the thousands of corporations that have your data (some of which you never heard of) to have a semblance of a complete picture is impossible.

Another data right is the right to rectification (or to correction).[49] This right gives one the ability to rectify errors in one's records.[50] Those who invoke it can request

a corporation to correct inaccuracies or supplement information to correct wrong outputs.[51] The right to rectification requires each individual to be on top of records they don't hold. Reviewing records and submitting corrections in such a way takes an unfathomable amount of time and skill. Each person would have to know that the processing is happening, who's doing it, and that the data are inaccurate or outdated. The right to know doesn't do this for them. Making this issue worse, the data that corporations hold are in constant mutation as new data are collected and inferred. One's efforts can't scale to the number of corporations collecting and using one's personal data.[52]

The right to object (also known as right to opposition or restriction) can be used to stop the processing of someone's personal data.[53] The right to object and the right to restriction, while treated together in most jurisdictions, are bifurcated in the GDPR, serving an equivalent function depending on which was the legitimizing basis.[54] The right is a close cousin of the opt-out rights that the US historically focused on, and that the tracking regulations discussed in the last chapter tried to move past by evolving into an opt-in.[55] However, to exercise it, people must become aware of the data practice, such as through the right to know. The right to object burdens people with learning what processing is taking place, what its purposes are, and raising the applicable objections.[56] And exercising objections may not suffice. Under the GDPR, if a corporation establishes a legitimate interest in the information and shows it wouldn't interfere with other rights, it can override an objection.

The right to erasure (also known as right to deletion) allows people to have their data deleted from records.[57] The right, which extends beyond the EU to places such as Brazil and California, allows people to request deletion when a data practice didn't comply with the law or the data are no longer necessary for the purposes they were collected for.[58] Under the GDPR, erasure enables people to request the deletion of any of their personal data, subject to balancing.[59] The right to erasure is all about people monitoring the flow of their own data and taking individual action to have it removed.[60] The right requires people to find which entities they should approach to erase any ill-gotten information about them. People are sometimes even unaware of which entities have data about them, such as with data brokers. Mass transmission of data to third parties make it impossible to track down every data point and to delete the data.

Control-dependence also extends the consent illusion to newer and more controversial data rights. Consider, for example, the right to data portability, which primarily applies when the legitimizing basis was consent.[61] People can request for a copy of their personal data to be transmitted to another corporation in a structured, commonly used, and machine-readable format.[62] The right is convenient for people who want to change service providers and keep information such as their phone number.[63] The right to data portability is a new, more robust permutation of the right to access. And it's subject to equivalent limitations: it's hard to exercise, it relies on people actively exercising it, and, in most jurisdictions, it doesn't cover inferred data because they're technically not collected data.[64] Data portability may help level

the playing field for competition in many industries, such as telecom providers. But it won't increase competition for privacy because there's no functioning market for privacy in which to improve competition. Because, as discussed in a prior chapter, corporations don't internalize the consequences of the risks they create, they lack incentives to afford protection beyond rule-compliance.[65] Instead, corporations are incentivized to maximize data collection and the benefits they can extract. Relying on individual data portability rights to address the information economy's privacy harm is an example of the market view of privacy.

There's overall a productive, control-independent rationale behind the individual data rights system. Their exercise can provide insight into otherwise opaque data practices, improving transparency.[66] However, this only works if people actively exercise them. This rationale evades the problems of control-prioritization, but not those of control-dependence.

Data rights appear to empower people. But, in practice, in the information economy, they're options that people lack time and knowledge to use frequently and the power to use effectively.[67] The law on the books says that people can choose to exercise those rights to vindicate their privacy. But, in practice, they rarely have the opportunity to do so. These rights are helpful in individual-to-individual interactions – the types of interactions that escape the consent illusion.[68] For example, if you want to access your medical record from your doctor, the right to information or the right to access is helpful. If someone shared a picture of you without your consent, the right to erase is of fundamental importance. If you know your bank has mistaken financial information about you, the right to correction is convenient. If you want to switch cell phone carriers, the right to data portability makes that easier for you. But individual data rights can't protect people in today's multi-party, inferential information economy because they aren't equipped to operate in scalable, ever-present, and opaque corporate data practices.[69]

Consent Burdens

Hundreds of years ago, the contract law principle that a buyer of goods is responsible for ascertaining their quality, called *caveat emptor*, was introduced. In the information economy, *caveat emptor* expands to data because we're treated as buyers of digital products and our data are treated as what's given in exchange.[70] Each of us must decide what information to allow each company to collect and later find out the consequences of our choice. Individual data rights reinforce those choices. Data rights that people can rarely use protect individual interests they can't act on.

Regulators are used to considering "regulatory burdens": the costs regulations place on corporations, including for privacy and data protection. They rarely consider the costs carried by those whom regulations are supposed to protect. Administrative burdens are the converse – the workload, time, and effort people must put in to benefit from regulations. Administrative burdens can take many forms, such as

filling out paperwork, completing forms, submitting reports, or complying with procedures. These burdens become a significant challenge for people when they're time-consuming or difficult to manage. Being pulled into taxing administrative processes to access protection has a cumulative burden on people.[71] This cumulative burden can lead people to disengage and be accused of apathy. Data protection creates administrative burdens that Ella Corren calls "consent burdens."[72]

The amount of consent burden that a regime places on people helps determine whether agreements are successful in governing its interactions: when the costs of agreeing are high for people, consent-focused rules, including control mechanisms, don't work well.[73] Laws, in practice, put responsibility on individuals, who must add information from multiple parties to inform themselves, estimate the risks and benefits, make rational long-term decisions, and bear the consequences.[74] Laws' traditional attitude toward control has ignored the problems with that model – that control requirements disproportionately and counterproductively put regulations' weight on people's shoulders.

Consent burdens come in two forms. Before-the-fact burdens arise from information asymmetry and bounded rationality.[75] After-the-fact burdens arise from constraining rights and remedies by illusory agreements.[76] Before-the-fact burdens are validated by the myth of rationality. After-the-fact burdens are validated by the myth of apathy. For example, privacy opt-in systems aim to lower the burden on people from opting out of surveillance.[77] But because of privacy's moral hazard, they burden people with after-the-fact monitoring. If people opt in, they have to check that the data are being used properly. If people don't opt in, they have to monitor that their information isn't being collected. As anyone trying to manage their cookies noticed, this monitoring is effectively impossible.[78]

Data rights, like consent provisions, are burdensome. People would have to exercise their data rights toward thousands of corporations every day for them to be effective. Even if someone exercised these rights against each corporation that has their data, the data each corporation have change by the second. Expecting people to keep up with this task is as illusory as expecting them to examine and consent to thousands of data practices day by day.

Control-dependence empties data rights. There's tension in attempting to empower individuals by granting control-dependent rights in a digital environment of pervasive exploitation, made possible precisely because they're disempowered. Manipulation, for example, makes empowerment through rights illusory.[79] Through design, corporations can increase consent burdens to hollow out data rights. For example, people typically lack the skills, tools, or time required to exercise the rights to rectification and to object.[80] As a consequence, we end up with more options we can't use. Laws that are supposed to overcome the consent-based approach to the information economy instead make people's decisions more numerous and complicated for them to exert, while relying on them making those decisions for self-protection. Data rights, ultimately, also rely on the contracts worldview.

In the worst-case scenario, individual data rights can end up facilitating, rather than preventing, abuse of corporate power.[81] Relying on people's exercise of data rights can lead to the unfair blaming of individuals when they fail to exercise their rights. Blaming people for not exercising their rights elides the fact that exercising them is challenging. When the privacy myths permeate enforcement authorities, they stifle improvements authorities could make by looking beyond individual control.[82] Authorities, particularly outside the EU, occasionally rely on the myth of rationality, assuming people can enforce these individual rights – just as others assume people can evaluate each privacy agreement. When people don't invoke rights that they lack the tools to use, opinion-leaders often conclude that they must not care about their privacy.[83] In line with the myth of apathy, rather than taking infrequent use of data rights as evidence that people need additional protection, it's misconstrued as evidence that they could do with less.

In theory, the law aims to halt socially harmful practices while allowing for socially valuable ones by passing data practices through the strainer of individual autonomy. In practice, the law legitimizes exploitation by covering harmful activities with a veneer of legitimacy because they were supported by supposed individual autonomy.[84] Systems of individual data rights leave out common interests that are crucial in light of inferential harms. Traditionalist policies, in doing so, cling to undefined ideas of autonomy and gloss over the incoherent outcomes of pursuing them.[85] Relational data, which allow others to make individual choices on our behalf, exemplify the incoherence.[86]

The logic of individual control, extending *caveat emptor* to data, is that people must oversee and, where necessary, intervene in their data's processing. This logic transforms people's *control over* processing into *responsibility over* (self-managing) processing – and, therefore, their protection.[87] Shifting responsibility toward people is often defended under the premise of empowering them. It produces the opposite: it leaves them vulnerable, providing them with tools that are difficult for them to protect themselves with.[88] In other administrative systems, such as welfare programs, imposing costs and inconveniences on those protected when trying to access the system has been shown to undermine their usefulness.[89] Regardless of the regulatory burden on corporations in the information economy, data protection laws' consent burden on people is excessively high.

***

The narrative that highlights the importance of individual control enables and obscures harmful processing, which is unforeseen and mechanically agreed upon by people.[90] Individual control is embedded in individual data rights. The limits of individual data rights are the limits of the law's traditionalist approach, which focuses on individual choices while ignoring harmful social dynamics. Harms in the information economy aren't just to individuals. They're also to groups and to

society.[91] Because individual control is disconnected from avoiding data harms, relying on individual choices, including choices to exercise individual rights, fails to protect people in an environment of moral hazard and unchecked power.

The rights themselves aren't the problem. Within the information economy, they can be useful when used by organizations who combine ability to pool common interests, time, resources, and knowledge of specific problems.[92] The problem is relying for protection on rights that are built on individual control because doing so distracts from addressing informational exploitation. Although individual data rights make people negligibly better off, relying on them to regulate the information economy is detrimental.[93] Data rights don't need to be so individualized, departing from the human rights tradition, which recognizes the interests of groups.[94] Data rights would improve if they moved away from the narrative of bilateral contractual relations between one individual and one corporation. Protections that don't depend on control and apply at-scale provide more suitable protection for the reality we live in.

B THE PROCEDURAL APPROACH AND ITS LIMITS

While Frances Haugen's testimony happened, Meta published a new policy stating the company aims to "serve everyone; promote economic opportunity; build connection and community; keep people safe and protect privacy."[95] The company's rhetoric has privacy and human rights at the forefront: it vows to conduct human rights due diligence and disclosure, remedy human rights impacts, protect human rights defenders, and "promote a climate of respect and awareness for human rights."[96]

Meta's incongruity between rhetoric and outcomes extends to the company's role in developing the metaverse. The metaverse collects more personal information than ever before, while potentially being more addictive. Meta said it intends to involve human rights and civil rights groups "from the start" in building the metaverse. It said it's looking to minimize "the amount of data that's used, build technology to enable privacy-protective data uses, and give people transparency and control over their data."[97] The company's track record and the reality on the ground raise doubt about the strength of these commitments. If we have anything to learn from Frances Haugen, it's that Meta seems to be performing accountability, making promises of increased privacy with one hand while undermining privacy, and human rights broadly, with the other.[98] All while respecting, ostensibly, data protection law's procedural safeguards.

Data Protection's Procedural Turn

Data protection laws consist of default and mandatory rules. People can agree to waive default rules, while mandatory rules are consent-independent. In most publicly enforced regulations, defaults are uncommon: most rules are mandatory, not allowing parties to contract around them. By contrast, most contract law rules are

defaults, where the law sets what applies unless parties agree otherwise. Mandatory rules for data need to be more substantive and less procedural.

Parts of data protection laws set consent-independent, mandatory rules, establishing what companies can't do after acquiring agreement. Under the GDPR, for example, companies can't seek individual consent to avoid having privacy by design or to waive the duty to have a data protection officer, when applicable.[99] These rules apply independently of agreements between people and companies, aiming to lead to data practices that companies believe would minimize risk. They exist in opposition to default rules, such as the prohibition of third-party sharing, which people can override by agreement. Consent-independent rules are key for personal data. The failures of privacy notices and the illusion of consent extend to beneficial legislative defaults, which corporations can easily nudge people away from.[100] Deciding what's allowed at the legislative level frees people from needing to self-manage privacy choices. Substantive, consent-independent rules avoid the practical and moral limits of relying on individual choices in the information economy. However, most of these benefits are lost in procedural rules.

Because privacy harm is difficult to identify in advance, legislators drafting data protection rules determine wrongness through procedure. They identify wrongness in a way dissociated from harms, equating it with prohibited corporate conduct. The main question isn't whether a data practice is harmful, but rather whether someone used personal information in a way that's forbidden – usually, without a legitimizing basis, such as agreement.

Focusing on procedure means insufficiently distinguishing harmful data practices. Even before the inference revolution, Woodrow Hartzog worried that laws "quickly turn FIPs-based privacy rules into formalistic exercises designed to extract consent and use the gift of control to saddle the data subject with the risk of loss for data misuse."[101] Fred Cate similarly pointed out that "data protection, with its reliance on narrow, procedural FIPs, is not working … privacy protection is not enhanced, individuals and businesses pay the cost of bureaucratic laws."[102] The FIPs focus on procedure, not on substantive protections, because they aim to facilitate data collection, not restrain it.[103]

Procedural rules provide legal certainty to the entities they regulate – a benefit over legal standards. Corporations usually lobby for procedural rules, which are specific and predictable in their application, as opposed to flexible standards. The success of this certainty-seeking dynamic can be attributed to how the FIPs have historically been applied.[104]

This certainty comes at a high cost. Procedural rules work best when we know what behaviors are harmful. When we don't, for example because conditions change rapidly as they do in the information economy, procedural rules fail to capture social values.[105] The procedure-focused way that data protection has been applied undermines the benefits that those provisions could capture by moving past individual control. Data protection rules that determine wrongness through procedure have

two limitations: including nonharmful activities and excluding harmful activities. If the aim is to prevent harm, then procedural rules have made laws simultaneously over- and underinclusive, overregulating and underprotecting.[106]

Underprotection

Early criticisms of the GDPR argued that it creates a comprehensive but complicated regulatory model that's unable to achieve what it aspires to: protect people's rights.[107] Every regulatory area underprotects to some extent because legislators can't anticipate all possible negative outcomes. Personal data's underprotection is a problem of degree because of the large number and magnitude of data harms that laws leave out. And it's a problem of kind due to its pairing with overregulation.

Procedural protections, although consent-independent, can't anticipate, and much less prevent, most negative outcomes for data. So they leave risks and harms out. US federal privacy law suffers a version of the underinclusion problem because it focuses on which actor processes information, leaving out similar data practices with similar risks from other actors.[108]

Regulating a type of technology rather than a data practice is another way to underinclude.[109] European cookies regulations discussed in the last chapter had this problem, as they meant to regulate tracking but left out other tracking methods.[110] One of those is tracking through browser headers, as Paloma Gaos sued Google for.[111] Procedural rules don't capture harms from technologies that keep changing because technological change introduces new risky activities that legislators didn't predict.[112] The US Video Privacy Protection Act, for example, is underinclusive because it regulates a technology rather than the conduct it enables; it didn't anticipate the ways people watch movies today.[113]

Most data harms come from the abuse of an otherwise permitted activity, not from engaging in a prohibited activity. As the examples mentioned throughout this book illustrate, data abuses happen daily within the boundaries of what procedural rules allow. Abuses inevitably fall between the cracks when laws' mandatory aspects are procedural. This dynamic replicates preregulatory scenarios where corporations can extract data for profit in ways that harm people's privacy, finances, equality, reputation, and their bodies.

The procedural-rule focus turns data protection compliance into box-ticking exercises.[114] When the tech industry can interpret and implement the law by way of checklists, records, and documentation (like privacy impact assessments), companies find ways to undermine the law in practice. "Check-the-box" compliance ends up being a performative activity that allows companies to evade accountability.[115] This on the ground reality shows where the law went wrong. Obligations to fill forms shift the focus away from what matters, reducing risks of harm, because preventing harm in data practices requires thoughtfulness.

Procedural rules result in victims of data harms fading into the background – something that regulations that focus on outcomes can avoid. Victims can complain to their data protection authority about having suffered harm. But if the authority investigates, and companies did comply with the law by obtaining agreement, victims often have no recourse even if they were harmed.[116] Besides, whether and how authorities investigate and sanction is their prerogative. And, in many jurisdictions, they must do so with delays and shortcomings produced by limited resources.[117]

Overregulation

One of the first relevant data protection cases illustrates its overregulation problem.[118] Over a decade before the GDPR, a catechist at a Swedish parish called Bodil Lindqvist built a website that provided community updates and helped coordinate meetings. The website had some information about parish members, such as their hobbies, and let parishioners know that the priest's availability would be limited as he had injured his foot. This would come to be a mistake. When the website came to the attention of the Swedish authority, Ms. Lindqvist learned that she breached the law by processing people's information without their consent.[119] Worse, she had processed health data: a broken foot. For the oversight, she faced three criminal charges and a fine.[120]

Scholars and courts often remember this case as a success, as it acknowledged the right to data protection.[121] But we can forget that the case had a hefty price – someone of modest means who, without profiting from others' data and vested with good intentions of communicating with her community, faced criminal sanctions that many deem disproportionate.[122] Lindqvist's case illustrates how procedural provisions overregulate. The reason the case was overinclusive is that, like many others, it was dissociated from harmful outcomes.

Overregulation extends to the information economy. As AI inferences take over varied aspects of our daily lives, for some, data protection law becomes "the law of everything."[123] Regulating activities without victims is a common consequence of moving an issue from harm-focused mechanisms into procedural rules. While the problem of overinclusion exists outside data protection, its magnitude makes it a concern – particularly when paired with underprotection. Procedural rules for everything are the antithesis of risk reduction.

The GDPR has been accused of imposing compliance costs that large, US-based companies can handle more easily.[124] These costs, critics argue, lead the GDPR to reduce competition by increasing entry barriers for new players and cementing existing monopolies.[125] Empirical studies suggest that the GDPR reduced vendor competition by 17 percent and increased Google and Facebook's market share by 6 percent.[126] Accusations don't stop there. Less persuasively, others accuse data protection of interfering with journalism and free speech,[127] access to information,[128] and commerce generally.[129]

Independently of their individual merit, these wide-ranging critiques share a common concern. They aren't objections to regulating personal information generally. These critiques are concerned with overregulation stemming from a procedural focus. For example, consent provisions, while least useful for people, have the largest disparate effect for large and small players: acquiring valid individual agreements is costly, but economics of scale and scope reduce its cost for large players.[130]

Overregulation doesn't have an easy fix. It's a consequence of privacy's procedural nature because harmless or socially valuable uses of data are difficult for legislators to anticipate. Procedural restrictions for data increase compliance costs and prevent valuable data uses in a context where technological changes constantly change levels of risk.[131] For example, it's a mistake to treat all targeted advertising as quantities of a single data practice; some data practices for targeted ads harm users and some don't.[132] Rather than treating all data practices the same, one needs to distinguish among them.

Laws often address data's valuable uses with exceptions to procedural rules, such as those for medical research, journalistic purposes, and historical records. Because valuable uses covered by the exceptions are unpredictable, these exceptions are necessarily indeterminate.[133] So either exceptions get proceduralized, thus losing their intended purpose of capturing unpredicted valuable uses, or they introduce indeterminacy in a system of procedural rules, defeating the predictability-increasing purpose of having it.[134] Moreover, countless harmless uses that happen day to day, such as that of Lindqvist, fall outside the valuable uses and public good exceptions.

The procedure-and-exception approach is a consequence of portraying needed protections as protections for each individual person. Relational data and group privacy interests show that "exceptions" to individual privacy when confronted with group interests, such as health and speech, misrepresent the underlying dynamics. The approach perpetuates the reductionist view that all privacy is individual and its dichotomous implication that laws can either make individuals choose to give it away or have their individual autonomy overridden. Things aren't getting easier. Since the Lindqvist case, AI reduced the costs of surveillance and allowed for inferring new personal data, introducing further group harms and collective interests.

The overregulation problem of addressing situations with no harm is also present in US privacy law. For example, the Telephone Consumer Protection Act, which aims to eliminate those robocalls that everyone dislikes, focuses on regulating a technology (auto-dialers) rather than a social practice (spam calls). As a consequence, it confused the legal status of non-spam automatic replies, inhibited businesses' ability to contact their existing customers, and slowed down the processing of do-not-call requests.[135]

In the meantime, we continue to receive robocalls and spam texts. Laws like the US Telephone Consumer Protection Act, in other words, also underprotect.

An Example: The Right to Be Forgotten

Protection and procedure compliance don't correlate. Companies who must abide with data protection procedures perceive them as robust because they must spend significant amounts of time and resources in compliance.[136] For example, corporations complying with the GDPR must produce detailed, and allegedly costly, documentation of their data practices and rule compliance.[137] But those whom the law aims to protect experience it as merely symbolic – while they're harmed.[138] High compliance costs combined with minimal protection lead to a situation in which no one wins.

An example of simultaneous concerns of overregulation and underprotection is the controversy surrounding the right to be forgotten. Before the GDPR, the *Google Spain* case recognized the right to delisting, ruling that search engines must delist content that's "inadequate, irrelevant or no longer relevant, or excessive."[139] The right provides individuals the option to remove information from search engine results.[140] If an individual notices a disagreeable use of their data, they can request a search engine to remove the data from search results regardless of whether it's harmful.[141] Recognized widely outside Europe, delisting has been adopted, for example, by Argentina, Brazil, Colombia, India, Japan, Korea, Mexico, and Russia.[142]

Delisting has been the locus of debate across the globe. It's one of the most contested legal innovations for personal data.[143] That's because many believe the right to be forgotten overregulates. They consider the right as having tension with free speech and access to information.[144] They argue delisting information can restrict the expressive rights of publishers and searchers, as it makes information harder to find.[145] Critics worry that the right can lead to overdelisting socially and historically relevant information.[146] They posit that, to avoid liability, search engines might remove most information when requested.[147] Some scholars propose resolving tensions pertaining to the right to be forgotten by focusing it on harmful content.[148] This effort illustrates the broader point that anchoring data provisions on harm may solve many of their overregulation and underprotection problems.

The right to be forgotten, more importantly, is underprotective. Even those with the means and inclination to make individual requests might quickly tire under the number of requests normal online activities need and the number of entities these requests must be made to.[149] Moreover, thoroughly delisting links is often impossible because data get rapidly traded between corporations. The right can work on small datasets, such as a public article, photo, or post, not on the inferences that matter in our interactions with companies, because it's difficult to identify and untangle data from the inferences they create after being combined with other data.[150] This reality leads to critiques that the right gives false hope to the people to whom it's granted. The right to be forgotten, for many a symbol of strict regulation,

illustrates how the consent burden can import the procedural approach's limits into individual rights.

Power dynamics permeate the right to be forgotten too. Upon receiving a request, a search engine must determine whether the request outweighs other rights or interests, such as free speech and access to information, as the right is subject to balancing.[151] While the right to be forgotten created compliance costs, it also empowered Google by cementing its position as a global administrator of access to information.

***

The FIPs aren't inevitably traditionalist: nothing explicit in them reduces them to user agreement and procedure. They indicate that any processing of personal data must be "lawful, fair, and transparent."[152] But governments around the world, when crystalizing the FIPs into laws, turned them into procedural protections with room for corporations to circumvent.

The US FTC Chair, Lina Khan, is amenable to moving past the procedural approach. In one of her first speeches about privacy, she stated: I believe we should approach data privacy and security protections by considering substantive limits rather than just procedural protections, which tend to create process requirements while sidestepping more fundamental questions about whether certain types of data collection and processing should be permitted in the first place.[153] The next section explores one way to do this.

C REDUCING RISKS OF HARM

At a Washington Ideas Forum in October 2010, then-Google chief executive officer (CEO) Eric Schmidt was characteristically candid to a startled audience. "With your permission you give us more information about you, about your friends and we can improve the quality of your searches," he said. "We don't need you to type at all. We know where you are. We know where you've been. We can more or less know what you're thinking about." And, after a pause, added: "Was that over the line?"[154]

Traditionalist data protection laws focus on two mechanisms. First, they help each of us reduce our own harm through individual choices. This burdens people. Second, they establish procedures for corporations to complete. This forgets about people. No one thinks this system succeeded in aligning corporate incentives and resolving individual and social digital harms.[155] Not even those in the industry that produces those harms.[156]

Regulations for the information economy would improve by shifting their focus to harm-reduction. Three paths go in this direction: substantive control-independent rules, risk-based legal standards, and accountability tied to harm.

Prohibiting High-Risk Data Practices

Laws need accountability mechanisms that rein in broadly dispersed, systemic data harms. To begin addressing them, they could make their mandatory provisions that transcend "I agree" moments substantive rather than procedural. Laws could limit what corporations can do with our collected and inferred personal data. Incorporating prohibited data practices would free people from having to self-manage risk-related choices over which they have uncertainty and powerlessness.

Legislators can prohibit high-risk data practices, likely to be against collective best interests, while recognizing data processing as a legitimate activity. The law prohibits high-risk forms of otherwise allowed activities in various areas. It doesn't for data. In attempting to make data collection more ethical, laws can miss the possibility that not all data practices may be justifiable and some may be impossible to do ethically.[157] Identifying data practices, such as specific uses for personal data, as too risky and prohibiting them independently of agreements parallels how the law addresses risk in other domains. By focusing on a social dynamic rather than on procedure, they can avoid over- and underregulation problems.[158]

The GDPR engages in similar risk assessments, but they can improve. For example, the classification of sensitive information is motivated by its higher risks.[159] But this idea builds on an unhelpful binary in which one type of information is seen as inherently harmful and another as inherently harmless, as the Lindqvist case illustrates.[160] The right to be forgotten allows one to delist high-risk information. But it depends on individual action. Data protection impact assessments are consent-independent and systemic, aimed at providing accountability through balancing risk to fundamental rights with other interests. But they're weakened by their prospective and hypothetical nature: by remaining procedural, they turn into box-ticking exercises. Legislative attention should focus on risk of harm while moving assessments past procedure and individual control.

The key to calibrating responsibility to risk of harm is that prohibitions meet three criteria. First, they can't hinge on user agreement, like requiring explicit consent to process sensitive information. Second, they should address systemic rather than individual problems, accounting for relational data – not merely providing individual control options. Third, they must be substantive, rather than procedural.

Prohibiting high-risk data practices would bolster laws' after-the-fact accountability. Limiting high-risk data uses, for example, curbs informational exploitation because it focuses on ongoing data practices. These prohibitions avoid burdening people with making risk-reducing choices at "I agree" moments. Instead of identifying unacceptable data practices through a (nonfunctioning) market, legislators would do it through the political process. It would be a collective process rather than an individual one, fitting for collective rather than individual harms.

To create desirable substantive use-restrictions, some jurisdictions use AI regulations to prohibit specific high-risk data uses or purposes. An example of this is the

proposed EU AI Act.[161] The Act is structured by risk, prohibiting some uses of AI considered the riskiest, such as social scoring in the public sector and facial recognition for law enforcement, with exceptions.[162] The Act includes a harm requirement in the prohibitions, stating that it's for an activity within the parameters that "causes or is likely to cause that person or another person physical or psychological harm."[163] The probabilistic harm requirement may be criticized for limiting the provision's scope. However, it correctly presses on the link between ongoing restrictions and risk prevention. It makes explicit that ongoing restrictions aim not to maximize control but to prevent harm. The proposed Canadian Artificial Intelligence and Data Act takes a similar risk-reducing approach.[164] Facial recognition bans in some US cities are another example of this approach.[165]

The watered-down version of prohibiting risky uses in data protection law is the purpose limitation principle, taken from the FIPs. The principle could more accurately be called purpose specification, as Canada calls it, because it doesn't limit any purposes but only mandates that corporations specify them. The principle relates vaguely to the idea of addressing risk systemically. It doesn't limit any uses and it operates through privacy policies. It operates before-the-fact. As a consequence, it doesn't address informational exploitation as prohibiting high-risk uses and setting liability do.

Enforcement illustrates how use-prohibition is systemic. Enforcement can take two forms: fines and private rights of action. Upon a violation of a use prohibition, depending on the type of enforcement, a noncompliant corporation faces a fine (public enforcement), monetary damages (private right of action), or both.[166] In either case, responsibility for engaging in risk is implemented as responsibility for engaging in a prohibited use that's likely to be harmful. While this is not the case for all forms of protection, the best-positioned entities to enforce risk provisions are enforcement agencies. They have better information about violations that increase widespread risk without producing individualized harm.

Reforms toward reducing risk systemically in line with AI regulations would abandon control-reinforcement and procedure-dependency in data protection law to move it toward meaningful accountability. Data protection authorities can enforce these rules better than control-based ones because these rules don't vary on a person-to-person basis.

A Shift to Legal Standards

Rules are specific instructions that must be followed. They typically provide clear guidance on how to act. For example, traffic laws are a type of rule that specify how people must operate their vehicles on the road. Standards are broader principles used to evaluate whether someone acted wrongly. Standards are open to interpretation. For example, many professional codes of ethics include a standard requiring lawyers to act with integrity, rather than listing specific behaviors, because acting with integrity depends on the context.

A possible response to procedural rules' limitations is making data protection law more standard-driven. Making laws more standard-driven means putting after-the-fact accountability mechanisms at their center, rather than as an add-on for before-the-fact provisions. Data protection standards include data minimization, privacy by design, and negligence or strict liability in liability provisions. These substantive provisions focus on systemic effects, matching the GDPR's declared focus on accountability, shared by other EU-inspired jurisdictions.[167]

One GDPR standard that addresses risk systemically is data minimization.[168] It requires that personal data are only collected and processed to the extent necessary for specified purposes.[169] It's also present outside the EU, such as in US state legislation.[170] Data minimization requires corporations to consider alternatives and adopt the one that requires the least data to achieve the desired outcome. It doesn't attempt to specify what's sufficient data for each purpose in advance at the legislative state.

Limiting the amount of data that companies collect reduces informational exploitation as well as their potential for other harms, such as discrimination. Data minimization mitigates boundless data collection without burdening each individual to do so. It doesn't leave it to individuals to determine how much data are appropriate; regulators must do so in light of specified purposes. When enforced by a central authority, data minimization works as an improved version of the individual rights to object and erase: it addresses overcollection, but it does so systemically. Conversely, like those rights, individuals find it impossible to monitor. Relying on individual complaints to enforce the data minimization principle, therefore, boils it down to a replication of the less useful rights to object and erase. Data minimization thus shows that standards that address risk need an enforcement authority with investigatory and sanctioning powers, which some jurisdictions lack.

Another systemic standard is privacy by design, known in the EU as data protection by design. It requires companies to implement measures that consider privacy during all phases of data practices. It was motivated by the view that "the future of privacy cannot be assured solely by compliance with legislation and regulatory frameworks."[171] That's because "legislation and regulatory frameworks" is often equated with "procedural rules." Privacy by design, when adequately implemented, can establish a risk-utility standard, which requires manufacturers to adopt design precautions proportionate to the magnitude of expected risk.[172] It's a method of preventing harm with a flexible legal standard by establishing accountability, without requiring legislators to predict unpredictable consequences.[173] For example, an AI system would meet this standard when it doesn't introduce foreseeable risks of harm that a reasonable alternative design would have avoided where the omission of the alternative design renders the product unreasonably risky.

A concern against legal standards is the introduction of indeterminacy. Some degree of indeterminacy is a consequence of developing laws that respond to future problems and technologies that legislators can't predict.[174] One can't predict all the

negative consequences of data practices, so constructing flexible duties that courts and regulators can apply keeps protected groups at center stage. Standards work best when society agrees on the values to be protected but it's difficult to predict actions' wrongness before-the-fact.[175] Standards' indeterminacy gives them the flexibility to adjust to unpredictable harms to social values; it's also their main benefit.[176] For example, strengthening privacy standards could make data breaches less damaging if, as a result, a breached company holds less personal information or the information it holds is less risky.[177]

Standards' indeterminacy isn't absolute. The rules–standards division is a gradient, not a binary, and data protection doesn't need to be at the end of that gradient. Standards become more certain with time as they're applied to different situations.[178] For example, consider the duty of loyalty, which agents have toward their principals and boards of directors owe to the companies they work for. The duty of loyalty is a standard, which means that courts decide whether an agent was loyal to their principal (or a board member was loyal to their company) when they're sued for it. The obligation to "be loyal" sounds uncertain, but the law evolved to give it clear meanings, including specific duties about what information to disclose and how to behave when faced with a conflict of interest.

Specifying standards with time makes them more rule-like, but keeping some flexibility is desirable. The problem with the FIPs was precisely turning principles into procedural rules, keeping their downsides but losing their benefits.[179] Regrettably, data protection standards are often implemented as if they were sets of rules that one can turn into box-ticking exercises. Data minimization, for example, is critiqued for being overinclusive and ignoring varying levels of risk – a problem characteristic of rules.[180] When the standard's application crystalizes it too much into procedural rules, it loses its ability to capture unpredictable harms.

Privacy by design, similarly, is sometimes either crystalized into too-specific procedural rules or made unhelpfully vague.[181] A helpful permutation of privacy by design, rather, is combining a risk-utility standard with a prohibition of deceptive design. This prohibition, as a second-best to acknowledging that agreement in the information economy doesn't capture consent, would respond to the reality that design affects privacy choices.[182] It could reduce deceptive mechanisms such as dark patterns.[183] Well-established theories of preventing deception, such as negligent misrepresentation torts, can serve as a basis for its application.[184]

A controversial standard of these characteristics that receives significant policy attention is the duty of loyalty.

Information Fiduciaries: The Standard of Loyalty

The theory of information fiduciaries suggests that entities who invite others to trust them with their personal information, and who profit from it, should be required to act in the best interests of the people who trusted them with it.

Information fiduciaries theory states data companies should act in the interest of their users – or broadly of those whose data they process.[185] In this context, best interest means making sure data practices don't endanger or negatively affect people.[186] Imposing fiduciary duties means holding tech companies liable if they fail to prioritize user interests that they should protect.

Fiduciary duties are standards. By operating after-the-fact, fiduciary duties can adjust to new harms we haven't yet anticipated.[187] As Woodrow Hartzog and Neil Richards explain, "loyalty's supposed fatal flaw – its indeterminate vagueness – is actually a great strength of flexibility and adaptability across contexts, cultures, and time … [It] allows us to deal substantively with the problem of platforms and human information at both a systemic and an individual level."[188]

Information fiduciaries would begin to address the nuanced limitations of existing laws because fiduciary duties could bolster it with mandated behavior that's independent of agreements extracted from users. Fiduciary obligations likewise depart from procedural approaches tied to determining prohibited behavior in advance. They determine whether a data practice was harmful or didn't prioritize people's wellbeing after the data practice takes place. By introducing consequence-focused accountability, they depart from privacy's procedural turn.[189] As a consequence, they can avoid overregulation and underprotection problems.

The fiduciary expectation responds to the power asymmetry between corporations and their users that enables informational exploitation.[190] It would require corporations to change business models to mitigate manipulation.[191] Tech giants have more power over our future than doctors, lawyers, real estate agents, investment managers, and estate executors, among others, who have fiduciary duties toward us based on that power.[192] They place themselves in a position to affect others' wellbeing, which enables informational exploitation. The proposals to impose duties of loyalty to entities who invite people to trust them with information, making people vulnerable to them, are a response to that power.[193] Fiduciary duties can address the asymmetries of power that leave people vulnerable in the information economy because that's what they're designed to do in other social relationships.[194] As long as they're not limited to contractual relationships, they address moral hazard's incentive misalignment that leads to informational exploitation.

The information fiduciaries approach, however, isn't free from criticism. First, critics argue that the approach fails to explicitly protect non-users' data, leaving out those without prior relationships to duty-owing companies.[195] Relatedly, fiduciary relationships would, in principle, not protect users from indirect harm once their data is sold or shared by the fiduciary.[196] Second, scholars critique information fiduciaries for the absence of a shared understanding of a trust relationship, which is a vital element of traditional fiduciary relationships.[197] Third, with dubious corporate law foundations, others critique that fiduciary duties to shareholders may conflict with new duties as information fiduciaries.[198] Fourth, because platforms' profit depends on personal data, critics believe it would be complicated to

identify limits over what information fiduciaries can do with it without destroying their business models.[199]

The following chapters propose a simpler alternative: liability for material and immaterial harm, including for informational exploitation. The liability solution is simpler because information fiduciaries presuppose the ability to compensate, so one needs a liability framework in place to implement information fiduciaries – but one doesn't need the controversial fiduciaries idea to implement the liability solution. The information fiduciaries proposal implies establishing duties of care and loyalty by data giants to their users.[200] In the following chapters, I argue that an intermediate duty not to harm is enough.

* * *

To regulate the private sector effectively, lawmakers must reorient data protection laws. An ideal reorientation would be threefold. It would de-emphasize control in data protection rights, keeping them for person-to-person interactions without relying on them to solve power dynamics in the information economy. It would bolster data protections law's substantive provisions over procedural ones. It would expand data protection law's standards that address risk of harm systemically, creating accountability that can adjust to new harms.

Individual control rights with public enforcement are better for privacy than a free market system, but they're insufficient. Their guiding principle is a transactional model, even though they operate over a social reality that's not primarily constituted by voluntary transactions. Data protection laws built on the FIPs inherit their weaknesses: rationality and apathy assumptions that build back doors into the protection system. They include nonharmful data practices and leave harmful data practices out.

The law often combines risk-reducing standards with after-the-fact civil liability when there's uncertainty about what measures prevent harm. The law uses these front-end safety measures in conjunction with back-end threats of liability to prevent harms like the Pinto incident. This combination exists in areas as diverse as driving regulations, environmental protection, competition law, consumer protection, professional malpractice, product liability, and any kind of license or permit such as building, air law, trains, and financial products, among others. Data, as the next chapter details, need this system too.

6

Pervasive Data Harms

Privacy law expects people to behave as if they had clairvoyance.

In 2016, Uber had a data breach involving its drivers' and users' information. An Uber driver sued, claiming that the company failed to secure their personal data from unauthorized parties. But the judge didn't see any harm done. He explained that privacy harm, to be real, must be "highly objective … from deliberate and significant invasions" and "individuals who are sensitive or unusually concerned about their privacy are excluded."[1]

Judges often claim they're unable to assess privacy harm. And, to some extent, they're right. Judges are tasked with determining whether there's harm in each case and if so how much, which are tricky questions to answer in the absence of physical or economic harm. Contrast this description with people making daily privacy choices, such as agreeing to a data practice or enforcing a data right. While our legal system accepts that courts may be unable to identify privacy harm after it occurs, it expects people to identify harm (and act accordingly) *before* it happens. The law hastily accepts that legal experts may be unable to see privacy harms and then expects nonexperts to anticipate those same harms. This expectation is absurd.

Privacy law places the onus on those whom it protects. It unreasonably expects people to foresee the consequences that may arise from data practices outside their control – and beyond their ability to predict. It's up to each of us to engage in social and commercial life in the information economy at our own risk. But if the judge in the Uber case couldn't see the data leak's harm after it happened, how was a "sensitive or unusually concerned" driver supposed to anticipate it? Even if he could, what was he supposed to do to prevent it? The burden of anticipation on people adds to the few incentives for corporations to take measures that mitigate risk.

Two mechanisms contribute to this unrealistic expectation. The failure of individual control mechanisms such as consent provisions defeats the expectation that people will anticipate these harms and agree only to data practices that don't harm them. Procedural rules are also woefully insufficient for protecting personal information because they're insufficiently related to preventing harm. These rules are

typical of contractual activities, but privacy harm occurs outside them. Hacks such as the one the Uber driver faced are essentially digital snooping that people experience because someone didn't keep their data safe enough.[2] They're accidents, but the law tries to address them with principles from contracts.

Harm prevention requires accountability for the consequences of data practices, not just accountability for corporations' promises in privacy policies and compliance with procedural rules. Laws formed primarily by individual control provisions and procedural rules fail at curbing informational exploitation. To address it, privacy law must create responsibility for corporations stemming from the impact their data practices have.

Civil liability, which allows for court-determined compensation based on harm, is a common legal method for tying accountability to the consequences of corporate behavior. For civil liability to be workable in the information economy, it must overcome the privacy fallacy and incorporate intrinsic privacy harm. Civil liability, thus modified, can compensate people for the resulting harm more effectively than our current model and address informational exploitation by leading corporations to internalize (incorporate the costs of) the risks they create.

Identifying privacy harm is difficult for courts, but not uniquely difficult. There's an irony in privacy law's trust in people's ability to predict and prevent harm to themselves paired with its distrust in legal professionals' ability to identify harm after it happens. This chapter suggests how one can identify privacy harm, aiming to provide courts and regulators with a way to move beyond the privacy fallacy, which leaves them oscillating between failing to recognize privacy harm at all or treating all data practices as harmful.

A WHAT PRIVACY LIABILITY IS FOR

In 2021, TransUnion, one of three large credit bureaus (Equifax and Experian being the others), mislabeled thousands of people as possible terrorists and other national security threats in credit reports made available to employers and creditors.[3] One of the victims, Sergio Ramirez, learned about this mistaken designation when he was prevented from buying a car. He sued TransUnion as part of a class action, arguing that the company didn't take reasonable measures to ensure its files were accurate. The company argued that plaintiffs lacked the right to sue because they didn't suffer any concrete harm.[4] The US Supreme Court sided with TransUnion. The plaintiffs' risks of harm they were exposed to were insufficient.[5]

Addressing situations like TransUnion's requires two things. First, recognizing the material harms that many victims, such as Ramirez, experienced. Second, recognizing the intrinsic privacy harm that all victims experienced. Privacy harm is the wrong of producing unjustified privacy losses for others for private gain, violating privacy's socially recognized value. Privacy harm will remain invisible, and exploitation in the information economy will proliferate, as long as courts and regulators

perceive privacy interferences solely through the lens of monetary losses, falling into the privacy fallacy of acknowledging privacy's intrinsic value in theory while dismissing it in practice.

Data Harms

Data practices in the information economy can harm people in various ways. Such harmful results are no longer exceptional and they increasingly occur through inferred information.

Data harms include reputational harm (for example, when employers find inaccurate information about a job candidate), financial harm (such as identity theft), physical harm (like doxing, where the disclosure of personal information often leads to bodily harm), discrimination (for example, when a member of a nonvisible minority is outed), and harms to democracy (such as when someone's tricked into voting for a candidate they wouldn't have voted for otherwise).

The information economy is plagued with reputational harms. While harms to people's reputation happen offline, digital abuse and harassment amplify them.[6] Digital abuse, as Ari Waldman puts it, "is particularly pernicious because it is cheap, fast and permanent."[7] Countless women see their intimate information and naked bodies commodified.[8] Women who face digital abuse are often accused of engaging in sex work or pornography.[9] Digital abuse often involves nonconsensual distribution of intimate images, impersonation, or both.[10] In a US case, Matthew Herrick sued Grindr because it lacked features to prevent impersonators and dangerous conduct, allowing impersonators to direct thousands of strangers to his home and work looking for sex.[11] Grindr profited from Herrick's data but didn't provide basic safety, even after Herrick asked for help.

Financial harm is another common data harm.[12] A salient example is identity theft enabled by stolen or leaked personal data. Examples of financial harm also include credit card fraud; insurance premium increases due to data leaks that undermine a person's insurability;[13] increased prices due to price discrimination as surveillance leads to personalized pricing;[14] and ruined credit scores, which disadvantage people looking for a loan, a home, or a job.[15] Manipulating people into buying things they don't need or want, called "behavior modification," is a pervasive business practice that harms people's finances.[16]

A third type of data harm, crossing the boundary between digital and physical, is harming people's physical integrity.[17] Digital abuse enables stalking online and offline that, for some victims, leads to bodily harm or threats of serious bodily harm.[18] In extreme cases like Tyler Clementi's, described in the book's Introduction, they even lead to death.[19] Another form of digital abuse is doxing, which enables physical abuse by others.[20] Data-enabled harms to physical integrity are disproportionately suffered by women – who throughout history have disproportionately experienced sexual privacy harms.[21]

A fourth type of data harm is discrimination – when members of historically disadvantaged groups are treated unjustly due to their group membership.[22] Discrimination is amplified, for example, when a platform allows its users to make decisions based on race and other protected characteristics. Website Roommates .com did so by asking subscribers about their gender, family status, race, and sexual orientation, to allow other users to filter by those criteria.[23] Facebook used to make it possible for marketers to tailor who saw ads by race, gender, nationality, and other protected characteristics. It still has over 5,000 user categories, some of which enable discrimination by advertisers.[24] When algorithms make decisions based on people's information, opaque discrimination can occur as a consequence. Algorithmic discrimination takes place on a larger scale than human discrimination, while it hides behind promises of neutrality.[25] Discrimination shows how data harms are often social.

A fifth type of data harm is harms to democracy. In recent years, online efforts, many of them through mainstream social networks, were found to influence voters based on their data.[26] The controversy involving the use of data from millions of Facebook users by Cambridge Analytica reflects this. Cambridge Analytica was a consulting firm that worked for political campaigns, including Donald Trump's, that obtained personal data from Facebook users without their knowledge for targeted political ads. The scandal, which led to public investigations and a settlement for $725 million, led commentators to argue that big data threatens democracies by influencing voting outcomes around the world.[27] The scandal illustrates the limits of users' agreements, the ease of targeted online manipulation, and how informational exploitation leads to widespread harms.[28] Manipulation in the information economy that involves privacy harm may also result in social harms to liberal democracy.[29] The thing is, it's unclear whether Facebook broke any laws.[30]

These are common examples of data harms, but not the only ones. People can be blackmailed based on their personal information.[31] They can suffer post-traumatic stress disorder after being doxed. They can be subjected to unlawful arrest after being swatted – when someone falsely reports an emergency to use law enforcement to frighten or harm another person. As technology evolves, new data harms that are difficult to anticipate so as to specify them in legislation continue to emerge.[32] They all have one thing in common: they're enabled by the collection, processing, and sharing of personal data.

Privacy Harm and Consequential Data Harms

Data harms are consequential harms of data practices. They include deliberate practices, such as TransUnion's, and profiting from people's data without keeping it safe, like Uber in its case against a driver or Grindr in its case against Herrick. Privacy is tied to a host of harms because data-driven interactions permeate countless aspects

of our lives. When those harms happen, one shouldn't lose sight of the fact that data practices also produce privacy harm. When a person is subjected to harms due to the collection, processing, or disclosure of their personal data, identifying both their eventual privacy harm and consequential harms is helpful for determining how to remedy them.[33]

In one of their earliest distinctions, Ryan Calo called these consequential data harms "objective" and privacy harms "subjective." In Calo's words, consequential (objective) harm is "the actual adverse consequence – the theft of identity itself or the formation of a negative opinion – that flows from the loss of control over information or sensory access."[34] Intrinsic (subjective) harm is, for the most part, "the perception of loss of control that results in fear or discomfort."[35] This framing tracks the distinction between material and immaterial harm in the GDPR.[36]

I refer to Calo's "objective harms" as consequential harms because, although they're external to privacy's intrinsic value, they happen because of the collection, processing, or sharing of personal information.[37] Rather than an affront to privacy's social value, they affect other values, such as people's finances, reputation, and physical integrity.

A single data practice can produce various harms. Picture a data broker that publishes or sells people's names and addresses. When brokers do this, they facilitate consequential harms by third parties, such as bodily harm if the information sharing results in violence, or psychological harm if someone develops post-traumatic stress disorder after suffering harassment.[38] By enabling and facilitating these harms, they're complicit in their perpetration.[39] They're also engaging in privacy harm. Publishing that information constitutes privacy harm because, as discussed below, it exploits people in a way that interferes with privacy's socially recognized values, such as autonomy and intimacy.[40]

The interaction between privacy harm and consequential data harms is similar to the tort of battery, which protects people from inappropriate or harmful physical contact. Battery chiefly protects one's physical integrity, but that doesn't render all harms caused by battery physical harms. Battery, for example, can cause psychological harm if an injury is severe enough. It would be inaccurate to treat those psychological harms as physical harm because they were caused by battery. Similarly, the privacy tort chiefly protects privacy values, but that doesn't mean that the only harms that a privacy intrusion can cause are privacy harms.

Identifying privacy harm clarifies its close relationship to consequential data harms. Recognizing privacy harm helps victims obtain needed redress for these other interests as well. For example, when credit bureaus are hacked but victims lack evidence that this caused them financial harm, courts are often unsure whether to grant people a remedy.[41] Recognizing privacy harm is especially important for marginalized communities, such as the LGBTQ community, because of privacy's distributional effects: its relationship with preventing discrimination, promoting intimacy, and protecting autonomy.[42]

The Problem: Harm under the Privacy Fallacy

The privacy fallacy results in a reductionist view of the world where people's privacy is only worth protecting to prevent material harms happening to them. This mistaken conception has enormous practical implications: it interferes with the right to sue and obtain compensation.

The main hurdle to achieve accountability in the form of liability is to prove that one was harmed. The reductionist approach interferes with the right to sue and obtain compensation because it prevents courts from identifying harmful privacy losses.

In the US, there's a court split on how to address the challenge of identifying privacy harm.[43] To grant the right to sue, many American courts require data misuse to be tied to consequential harm.[44] Most federal cases involving financial information, for example, are dismissed because plaintiffs couldn't prove financial harm.[45] To ground a lawsuit, stolen financial information must have led, for example, to identity theft.[46] These courts call subsequent consequential harm, such as financial or reputational, "actual" harm, and use it to identify and measure the gravity of an offense.[47]

This position arises, in part, because of the American standing doctrine. To have standing means to have the right to sue. To sue at a US federal court, one must establish a concrete invasion of a legally protected interest that affects one differently than everyone else (called an injury-in-fact). To satisfy this requirement, one must have a personal stake in the outcome of the case, and must be able to demonstrate that one has been particularly impacted by the issue at hand. The US Supreme Court (unsatisfactorily) addressed the right to sue in privacy in light of this requirement in the TransUnion case. It indicated that Ramirez and other members of the lawsuit needed a concrete harm to sue, but it failed to identify privacy harm as being concrete.[48] As a consequence of equating concrete with consequential, most privacy and data security actions in the US fail the moment they arrive at federal court.[49] Curiously, national security statutes in the US implicitly recognize intrinsic privacy harm for some types of collection, making its rejection for the information economy somewhat ahistorical.[50]

Other US courts, however, focus on rule violation, most frequently a procedural or consent rule, for people to sue. They focus on statutory violations at the collection or disclosure stage to ground legal action.[51] Some of them note, for data breaches, the absurdity of waiting until stolen personal information is misused and it creates material consequences to find harm.[52] They consider that no harm is required to sue for data breaches when a statute provides the right to sue.[53]

Comparable court splits exist in Europe. For example, they do among German courts regarding compensation for GDPR violations. Some German courts accept any GDPR violation as sufficient to warrant compensation.[54] After a company mistakenly forwarded someone's banking application to an uninvolved third party and failed to notify the victim of the incident, for example, a Darmstadt court awarded nonmaterial damages. The court established that the accidental sending is enough

to award damages since it results in the person losing their control over their data.[55] Other German courts adopt the opposite view and consider breach insufficient, also requiring consequential harms.[56] When a booking portal illegally shared someone's information with other travel agencies they had used in the past, a Hannover court dismissed the claim, stating the data sharing constituted only a "perceived inconvenience."[57] With variability, courts in Luxemburg tend to be satisfied with a violation of a legal rule and fault, while courts in Spain and Italy tend to require proof of consequential harm.[58]

European courts struggle to navigate harm absent the constraints of American federal standing. In a 2021 Austrian case, the postal service collected information on political affiliation and offered it to political parties for algorithmically driven targeted ads.[59] An anonymized plaintiff was illegally labeled as having a high affinity for far-right populism. They sued the postal service claiming that the association was insulting, damaging to their reputation, and shameful.[60] They asked for nonmaterial damages for distress, anger, loss of trust, and feeling of exposure. The Austrian Supreme Court referred it to the Court of Justice of the European Union to clarify the scope of nonmaterial damages.[61] The Advocate General's opinion, which avoids taking a stance on whether the plaintiff is entitled to nonmaterial damages, shows the difficulty in assessing harm.[62] The opinion takes a dismissive approach to nonmaterial (intrinsic) harm, reframing the question as "compensation without damage."[63] The opinion has difficulties finding how to identify privacy harm as it struggles to distinguish between what it describes as "mere upset" and "genuine non-material damages."[64] Similarly, activists worry that removing compensation for a statutory violation would mean people would rarely receive any compensation for nonmaterial harm.[65] The court ruling is pending.

Canadian courts also fall into the dichotomy. They routinely dismiss cases that claim stress, anxiety, or risks produced by data losses, stating that these harms are not compensable but rather a normal inconvenience of living in society.[66] They did so even when someone left a laptop with people's unencrypted financial information on a train.[67] On the other end of the dichotomy, there's the Canadian Supreme Court. When Deborah Douez and others sued Facebook for its "sponsored stories," which used their names and pictures without their consent for ads, breaching provincial law, the court allowed users to sue without claiming harm.[68]

The split in courts' approach to harm is coupled with a temporal dimension. Overall, courts are likely to dismiss cases when plaintiffs claim a threat of future harm, as opposed to a harm that already occurred. Most courts hold that the threat of future consequential harm is insufficient, requiring present harm as well.[69] Some hold this conclusion when the harm is imminent.[70] For example, when financial information is involved, these courts regularly dismiss cases where the harm alleged is a risk of identity theft – or preventive measures taken to avoid it.[71] However, a few courts hold that a substantial risk of future consequential harm, when paired with a rule-violation, can be sufficient to sue.[72]

Across the globe, in sum, courts dismiss privacy cases for lack of harm based on a reductionist definition of harm. Courts do so under the assumption that surveillance doesn't harm.[73] Courts' demand for more than privacy harm for privacy cases may be the biggest problem in privacy litigation internationally. Some courts don't consider privacy harm as "actual" because they don't see it as concrete and tangible. For them, only consequential harms that courts have historically dealt with (economic, physical, reputational, etc.) meet this threshold. These courts engage in privacy harm exceptionalism by not recognizing the paradigmatic data-driven harm in the information economy, while they recognize intangible harms in nondata contexts.[74] Privacy harm exceptionalism results from the privacy fallacy.[75]

As a response, other courts focus on procedural rules. They base their reasoning on privacy and data protection statutes that identify illegal data practices and recognize victims' right to sue for it.[76] What's prohibited to do, under this view, is actionable. Some courts emphasize this form of wrongness in their rulings. For example, they explain that, by granting the right to sue in these statutes, Congress stated that conduct in breach of them is wrongful and should be addressed by courts.[77]

Harm through Procedure at the Court Level

The divergence among courts shows they struggle with how to evaluate privacy harm.[78] This divergence is driven by the dichotomy of considering any statutory violation as sufficient to sue or require plaintiffs to show consequential harm. Courts, as they see it, have two options to provide redress. The first is to require financial or physical harms. The second is to allow people to sue whenever a corporation breaches a statute that grants the right to sue. This dichotomy is mistaken.

Privacy harm agnosticism is motivated by informational limitations. It's relatively easy for courts and regulators to determine when there's a statutory violation, while harm is more challenging to identify. The easy way out of the harm-identification dilemma is establishing that illegal data collection, use, or disclosure constitutes harm in itself. According to this approach, courts should distinguish between plaintiffs who should be able to sue and those who shouldn't based not on whether victims were harmed, but on whether a data practice breached a legal rule – often a procedural one. In sum, in this view, the right to sue depends not on the effect of the loss on the victim but on the behavior of the offending party. Courts' difficulty with identifying privacy harm is troublesome, as harm plays a central role in granting the right to sue and compensation.

People can be harmed, however, by lots of data practices that legislators didn't anticipate. The approach replicates, at the judicial level, privacy law's procedural turn explored in the last chapter.[79] As a result, courts approach privacy cases in both an over- and underinclusive manner. Simultaneously, they reject cases that deserve redress (where people were harmed) and occasionally allow some cases to proceed when a data practice wasn't harmful.

The procedural response replicates in privacy a problem that takes place for obligations of data security, which have been fractured. Many data security implementations have focused on rule-compliance, creating the false impression that security problems are solved by box-ticking procedural, administrative, and technical measures specified in advance.[80]

At their worst, courts require both elements of the dichotomy, as opposed to requiring neither. Consequential data harm is, under this position, a necessary but insufficient condition to sue. A statutory violation for this position is likewise necessary but insufficient.[81] The creation of new hurdles for compensation slowly reconceives the role of courts in a way that benefits powerful economic actors, providing minimal protection for data harms.[82]

That's the trick that the US Supreme Court employs. TransUnion breached the statute, but the court rejected the plaintiffs' claim arguing they lacked concrete harm, which is a requirement for US federal courts. The court provided no clear standard for determining what would be "concrete."[83] It just provided examples by saying plaintiffs need a "close relationship' to harms traditionally recognized as providing a basis for a lawsuit in American courts – such as physical harm, monetary harm, or various intangible harms including reputational harm."[84] Had victims suffered consequential harm without a procedural violation, they would have been equally unprotected by federal law.

The TransUnion case shows the practical consequences of identifying intrinsic privacy harm. The court expressed concern that there wasn't enough interference with reputational and financial interests of all members of the lawsuit to justify the right to sue.[85] That may be correct. The issue is that it's the right answer to the wrong question. TransUnion also interfered with people's privacy.

The court did recognize, at least, that "intangible harms can also be concrete."[86] It just failed to recognize these concrete intangible harms in the case.[87] In a world where terrorists and ordinary citizens are treated very differently, it's a harm in itself when an entity in a position of power such as a credit rating agency wrongly labels people as terrorists without their knowledge.[88] Requiring that plaintiffs prove some type of harm is workable only if all harms, including privacy harm, are recognized.

A focus on consequential harms doesn't help address the plaintiffs' claims in the TransUnion case.[89] Those other harms had not yet materialized for many of them. But in the future they will, so conditioning standing on them now leads to their harms being left unaddressed.[90] When these other harms materialize, proving their relationship with TransUnion's actions will be too burdensome for these plaintiffs, also leaving them unaddressed. Before-the-fact, courts are similarly situated to people making privacy choices and legislators drafting procedural rules: they rarely know what subsequent harms will happen.

***

Meaningful protection in the information economy is contingent on a cause of action where liability can be established without proof of consequential harms. Otherwise, privacy claims wither for want of material harm, which may only appear years later and in unexpected ways. Consequential data harms and procedural violations are equally insufficient to ground accountability. While requiring consequential harms undermines redress, positing that a statutory violation is necessary constrains private rights of action to situations where corporate behavior matches prohibited behaviors that legislators anticipated.

The unresolved question is how to differentiate harmful collection, processing, and disclosure from nonharmful ones. While most data practices produce privacy losses, some breach procedure, and some produce harm, the latter don't perfectly overlap. A better way out of the dilemma is basing privacy lawsuits on privacy loss and harm.

B PRIVACY LOSSES AND HARMS

Clearview AI is a corporation that built a powerful facial recognition software by scraping pictures from the Internet, such as from social networks.[91] Shrouded in secrecy and backed, among others, by Peter Thiel, it "invented a tool that could end your ability to walk down the street anonymously, and provided it to hundreds of law enforcement agencies [and corporations]."[92] The company can even see what the law enforcement agencies that it lends its software to search for.[93] Facial recognition is an example of a data practice that falls outside consent models and outside regulatory breach, and should be covered by both.

Facial recognition companies such as Clearview AI argue that they don't reduce anyone's privacy because they use pictures that are available online.[94] But facial recognition has an enormous surveillance capacity.[95] It's inescapable, unlike surveillance one can choose whether to engage with, such as fingerprint scans, or those where one can change the object of surveillance, such as cookies. It's invisible, as people don't know if they're subjected to it. And it's ubiquitous because it surveils thousands of people simultaneously. These characteristics make facial recognition possibly the most privacy-reducing surveillance mechanism ever invented. One of its investors, David Scalzo, told the *New York Times* that it "might lead to a dystopian future or something, but you can't ban it."[96] He might be right.

Loss by Data Collection and Inferences

Privacy analyses require a continuous, rather than a dichotomous, view of privacy.[97] This view requires asking whether someone formed a better picture of you, avoiding false binaries such as public versus private.[98] One should do this by identifying whether an observer gained probabilistic information about someone.[99] This focus on probabilistic information allows one to capture inferences and relational data,

such as the ones that facial recognition produces. I call this privacy loss to differentiate it from privacy harm.

In Brown v. Google, Chasom Brown and others filed a class action against Google for surreptitiously tracking them across the web, including outside Google products, without their knowledge. Google can collect information through tools such as Google Analytics, Ad Manager, plug-ins, and the "Sign-in with Google" button. This information includes what people do online, what they're viewing, and what device they're viewing it on, among other details.[100] Google profits from selling targeted ad spots based on people's information, so tracking allows it to place those ads more effectively.[101] Chasom Brown and other members of the lawsuit felt similarly situated to people invisibly and inescapably tracked by Clearview.

To illustrate privacy loss, imagine someone suing with Chasom Brown, called Drew, about whom Google wanted to know their willingness to pay for vacation flights to place ads and pricing more effectively. Google is unable to collect that information directly: it can't call Drew and ask how much they would pay – although it's working on it.[102] In the meantime, Google relies on statistical inferences. When Google has few data points about how much Drew is willing to pay for their next flight, there's a wide range of possible prices. However, Google knows the overall distribution of that information in the general population. Some of those options, such as a willingness to pay $0 or $2,000, are unlikely. Other options, such as a willingness to spend between $200 and $500, are more likely because they're closer to the population average.

If Google were an individual, privacy loss would stop there. Google, however, also has baseline information about Drew, such as their age. That allows it to estimate from a more precise distribution for their age group, rather than the distribution for the general population. This improves Google's probabilistic knowledge. Google can then collect data about Drew to form a clearer picture. Imagine Google tracks that Drew browses four-star hotels. This data point suggests that Drew has disposable income, so they're unlikely to pay $0 for flights or to pay for a first-class flight. These data don't give Google complete certainty about the target information. But the more data Google assembles, the narrower that range of plausible numbers are for what Drew would spend. Each time Google collects another data point, it becomes more certain. As Google gets more specific information, such as how much Drew previously paid for flights, it develops a better estimation, ruling out unlikely options and focusing on a narrower range of plausible ones. Google then forms a clearer picture of the target information by running analytics to aggregate these data. Each of these certainty-improving steps constitute probabilistic inferences.

Every increase in Google's certainty results in an equivalent privacy loss. Google's certainty and Drew's privacy loss are coreferential – two sides of the same coin.[103] In every step, Drew faces a "loss of obscurity."[104] One can identify whether Drew had a privacy loss, even if Drew doesn't know it yet, by looking at whether Google's probabilistic knowledge about Drew improved.[105] The more certain Google is about

the truth of its probabilistic knowledge about Drew (or the lower the chance of error in its estimations), the bigger Drew's privacy loss is.

The idea of probabilistic privacy loss is crucial in a world where entities such as Google and Clearview AI mostly affect our privacy by making inferences about us. In the information economy, we interact with recidivist privacy invaders who learn about us from inferences, relational data, and de-identified data – something unfathomable in the age of fax machines when privacy law was conceptualized. A single data point almost never meaningfully increases the precision of a corporation's probabilistic knowledge. Instead, estimating from an enormous amount of otherwise insignificant data points is revealing.

This framing of losses relates to the importance of viewing privacy as a matter of degree.[106] This view, unlike binary views, captures situations where the loss is produced by aggregating innocuous data from hundreds of entities. It captures inferred information when the entities that collected the information that led to inferences are different. Binary conceptions of privacy (either you have it or you don't) are unhelpful in a social and economic context where pervasive corporate data practices combine to reduce our privacy by different degrees.

Loss by Data Sharing and Leaking

In addition to data collection, data sharing and leaks improve probabilistic knowledge, resulting in inferential reductions to people's privacy.

In the Frank v. Gaos case, Paloma Gaos sued Google for sharing information about her and other users' search terms to third parties, providing websites with users' personal information by informing them of the search terms that led users to their website.[107] They alleged that the unauthorized disclosure led to a feeling of being surveilled.[108]

Gaos faced a privacy loss. Google provided information about her to third parties. Google's estimation about Gaos remained unchanged: disclosing information to the third parties didn't make it learn anything new about her. She lost privacy toward the third parties, not toward Google.[109] By giving her search terms to websites, Google allowed those websites to improve *their own* probabilistic knowledge about Gaos and other plaintiffs. Gaos faced a privacy loss because of those inference-enabling increases in certainty. Although Gaos' privacy loss was toward third parties, it's warranted for Google to be the one to compensate Gaos, as Google caused her loss.

When you share information with a group of people and you expect them not to share it further, you lose some control over that information but still expect privacy over it. That information may be "public" toward those you shared it with, but remains private for the rest of the world.[110] Courts, particularly in the US, often struggle to determine when shared information remains "private," and thus protected by privacy.[111] This struggle follows the public versus private dichotomy, which sees privacy loss through the binary view. For Gaos' privacy loss analysis, it's irrelevant

that Google already had Gaos' information (that the information was already "out there") or that Google acquired the information lawfully (with users' consent).

The answer to whether information is private should be found by assessing how information spreads. Network theory teaches us that information has the potential to spread to everyone. To assess whether information is a "private matter," one should examine whether the information would have reached the third party without the perpetrator.[112] Someone probabilistically reduces someone else's privacy when their data practice causes information that would have otherwise been (more) obscure to become (better) known by someone.[113] Applied to Paloma Gaos, one should ask if the third parties would have had all knowledge they obtained from Google's disclosure without it. The answer is likely no.

The Grindr investigation mentioned earlier in the book, where the app shared its user base with third parties revealing their sexual orientation and HIV status, illustrates how the information receiver distinction applies.[114] Grindr already had the information about its users' sexuality and HIV status. It would be wrong to say that, due to this fact, these users had no privacy loss when Grindr shared that information. While Grindr's knowledge of such users' information was already accurate, the third parties' knowledge wasn't. Sharing the information with third parties produced a privacy loss for Grindr users because, after acquiring the information, third parties' knowledge about the users improved. In other words, Grindr produced a privacy loss because, although its knowledge remained unchanged, third parties became more certain about people because of Grindr's actions.

Data breach cases involve this type of privacy loss. The corporate intention differs, as breached companies don't intend a breach, but rather just intend the security measures that were insufficient to prevent one. However, relevantly for privacy analyses, the victim's loss is equivalent, as is their eventual harm. Like Paloma Gaos, the Uber driver mentioned at the beginning of this chapter had someone else's probabilistic knowledge about him improve due to the breach, not Uber's.

Probabilistic losses are also relevant to tort law. Loss by data sharing is something that could fall under the tort of public disclosure of private facts.[115] Under an eventual tort claim, Gaos' claim would be against Google, not the websites. The difference between an intrusion upon seclusion tort and a public disclosure of private facts tort in terms of the victim's loss is whose probabilistic knowledge is improved.[116] Under intrusion, the perpetrator improves their probabilistic knowledge about the target person. Under disclosure, the perpetrator improves a third party's probabilistic knowledge. The perpetrator is the same, while the type of loss differs. Under this view, someone should be liable for public disclosure of private facts when they reduce the obscurity of someone's information to the point that it becomes easily known by others, even absent publication.[117] Intentionally increasing the audience of information already "out there" should be public disclosure of private facts.

Both forms of probabilistic privacy loss can combine. In the TransUnion case, Ramirez and others contended with both kinds of privacy losses.[118] The first was

creating an incorrect inference about them (that they were terrorists). The second was disclosing the inference. Ramirez's privacy loss was produced by both TransUnion concluding he was a terrorist, which inappropriately affected TransUnion's estimation about him, and TransUnion disclosing an incorrect terrorist alert, which inappropriately affected others' estimations about him.

Privacy loss is a descriptive concept, in the sense that computer scientists tend to talk about privacy, and privacy harm is a normative one, in the sense that lawyers and philosophers tend to talk about privacy. Identifying whether there's a privacy loss in a case determines whether there are privacy values at play worth examining – it doesn't replace the analysis. A loss of obscurity or secrecy by itself isn't harmful because obscurity and secrecy aren't social values.[119] If there's a privacy loss, the case warrants a privacy harm analysis. Courts must undertake normative judgments when they evaluate which privacy losses deserve redress.[120]

Harmful Privacy Losses

Privacy losses are harmful when they exploit. Privacy harm is the wrong of informational exploitation – profiting from someone's data while disregarding their wellbeing when in a position of power toward them.

In a famous 2021 British case, Richard Lloyd sued Google for bypassing his browser's cookie-blocking to collect his personal data without his knowledge.[121] Lloyd requested compensation for each person in a group of 4 million people to whom Google did so. The UK Supreme Court dismissed the case, stressing that people are only entitled to compensation if they prove that they personally suffered harm – Lloyd didn't consider the facts specific to each one of them individually.[122]

Cases that claim loss of control, like Richard Lloyd's, are routinely dismissed on these grounds. Many courts acknowledge that surveillance can be harmful, but they lack a clear picture of what makes it so and, consequently, they misunderstand and dismiss privacy claims.[123] The UK Supreme Court concluded that the term "damage" refers to consequential harm such as financial loss (which it calls "material damage") or mental distress. The court required "damage" to be distinct from the data's unlawful processing, emphasizing that the required harm can't be the unlawful processing itself.[124]

Claims like Lloyd's illustrate that recognizing intrinsic privacy harm is key to protecting privacy's social value. As Ryan Calo says, "[d]escribing the outer boundaries and core properties of privacy harm helps to reveal values, identify and address new problems, and guard against dilution."[125] What the UK Supreme Court lacked was a notion of privacy harm (which it would call "immaterial damage") as a type of harm that data practices can also produce. The US Supreme Court also lacked this notion in Ramirez's lawsuit against TransUnion, getting lost in examining reputational and financial losses.

Because informational exploitation is informational, people can't suffer privacy harm without facing privacy loss. But people can face privacy loss without suffering privacy harm.[126] The priest from the Lindqvist case discussed in the last chapter, for example, faced a privacy loss without harm when the catechist shared news on her blog.[127] Losses of obscurity can even be desirable for building trust, communicating with others, and generally participating in social relations. Under some circumstances, such as to correct a misconception, they might lead to a material gain. Social network users face privacy loss when they share information on them, but whether they're harmed depends on the social network's data practices. Data practices can, but not always do, give rise to privacy harm and other data harms.

Losing control over one's personal data, as Lloyd did, is a loss of privacy, not a harm. Limiting causes of action based on loss of control, as the law currently does, isn't the problem.[128] The problem is that loss of control cases fail because courts don't distinguish between mere loss of control and harmful loss of control. This is something impossible to do while mistakenly seeing individual control through the privacy fallacy.

Because privacy losses are ubiquitous in the information economy, conflating privacy loss and privacy harm would lead one to believe that all data-mediated interactions are privacy-interfering. As a consequence, one would have to either consider that all data practices produce privacy harm, impeding valuable activities and relationships, or that none of them do, abandoning remedies. A loss–harm distinction, with the consequence of overcoming the dichotomies that legal actors are currently forced into, allows courts and regulators to better address social and economic relationships in the information economy.

Recognizing that privacy harm is more than a proxy for future reputational or physical harm – or, in the case of Richard Lloyd, financial harm – introduces some short-term legal indeterminacy. It implies evaluating when losses are harmful in a way that separates privacy harm from the increased risk of future consequential harms that courts are used to addressing. The cause of this indeterminacy is that people reasonably disagree about what privacy protects, so courts may rely on various principles to decide a case.[129] The consequence of the disagreement is that decision-makers will perceive privacy harm through the lens of the values they prioritize.[130] There may not be perfect consistency, as decision-makers grant different prominence to each of these values. That would still be an improvement. That's how the law addresses other social values such as democracy and free speech. Courts and scholars disagree about what these values protect while maintaining a common understanding that they're intrinsically valuable – besides being desirable instruments for something else, such as economic development.

Providing flexibility in a legal framework that recognizes that people can disagree about the function that privacy plays is advantageous. It means that not only people who believe in a particular conception, such as control or limited access, can implement it. The only thing that intrinsic privacy harm requires is recognizing that there's something in privacy worth protecting.

Privacy Harm as Harm to Privacy's Values

Recognizing privacy harm is the logical consequence of recognizing that privacy has intrinsic value – that it's worth protecting in and of itself.

In the infamous US Supreme Court case Spokeo v. Robins, Thomas Robins sued the Spokeo website for making ghost profiles about him and others with false information about their education and employment history. When potential employers saw misleading information about Robins on the Spokeo website, they were less sure about Robins' employment information, which he needed them to know for obtaining interviews. Robins, undoubtedly, would have been better off had Spokeo published nothing about him. But Robins and others lacked concrete evidence of reputational harm through actual job losses, so the US Supreme Court was unsure of whether they should be granted remedy under federal law.[131] The Spokeo case was a precursor of TransUnion in narrowing people's right to sue for privacy in the US.

To determine whether a loss was harmful, one must examine privacy's values. Those social values allow one to determine which data practices that produced privacy losses produced social harm. While it's impossible to have a comprehensive list of values for any type of social interaction, in a study of privacy scholarship Daniel Solove identified six. Privacy scholars have grounded privacy's importance, most of the times, on the right to be let alone, informational autonomy through a limited access to the self, concealing information through secrecy, control over one's personal information, personhood as the preservation of one's dignity, or intimacy and the promotion of relationships.[132]

These values are the pillars of the social norms that relate to privacy because those social norms are structured to protect them.[133] While this list is not exhaustive, interfering with these values amounts to interfering with what, throughout history, most scholars have argued privacy intends to protect.[134] While privacy values intersect, in corporate collection, processing, and sharing of personal data, two frequently affected values are autonomy and intimacy.[135]

Our autonomy can be interfered with through our personal data. We develop ideas better away from surveillance or public exposure, so privacy protects people's ability to make their own decisions.[136] Online manipulation amounts to privacy harm when someone affects our decisions by using our personal data to target and exploit our vulnerabilities.[137] Facebook did so when it allowed advertisers to target teenagers whom it identified as feeling "worthless," "insecure," or "defeated."[138] Companies interfere with people's informational autonomy when they ignore legitimate consent refusals.[139] Richard Lloyd, for example, suffered privacy harm because, in overriding his browser's cookie blockers, Google operated not merely without his consent but against it. Lloyd had withdrawn consent and such withdrawal was ignored. Interfering with informational autonomy often leads to consequential harms. Cambridge Analytica harmed people's informational autonomy by deliberately manipulating them into providing information about themselves and

others, producing harm to democracy as a consequence. When someone uses our personal information to our disadvantage by covertly manipulating us, that constitutes privacy harm independent of its material consequences.[140]

Intimacy is about protecting the integrity of information about one's personal identity.[141] Intimacy is a crucial value in sexual privacy invasions, which place obstacles on forming one's identity.[142] It relates to a long history of privacy protections focused on inviolate personality.[143] It exists outside sexual privacy invasions as well. Identity theft causes financial harm to people as a consequence of the privacy harm that is their identity violation. Intimacy, as it relates to identity, is the privacy value affected in collective privacy harms that target a group identity.[144] For example, if an AI algorithm used for hiring disadvantages groups of people because of their gender, there's consequential harm of discrimination caused by the privacy harm of exploiting information about their gender identity. When Facebook provided its users' group identity to advertisers to facilitate discrimination against them, it produced identity-based privacy harm; advertisers produced the consequential discrimination harm.[145] Clearview AI and other facial recognition companies illustrate how surveillance tools increasingly produce group privacy losses and harms through inferences.

These harms can fit different doctrinal categories, depending on the jurisdiction. One way to categorize intrinsic privacy harm is as dignitary harm. In one influential formulation, dignity is about having people's intrinsic worth recognized and respected by others,[146] to which exploitation is contrary. Informational exploitation interferes with people's dignity because it's a form of instrumentalization.[147] Privacy harm, under this conception, is one way to treat a person as a means rather than as an end because informational exploitation is to use someone as a means for the end of making profit.[148] People don't have their intrinsic worth recognized when they're treated as if their wellbeing didn't make a difference. Disregarding the effects of data practices on people's wellbeing can thus constitute dignitary harm. Scholars of intimate privacy, for example, indicate how image-based sexual abuse affects victims' dignity independent of their physical, psychological, and economic harm.[149] Beyond data misuse, entities that create the conditions for data breaches can exploit by omitting safeguards over people's personal information that they profit from. The dignitary harms categorization may fit European legal frameworks, which have a history of relating privacy to dignity.[150]

Alternatively, one can categorize privacy harm as emotional harm suffered by a reasonable person. This alternative places some conceptual distance between the interference with privacy's social value and what a reasonable person would find emotionally harmful. But as long as privacy harm is seen as an objective standard, rather than a subjective standard depending on the victim's perception, it captures informational exploitation. In the US, doing so has the advantage that it falls under a type of harm that courts recognize.[151] Privacy scholars have argued that data breaches produce an amount of emotional distress analogous to the distress courts otherwise recognize as intrinsically harmful.[152] Other common law jurisdictions, such as the

UK and Canada, may be amenable to both approaches.[153] This approach requires moving past the contractual paradigm to use tort law principles.

Thomas Robins' case against Spokeo illustrates how harm can fit both approaches. When Spokeo made false information about Robins available to employers, giving him the option to pay Spokeo to correct it, the company exploited him. Robins didn't just lose control over his personal information. The company profited at his expense with disregard for his wellbeing. Because Robins was used as a means to an end, Spokeo's privacy harm interfered with his dignity. Similarly, because someone looking for a job would be reasonably worried and anxious if they found false professional information about them available online to employers, it amounts to emotional harm as suffered by a reasonable person. Because these harms respond to social values, they're independent of what Robins subjectively felt.

Courts that remain agnostic to privacy harm are tying one hand behind their back. Recall that identifying breach of a procedural rule is the traditional way to determine if someone should be able to sue for their privacy. Courts aren't limited to finding wrongness in documents written by the legislature; they can also determine it. A way of incorporating a wrongness standard, such as one that captures intrinsic privacy harm, is when a court enforces a standard embedded in social practice. When courts consider a form of harm to be socially significant enough that it must be made actionable, they can respond to it by extending tort law – or, in civil law countries, extend the interpretation of the relevant articles of the civil code. Regulators, such as European data protection authorities and the American FTC, can also adopt this richer conception of privacy harm.[154]

The Role of Social Norms

The boundaries of what affects people's dignity and emotional wellbeing change across cultures and time. To adjust to these changes without being restrained by a temporal or cultural approach, privacy harm can be identified through the social norms that pertain to privacy's values.

Social norms distinguish acceptable losses from unacceptable ones in a society.[155] One can use social norms to distinguish between harmless privacy losses and harmful ones because they form social standards about what's socially acceptable to learn about others.[156] Social-norms-informed assessments over privacy loss include values such as autonomy and intimacy because, by definition, social values inform social norms.[157]

Social norms, for that reason, can add precision to privacy harm inquiries.[158] They may shed light on when someone's autonomy or intimacy was interfered with. As Helen Nissenbaum explains, "what makes us indignant, resistant, unsettled, and outraged in our experience of contemporary systems and practices of information gathering, aggregation, analysis, and dissemination is not that they diminish our control and pierce our secrecy, but that they transgress context-relative informational [social] norms."[159]

One should identify the social norms relevant to a data practice given its context to determine whether it causes privacy harm.[160] The social standards applicable to data interactions depend on three factors: the entities involved, the type of information, and how the information was collected, processed, or shared.[161] In other words, to examine the relevant social norms, one must ask what the information is, who's involved in the data practice, and how it's carried out.[162]

The first factor is who's part of the information interaction, including who shares the information, who receives it, and who the information is about. People's wellbeing and informational norms vary depending on the observer. Most of us value sharing things about ourselves with friends or family but wouldn't value third parties learning about them or, worse, some of those things becoming public.[163] One could gain in wellbeing, for example, from one's partner noticing when one leaves for work every morning. But one may lose wellbeing, and a reasonable person may find it inappropriate, if a stranger gains the same information. Acquiring the same information in the same way may or may not violate social norms depending on who shares it with whom. This factor differentiates Grindr sharing its users' sexual orientation and HIV status with third parties from users sharing the same information with each other.

The second factor to determine social norms is the type of information. Paloma Gaos, who sued Google for data sharing, may be unharmed by whoever learns some types of information about her, such as if strangers read her LinkedIn bio.[164] This could overlap with information that many people already have, but not necessarily – for example, she may want strangers to find out that she got a new job when it just happened. One type of information that is frequently harmful to some but not others is gender. Someone outed as nonbinary or trans could have a significant disruption of their wellbeing regardless of whether they were also a victim of discrimination as a consequence, which is captured by privacy harm. For example, people who are outed as trans at their workplace face examples of data sharing that's socially inappropriate given the type of information involved.

Under a continuous view of privacy losses that captures probabilistic inferences, the type of information exceeds each collected data point. The baseline data to which a company aggregates new data forms part of the type of information. Sometimes, a small privacy loss produces no privacy harm but a larger privacy loss does, even for the same person and for the same type of information. For example, if Google had known nothing about Chasom Brown, he may have faced a small privacy loss when Google tracked him across his browsing behavior. But the same data can produce a large privacy loss given that Google knew a lot about him. The more Google knows about Brown, the more inferences it can make about him. The baseline information doesn't produce a mere difference in magnitude, but a difference in the type of information obtained. This difference can affect whether inferences become harmful, interfering with Brown's intimacy or putting him at risk of manipulation.

The third factor is the conditions under which the information is collected, processed, or shared. Consent makes some, but not all, information flows appropriate.[165]

For example, consent is a decisive factor for determining whether two people can record an intimate encounter or recording it was exploitative.[166] In other contexts, the required conditions are rather confidentiality, reciprocity, or notice. Uber's data breach, for example, was an inappropriate information flow because people's data weren't held confidentially even though confidentiality was required by the relationship between Uber and its drivers. It constituted privacy harm because profiting from people's data paired with placing insufficient security measures exploited people's informational autonomy and put them at risk of consequential harms.

This third factor informs the Lindqvist case discussed in the last chapter, where a parishioner shared information on the parish's blog. The priest faced privacy loss, but not privacy harm. In their informational community, it was expected that she would share the information with other members.[167] The disconnect between harm and sanction is what makes the outcome of the case intuitively and normatively inappropriate.

Privacy social standards, in sum, are tethered to privacy's social values.[168] Their entwinement means that one can evaluate the reasonableness of someone's privacy claim by identifying whether the data practice they sue about unreasonably interfered with privacy's social values.

It's common for context and social norms to be considered when applying privacy torts, for example, by examining the magnitude of the intrusion, the means of intrusion, the type of information obtained, and whether a reasonable person would expect the conduct. The notion of intrusion in tort law is inherently social and context-dependent. Once one reckons with the idea that corporations can harm absent procedural violations, there's no normative reason why the delineation of intrusive corporate acts should be treated differently.

***

The idea that privacy losses exist along a continuum (rather than as a dichotomy) allows courts and regulators to account for the fact that losing a small amount of privacy is different from losing a significant amount of it. Some privacy losses interfere with autonomy and intimacy values, but not all do. Social values determined by social standards distinguish acceptable intrusions into people's personal information from unacceptable ones.[169] Having laws and courts rely on those norms in assessing wrongfulness means that companies would be liable for data practices that a reasonable person would consider unacceptable or unjustified.[170]

Legislators, courts, and regulators can incorporate these social values into legal standards that define wrongness through privacy harm, as opposed to making wrongness pivot on procedural rules or agreements. In building those standards, social norms help distinguish unjustified (harmful) privacy losses from justified (unharmful) ones. Exploitative privacy losses, in this view, are unjustified by social norms.

C WHY HAVE PRIVACY LIABILITY

Steven Krenzel was a Twitter engineer in 2016, when the company needed money.[171] An American telecommunications company reached out with a potential solution. It asked Twitter to help it learn about cellphone signal strength based on Twitter data. When Krenzel provided signal strength information, the company said it was useless, so he went to the headquarters.[172] In his account: "I wound up meeting with a Director who came in huffing and puffing. The Director said 'We should know when users leave their house, their commute to work, and everywhere they go throughout the day. Anything less is useless. We get a lot more than that from other tech companies.'"[173] Krenzel initially refused, but Twitter's legal team reportedly approved the request because none of it violated Twitter's Terms of Service – or the law.[174]

No one knows what happened with the project. Ultimately, it may have been discarded by Twitter's then-CEO after Krenzel escalated a complaint.[175] But the story illustrates a larger point: the company could have done whatever it wanted with its users' data.

Second-Generation Liability Depends on Privacy Harm

Repairing privacy harm does more than compensate appropriately. It also reduces the risks of data harms by deterring harmful data practices. By doing so, liability can also curb informational exploitation. This duty not to exploit includes data practices and data breaches, as both involve profiting from someone's data; in data security, the profit motive is indirect but real.

Incorporating accountability into the information economy through civil liability has an enormous benefit: preventing exploitation like the large-scale one that Twitter almost engaged in. Liability mechanisms, rather than increasing people's control over their personal information, can curb harm in a context where control is impossible. Individuals and legislators can't anticipate and prevent all harm permutations in the information economy. But privacy law can reduce them by granting remedies.

Civil liability incentivizes risk reduction before-the-fact by making entities responsible for the harm those risks create after-the-fact.[176] By making privacy harm as much a risk to corporations as it is to their users, corporate liability could curtail informational exploitation by incentivizing corporations to focus on the process of minimizing the likelihood of the harm occurring. This mechanism would help reduce large-scale harmful surveillance like the one proposed by Twitter and (ostensibly) stopped by Krenzel. That only works, however, if entities are made responsible for all harms they cause.

The proposed liability aims to capture that function. By defining redress based on harm, compensation paid to people tracks the risks that they're exposed to. This leads corporations to internalize risks regardless of whether there was a regulatory breach or a promise involved. Private rights of action based on breach of regulated conduct can't engage in this form of risk internalization.

Outcome-based liability overcomes procedural rules' limitations, rather than replicating them. Existing forms of liability improve enforcement by reducing public resources needed by public authorities. But how rules are enforced doesn't change the nature of the rules. Corporations can still pay attention only to the specific mandated behaviors and ignore whether they're producing harm. It allows corporations to harm while avoiding liability. In the Twitter story, for example, users would have faced privacy loss and privacy harm. They would have done so in a way that was unanticipated by themselves and legislators. For Twitter's eventual liability to prevent it from exploiting its users, it must be based on harm, rather than regulatory breach, because it could engage in exploitation without regulatory breaches.

Liability so introduced would change the cost of data practices for the industry. Compensation can correct informational exploitation by varying compensation according to harm. If the cost of data practices wasn't fixed by what people agreed to or procedural steps taken, but rather varied by the harm caused, corporations would have to take risks into account because doing so would become cost-minimizing. The deterrence argument for outcome-based liability extends to cybersecurity. Reducing informational exploitation through reasonable security measures contributes to policy proposals to shift laws' focus toward minimizing risk.[177] In other words, corporations would have better incentives not to overcollect, overprocess, or overshare data, and to invest in reasonable security measures. Harming the people they profit from would become expensive.

The reticence to consider redress absent consequential harms, while maintaining a broad conviction that surveillance can be harmful, relates to a policy concern. The fear is that, if recognized, any data practice will face (and eventually lose) a privacy lawsuit to the point of making the system unworkable. Building liability on privacy harm avoids risks of frivolous lawsuits because lawsuits based on harm are, by definition, not frivolous. By extension, identifying harm to social values addresses concerns of under- and overenforcement, explored in the last chapter. It overcomes the dichotomy of treating privacy's value overinclusively or abandoning it.

Outcome-based liability is the paramount example of risk-reducing standards proposed in the last chapter.[178] If incorporated into privacy laws, this form of liability would still be a duty that arises from a legal wrong: the breach of the duty not to exploit others based on their personal information. Private rights of action have enormous potential for privacy protection, but they're mostly fallow. To protect people effectively in the information economy, private rights of action must depend on intrinsic harm.

Privacy Harm Liability Can Address Persistent Privacy Problems

Like substantive regulation, liability avoids the practical and moral limits of relying on individual control in a context where AI makes privacy harm relational. A regulatory focus on individual control has proven to lead corporations to overpromise and fail to deliver on their aspirational commitment to eliminate harm.[179] In the Twitter

example, there was no feasible way for people to know what to ask for – or give consent. Outcome-based extracontractual liability escapes problems of power-enabled manipulation and extracted agreements that thwart current protections.[180]

Outcome-based liability addresses the underprotection of inferred, relational, and de-identified data.[181] Inferences, as seen in the last three chapters, challenge existing protections, while they're the paramount risk we face. Liability built into a concept of probabilistic privacy loss overcomes this problem because responsibility is determined based on outcomes (rather than by individual agreements or procedures), so it can capture inferential gains in information in ways that the current system can't. Liability for privacy harm also captures collective harms through relational data in ways that individual data rights, and existing private rights of action based on consequential harms, can't.

This proposal has informational advantages over existing regulation. Legislators can't anticipate all harms. Risk minimization standards are desirable but, as discussed in the last chapter, their implementation consistently leaves a lot to be desired. Consequential privacy harms face similar information problems because they're incremental and difficult to quantify ahead of time, thus being limitedly helpful to establishing accountability.[182] While information asymmetries still exist under liability, courts are well positioned to address them because they act after the fact – together with having institutional advantages such as technical training and fact-finding capabilities that regulators in some, but not all, jurisdictions have.

A liability focus similarly overcomes the critiques to data rights, discussed in the last chapter.[183] There's a mismatch between individual, control-focused data rights and social, structural data harms.[184] Focusing on privacy harm, as opposed to individual control, procedure, or material harms, productively shifts legal actors' attention on structural aspects.

Outcome-based liability has one crucial advantage that's shared with fiduciary duties, also discussed in the last chapter: it addresses moral hazard, and therefore exploitation.[185] Under fiduciary duties, for example in corporate law between shareholders and the board of directors, the fiduciary's duty aligns incentives by deterring after-the-fact risky behavior that the other party can't see.[186] This proposal, while capturing that accountability-producing function, avoids the main critiques issued elsewhere against information fiduciaries. It can be implemented by legal actors who worry about aspects of the fiduciary proposal.

The information fiduciaries model has been critiqued on the argument that platforms and their users lack a shared understanding of trust relationships, which is described as a vital element of traditional fiduciary relationships.[187] Liability can be established absent a shared understanding of the relationship or an invitation to trust the entity with one's personal information. Bolstering it doesn't require placing special duties on corporations, but rather extending the duty not to harm that we already owe each other.

Information fiduciaries theory has also been critiqued because, unlike professional fiduciaries, platforms profit from personal data. Critics worry this economic difference complicates limiting what they can do with that data while preserving the information industry.[188] Liability doesn't place hard limits on what corporations are allowed to do with information. This allows it to avoid any broad application that risks making the information industry unsustainable. It avoids such risks of overexpansion by being anchored to a notion of immaterial harm.

Information fiduciaries have been critiqued for not protecting the data of nonusers whose information comes into the ambit of a social media platform such as Twitter or Instagram – a manifestation of relational data.[189] An information fiduciary's relationship would, in principle, also underprotect users from indirect harm if the fiduciary reasonably shares their data.[190] Liability avoids this problem by moving from a contracts paradigm into a torts paradigm, where no prior relationship is required. The fiduciaries model can overcome this objection by doing the same, but doing so may strengthen the first critique of risk of expansion.

Last, information fiduciaries theory has been critiqued because corporations already owe fiduciary duties to their shareholders, which may conflict with their new duties as information fiduciaries.[191] Independent of the merit of this concern, liability doesn't conflict with corporate duties. Liability is a standard method to make corporations responsible for their behavior in a compatible way with other obligations, so this proposal is not suspect of creating conflicting legal duties.

Corporate liability based on a duty not to harm, centered on informational exploitation, would overcome pervasive problems of our current system and establish meaningful accountability in a way that avoids concerns legal actors may have over other proposals.

Intrinsic Privacy Harm Surmounts Objections to Liability

Four common objections to liability are worth considering. One is the risk of meritless lawsuits. Another is difficult-to-establish causality. A third is whether insurance would undermine liability's benefit. A fourth is difficulties in identifying harm.

A first objection to liability is the risk of meritless nuisance lawsuits. For example, a recent report on federal US legislation argues: "Private right of action substantially increases companies' legal risks. Introducing this amount of legal risk inevitably leads to unnecessary lawsuits […]. If companies must spend money on compliance and legal fees, they cannot invest that money in other areas, such as by lowering prices, offering discounts, or creating new products."[192] Considering that a statutory violation itself is the harm leads to concerns of enabling frivolous lawsuits. People worry that plaintiffs can be creative and find a statute that allows them to sue without being harmed.[193] While it's unlikely that people would incur the cost of suing when litigation costs would outweigh benefits, a concern may be that lawyers encourage otherwise unmotivated plaintiffs to sue to vindicate a trivial procedural violation. If

that were the case, rulings that provide a remedy without requiring proof of harm could promote meritless lawsuits.[194]

The meritless lawsuits objection has a solution once one acknowledges harm to privacy moving past the privacy fallacy: basing compensation on privacy harm. The risk of meritless lawsuits exists in other areas of law, where courts curtail them to an acceptable level by avoiding overexpansive bases to sue. Their increased risk in privacy is created by the false dichotomy of compensating all privacy losses or none of them. This dichotomy leads to overly broad privacy claims, often from the corporate side, such as companies using privacy as secrecy to prevent algorithmic transparency or using GDPR compliance as a pretext to avoid sharing useful information in trials.[195] A concept of privacy harm linked to the reasons for which society considers privacy worth protecting allows legal actors to distinguish those frivolous claims. This improved understanding may also avoid under-compensation, which happens downstream when basing privacy on statutory violations without an evaluation of harm.[196]

Countless privacy losses have non-negligible effects. Cases like Chasom Brown against Google, Thomas Robins against Spokeo, and Sergio Ramirez against TransUnion should be distinguished from frivolous cases by the privacy harm involved. Recognizing and remedying harms in such cases doesn't open floodgates to litigation. It just compensates victims for immaterial harm as the law has done for centuries.

A statutory private right of action with clear limits on its scope can further narrow the range of lawsuits.[197] For example, statutes can set a statutory maximum for immaterial damages low enough for any strategic individual to lack incentives to sue. Concerns can also be mitigated by procedural measures, such as requiring plaintiffs to pay businesses' legal fees for claims that a court finds frivolous, as the CCPA does.[198] As a second-best, statutory damages could make compensation for privacy harm symbolic, leaving victims with any consequential harm if proven, a nominal amount for immaterial harm, and compensation for their legal fees to provide incentives for meritorious claims. Capping compensation for immaterial harm would eliminate the risk of frivolous lawsuits while allowing people to rectify informational exploitation and address standing problems for consequential harms. Nominal amounts, a well-recognized approach in tort law, may become meaningful for deterrence if aggregated in a class action.

A second objection is that causality is difficult to establish in privacy law. It's close to impossible, for example, for someone to trace back a duplicated credit card to the aggregation of different pieces of information. This problem appears in other areas of law as well. For example, whether fishermen's lost income stemming from oil spills was caused by an environmental harm is often contested.[199] Victims of data harms have parallels with victims of environmental harms who, for example, have difficulties proving that diseases were caused by specific emissions.[200]

These causation problems are specific of consequential harms. Consequential harms, such as financial harm, often materialize much later. They're latent.[201] Once

they do materialize, causality with a data misuse or data breach is difficult to establish.[202] These difficulties are produced because delayed harms are difficult to match with data practices.[203] It's difficult for plaintiffs to show harm that hasn't yet transpired, or the precise causal chain that links an actual harm to a defendant's actions long ago.

Given causality problems, acknowledging privacy harm together with other data harms is important from a practical perspective. Currently, relying on risk of future consequential harms runs afoul of the requirement that harm must already exist for it to be concrete.[204] If courts did away with the requirement, causality problems would turn the doctrinal problem into a practical one. Remedying solely consequential harms doesn't only leave privacy harm unaddressed. It leaves those consequential harms frequently unaddressed too.[205]

Identifying (intrinsic) privacy harm avoids causation quagmires because informational exploitation doesn't appear with consequential harms' delay. It has a clearer link with the data practices that cause it because it's formed by a privacy loss and its wrongfulness.

A moderated causation problem would remain for inferences where multiple actors are involved. Courts should address this problem by building on the idea of probabilistic privacy loss by data sharing, which captures privacy losses produced by more than one entity. In doing so, they can borrow a doctrine from mass product torts and establish joint and several liability – sometimes called solidary liability.[206] The doctrine holds multiple entities simultaneously liable when they contributed to indivisible harm but it's impossible to establish who was the proximate cause and who caused it by how much.[207] The victim can sue all entities or only one of them for the full amount. Later, the entities can recover from each other without burdening the victim to prove which one caused each amount.[208]

A third objection is whether liability would be useful with an insurance market. Cybersecurity insurance covering damages and fines for loss of and unauthorized access to personal information has become popular. A concern is that deterrence wouldn't happen if all corporations were insured. If the insurance market worked well, premiums would reflect risk, so insurance wouldn't impede deterrence.[209] But, based on cybersecurity insurances' performance, there are good reasons to be skeptical of how efficiently privacy liability insurance would work.

There are three regulatory options. The first option is banning insurance for privacy liability, a solution suggested for GDPR fines as a reaction to the non-rising levels of cybersecurity after the insurance market appeared.[210] Insurance exacerbates the individualization of informational exploitation victims under an administrative regime while benefiting harm-doers from collectivized protection.

An alternative is to do nothing. Insurance is problematic for causation-problem-ridden consequential harms. But, for privacy harm, victims could be compensated by insurances at least as well as by they would by corporations in a scenario of liability with no insurance. Further, liability with insurance sets better deterrence for corporations than no liability does. The evolution of insurance will depend on

the evolution of technology. If insurers learn what measures reduce risk – shifting information costs currently placed on legislators – they may be able to model premiums.[211] If they can't anticipate risk-reducing measures, insurers have incentives to establish scoring systems with premiums depending on riskiness, such as through history of harm. Insurers may not do this in the short term, but it would be difficult for them not to go bankrupt if they absorbed all harm from informational exploitation at an inflexible premium.

An in-between alternative is to regulate the insurance market to maintain deterrence by establishing a cap on insurance amounts. For example, by establishing that insurers can cover a maximum of 60 percent of any claim. An alternative but less effective option is only allowing insurers to cover claims over a minimum individual amount, increasing deterrence for individually low but widespread harm that's less likely to appear in court. These measures would be difficult to implement for consequential harms due to their temporal issue, but they're possible for privacy harm.

A fourth objection to outcome-based liability is that privacy harm is often difficult to determine. Relying on liability implies facing difficulties in determining compensation – and the indeterminacy of privacy harm could worsen them.[212] For example, people incur monitoring costs to prevent threats of data leaks and courts don't usually see those costs as compensable.[213]

Two things are certain in response to that objection. To the extent that privacy liability doesn't preempt public enforcement, investigation, and penalties, a lower-than-efficient level of liability is an improvement over no liability at all. Believing that few would sue is a reason to be *less* worried about implementing liability, not more.

Moreover, for any privacy harm indeterminacy, privacy harm is easier for courts and enforcement authorities to identify after-the-fact than it is for people (and legislators) to anticipate and prevent before-the-fact. Any objection to establishing liability based on the difficulty of estimating privacy harm also applies to the standard alternative to extracontractual liability provisions: liability for breach of consent provisions. The estimation problem is worse for consent provisions than for extracontractual liability because any indeterminacy is greater before-the-fact than after-the-fact. It's also because experts, such as courts and regulators, are better equipped to deal with such indeterminacy than people are while they go about their daily lives. If courts have a difficult time seeing privacy harm after it happens, how can one expect people to see it before it happens? Courts and regulators can use frameworks to assess privacy and data harms from past behavior.[214] It's more difficult for people to assess them for future behavior, particularly when combined with uncertainty and moral hazard.

Three further objections, difficulty in determining a standard, too few incentives to sue, and difficulties in assigning a monetary value, are examined in the next chapter on implementation.[215]

* * *

Establishing accountability in the information economy requires overcoming the consequences of the privacy fallacy. Problematically, courts often require plaintiffs to prove consequential harm, such as financial harm, to give privacy victims remedy. As a misguided remedy to the ill, courts have looked toward procedural breaches while skipping loss and harm, thus missing harms that legislators couldn't anticipate. As a result, victims of privacy harm lack a legal remedy, while those who are similarly situated (but can show other types of harm) have one. Harmful behavior, likewise, goes undeterred.

To identify harmful data practices, one must ask whether someone was exploited based on their personal information, impeding privacy's social value. That value is embedded in informational social norms. One way to evaluate it is by asking whether the data practice that produced a privacy loss violated social norms considering the type of information, the people involved, and the way the information was transmitted or processed. Courts could capture privacy harm under existing doctrinal concepts by conceptualizing it either as harm stemming from a violation to one's dignity or emotional harm under a reasonable person standard. Privacy harm must be built on a concept of loss that overcomes the binary view. Examining loss as probabilistic information gains is key, as it captures all-important AI inferences and relational data.

To identify privacy harm, we're left with a three-step inquiry. First, was there an information gain in the statistical sense, making it a privacy loss? Second, did it interfere with a socially recognized value of privacy, making it unjustified? Third, did the perpetrator derive any form of private gain, making it exploitative?

To be effective at reducing harm, privacy law needs outcome-based liability. The next chapter explores how to implement it.

7

Privacy as Corporate Accountability

Some of the clearest privacy and data harms happen as a result of data breaches.[1]

In 2019, Canadian financial conglomerate Desjardins revealed that 9.7 million of its current and former clients might have had their data disclosed, but it wasn't sure which ones.[2] As a "remedy," Desjardins gave each of its clients two options. They could continue as if nothing had happened, or they could agree to give their personal and banking data to a third party of Desjardins' choice to assess whether they had been a victim of fraud. The third party that Desjardins selected was Equifax, the credit rating agency notorious for its own massive data breach in 2017 that affected roughly 143 million people. If Equifax found fraud or identity theft, Desjardins promised to reimburse those clients up to $50,000 (CAD).[3] People's options were to give away more data to a third party to perhaps be compensated, or receive no compensation and ignore whether financial harm happened. If the reimbursement required exceeded the limit, they would still be undercompensated. Victims had only one option: to agree. Most of them did. After the story became public and victims filed a class action, the bank settled for up to $201 million to be distributed among class members who could prove material harm independently of what Equifax determined.[4]

One victim, who asked to remain anonymous, happens to be an expert in civil liability. She recounted to me her one-year nightmare of fraudulent charges to her bank accounts, constant robocalls, and harassment from credit collection agencies. She received $90 (CAD) for the time she lost mitigating these consequences and, by the time this book is published six years after the breach, is waiting to see if she'll get any other compensation.

The Desjardins case highlights the need for meaningful accountability. Without it, even those with knowledge, like the victim who works on civil liability, are powerless. Liability for harm is one such mechanism that can pressure companies to minimize harm. As it stands, it isn't a guarantee in privacy laws. But it should be.

For liability to be effective, laws must allow people to sue when there's informational exploitation. These situations include data practices and data breaches that produce privacy harm or other data harms, such as financial and reputational. This

change would produce enormous long-term consequences for corporate accountability and people's redress.

Outcome-based liability can work under individual or collective claims and under negligence or no-fault (strict) liability. Liability is most effective under forms of collective redress such as class actions because privacy claims are often individually small and widely dispersed. For consequential harms, the most effective basis for liability is no-fault, as the likelihood and magnitude of harm depends on the actions of corporations that collect, process, and share information, rather than users. When it comes to privacy harm, one should require intention for data practices and negligence for data security. Liability for privacy harm is most effective if it covers unintended and unforeseeable harm when those requirements are fulfilled.

A HARM-BASED PRIVACY LIABILITY

Equifax had a similar problem to Desjardins'. In 2017, a data breach led to 147 million taxpayers' financial information held by the company to fall into the hands of unknown recipients.[5] This breach caused privacy harm to millions of people, as well as an indiscernible amount of financial harm, largely to accrue in the future to an unknown subset of those people. In a settlement with the FTC and the US Consumer Financial Protection Bureau, the company agreed to pay up to $425 million, which is less than $3 per victim.[6] The Equifax breach was an enforcement action, not a lawsuit. But, leaving millions of victims undercompensated and the company underincentivized to avoid data breaches in the future, it illustrates the importance of having accountability tied to harm.

Equifax illustrates the privacy harms in data breaches to be countered by the protection of personal data: public exposure of personal details, insecurity as to who knows what about one, and being instrumentalized by an entity that chose to slack on security for data that creates profit for it and risks for others. It also highlights the problems of determining compensation without a viable harm framework. Further, the case underscores the unsuitability of the contracts model to structure needed duties not to harm, as these duties must go beyond the corporations with whom we have agreements. Privacy and data security have historically been dealt with separately. By treating them together when it comes to harm, one can get to the root of informational exploitation.

Legal Pathways

Liability can be brought through three legal pathways. First, when a data practice breaches a privacy or data protection statute (for example, breaching someone's right to know). Second, through a violation of data security law (for example, failing to notify a data breach). Third, through privacy torts in common law jurisdictions or the law of obligations in civil law jurisdictions (for example, intrusion upon seclusion). These legal pathways aren't mutually exclusive.

The GDPR and some US privacy laws give rise to the first legal pathway: private rights of action when a statute is breached.[7] These statutory violations, which occur during a corporation's ordinary course of business, are often data misuse, but they can also be wrongful collection or sharing. In these "business as usual" situations, a corporation knows how it collects, uses, and shares the data. Recent examples of their application are lawsuits against Clearview AI for building one of the largest facial recognition databases in history,[8] against Zoom for allegedly sharing data with Facebook,[9] and against Facebook for tracking its users' location without their consent when they turned off their location history.[10]

The right to sue for privacy is largely absent in US federal law.[11] Some federal laws contemplate it.[12] But the Supreme Court gutted federal law's ability to provide redress in the TransUnion case, shifting the responsibility of doing so onto state laws and state courts.[13] Comprehensive private rights of action, while available in many sector-specific state laws, are absent from all state data protection statutes passed to date: California, Colorado, Connecticut, Utah, and Virginia.[14] In California, they exist in limited form, available in case of a data breach caused by unreasonable security practices.[15]

In Europe, the Court of Justice of the EU ruled on the importance of private enforcement for data protection before the GDPR. The court said that the right to remedy data protection infringements is part of the fundamental right to a judicial remedy.[16] The GDPR stipulates private rights of action, contemplating the possibility of people initiating actions to obtain redress for material and immaterial harm.[17] The GDPR's private right of actions clauses improve the previous system, where some countries (for example, Greece and the UK) allowed for compensation for moral damage, while others (for example, Germany) only allowed compensation for material (called "pecuniary") loss.[18] Material harm tracks to what I call "consequential harms," and immaterial harm tracks to what I call "privacy harm."[19]

EU cases based solely on statutory privacy are infrequent. In theory, the GDPR has a private rights of action system that the US lacks. In practice, the primary method of enforcement is still public, carried out by national data protection authorities.[20] More importantly, the provisions are limited to statutory breaches, which replicates for liability the disjuncture between procedural rules and harm that many regulations have.[21]

In many countries that model their data protection laws after Europe, laws make it difficult for people to bring statutory privacy claims. For example, in Canada, one must first file a claim to the Office of the Privacy Commissioner, wait for the office to investigate and release a report, and then start a new application in court.[22] A few jurisdictions have comprehensive and directly applicable private rights of action.[23] The GDPR provides a template: private rights of action cases stemming from GDPR breaches don't need a prior declaration from a data protection authority.[24]

Data breaches, the second legal pathway, are different. Data breaches involve malicious actors. Corporations are often unaware of who accessed the data, what specific

data was compromised, and what the intruder's intentions are. Their difference from a corporate perspective matters for deterrence, as a corporation gains nothing from a breach itself; it gains in cost savings on security measures that increase its likelihood. From victims' perspective, the outcomes are the same: they gave their data to a party who was a poor custodian and faced privacy loss (possibly privacy harm) as a result.

Data breach claims often arise from hacks, but they also come from breaches produced by insiders, whistleblowers, or disseminators.[25] For example, they can arise from employees stealing data or misplacing physical devices. Most commonly, data breach claims arise when a company has insufficient protections against hacking in violation of a cybersecurity statute or fails to meet its duties to notify individuals affected by a data breach.[26]

The CCPA creates a private right of action for violations of the statute related to data breaches, giving consumers some ability to bring a lawsuit.[27] As a result, claims from data breaches have been brought forward in California.[28] The GDPR (as well as the CCPA) makes breach notifications to affected individuals mandatory.[29]

Tort law is the third legal pathway that can trigger a privacy claim. One recent example is Perrin Davis' claim against Facebook. Representing a group of users, Davis sued Facebook for collecting those users' personal data after they logged off. The court held that the plaintiffs showed harm to privacy interests and therefore established a sufficient claim for relief.[30]

In the US, the common law privacy tort has four facets: appropriation of one's name, image, or likeness; false light; intrusion upon seclusion; and public disclosure of private facts.[31] Appropriation protects people from others using their name and picture for commercial purposes. False light is implicated when someone uses true facts to create a false impression. Intrusion upon seclusion is what Perrin Davis established. It protects people from anyone who deploys intrusive means to obtain information about them. Public disclosure of private facts protects people from anyone who publishes intimate facts about them.[32] Intrusion upon seclusion and public disclosure of private facts most directly connect to privacy losses, as discussed in the last chapter.[33] Intrusion and disclosure claims have helpfully expanded since privacy torts were originally formulated.[34] However, because successful claims against companies based solely on privacy torts are infrequent, scholars consider that, in their current state, they're ill-equipped to address harms to privacy in the information economy.[35] Likewise, there's little court precedent on use of privacy torts for corporate privacy harm in the EU absent a GDPR violation.[36]

Privacy torts can be used as support in claims for violation of a privacy statute, merging two pathways. Tort-and-statute-based privacy claims are possible when a breach of a privacy statute is also a privacy tort. Local tort law has been successfully used to secure redress for data practices that fall under a tort and a statute by channeling victims' harm under traditional causes of action.[37] In the US, courts sometimes refer to privacy torts to assess whether someone suing under a privacy statute was sufficiently affected.[38] In some EU countries, privacy claims pairing

tort law with GDPR violations have been successful, such as in Germany and the Netherlands – including for nonpecuniary damages.[39]

A New Private Right of Action

Incorporating liability for privacy harm can be achieved by creating a separate private right of action in privacy laws. This would be functionally similar to a statutory privacy tort applicable to corporations in the information economy. It would create a new standard that merges privacy's legal pathways, allowing for a more effective way of holding corporations accountable.

The British case *Vidal-Hall* on browser data is an example of what private rights of action based on the consequences of data practices can look like. Judith Vidal-Hall and two others sued Google for collecting their Safari browser information through cookies without their knowledge, aggregating it, and using it for advertising.[40] They claimed damages for anxiety and distress without claiming financial loss. The court granted their claim based on their fundamental right to an effective remedy.[41] The court argued that, because data protection law chiefly protects people's privacy and not their financial interests, "it would be strange if the Directive could not compensate those individuals whose data privacy had been invaded by a data controller so as to cause them emotional distress (but not pecuniary damage)."[42] The case recognized misuse of personal information as a tort in the UK, allowing people to recover damages for nonpecuniary losses by combining this new tort and British data protection law.[43] The case fits one way to categorize intrinsic privacy harm discussed in the last chapter: emotional harm suffered by a reasonable person.

The centrality of intrinsic harm extends outside the UK. In Canada, for example, Deborah Douez sued Facebook for using her name and profile picture without her knowledge under "sponsored stories" to advertise products to her friends and others. The Supreme Court ruled that "the legislature's creation of a statutory privacy tort that can be established without proof of damages reflects the legislature's intention to encourage access to justice for such claims."[44] By "without proof of damages," the court meant without consequential harm.

Privacy law can likewise learn from cybersecurity law. Data security law has benefited from being built on principles, embodied in flexible standards that operate after the fact, which work as an accountability mechanism.[45] The duties contained in American data security law form an overarching rule of reasonableness.[46] The last twenty years have seen individual and collective cases of people suing when companies failed to implement adequate data security leading to a breach.[47] US law provides a corporate duty to provide security for the data that corporations hold and profit from, which William McGeveran calls "data custodians."[48]

The common harm of informational exploitation shows that this duty should cross over between data security and privacy law. Protection from exploitation warrants a duty that crosses doctrinal areas on the basis of the special relationship of

profiting from people's data while exposing them to harm. By adopting a similar standard, making corporations responsible for protecting personal data, privacy law can provide accountability.

The standards approach to liability that has been applied to data security law's private rights of action is also characteristic of privacy torts. It ought to be expanded to include other ways of inflicting privacy harm. Currently, this approach is missing from privacy and data protection law, as they fail to contemplate material and immaterial harm that happens absent a breach of procedural rules.[49] It should apply to situations where there's informational exploitation regardless of whether a specific interaction is covered by privacy law, cybersecurity law, or tort law. In situations where the offending party has more information, holding them to a standard that accounts for what they know and should know makes sense. The broadening of this standard, creating a duty not to exploit people for profit based on their personal information, would fit the common risks that are created by companies holding people's data for profit in the information economy.[50]

In an ideal world, the importance of outcome-based accountability for privacy protection would lead to expanding redress for privacy harms. Under current law, countless hurdles prevent people from obtaining redress.[51] These hurdles are the absence of private rights of action, strict requirements to sue when the right exists, and narrow material compensation.[52] The hurdles are connected by only consequential harm being considered. The uncompensated harms from Desjardins and Equifax, among hundreds of others, show the insufficiency of the current system to compensate victims or deter harm. By contrast, *Vidal Hall* highlights how courts can evaluate what constitutes an inappropriate degree of immaterial harm caused by a privacy intrusion to ground redress moving past the privacy fallacy. It provides a starting point for a standard that considers privacy harm.

Improving Existing Law Absent a Standard

Absent this proposed standard, laws could improve outcome-based accountability with two changes. First, they should provide a comprehensive private right of action for breach of statute. They should clarify, though, that the right to sue doesn't hinge on material, consequential harm, helping overcome questions of legislative intent.[53] An explicit private right of action of this type exists in the GDPR and many data protection laws outside Europe, such as in Argentina, Brazil, Singapore, and Canadian provinces.[54]

Second, statutes should make an explicit choice against preclusion. Statutes should make explicit that they don't preclude other lawsuits, such as through local tort law.[55] They should likewise make explicit that they don't preempt more specific statutes that may provide a better standard. In many jurisdictions, the extent to which publicly enforced laws preclude people from suing based on privacy torts is unclear.[56] When conduct is regulated by a privacy statute and falls under privacy

torts without breaching the statute, there's not always case law establishing that the tort suffices. Likewise, privacy activists in the US are concerned that an eventual federal bill that preempts state laws may reduce protection.[57]

Courts can better capture privacy harm absent legislative reform in several ways. In line with the proposed legislative change, courts can and should interpret existing privacy laws as not precluding tort law claims, integrating tort law as a complement to statutory privacy.[58] In the UK, for example, the Vidal Hall court ruled that, besides falling under data protection regulations, Google's misuse of information was also a tort.[59] UK courts generally allow private rights of action without them being precluded by British data protection law.[60]

For any form of liability to be effective, courts can't allow for consent provisions to curtail liability, such as by restricting forms of recoverable harm, arbitration clauses, or forum selection clauses. Currently, corporations rely on terms and conditions to limit their liability. Reducing informational exploitation requires ensuring that corporations can't use people's extracted agreement to limit their responsibility for harms generated by misuse or leakage of data.

Courts can expand privacy torts to adjust them to the current social and economic reality.[61] They can do so by building on the notion of probabilistic privacy losses. Courts can expand intrusion upon seclusion by considering that a privacy intrusion falls under the tort if it's offensive to a reasonable person, as opposed to highly offensive.[62] When Naomi Campbell was photographed leaving a rehabilitation clinic, modern English cases did away with the "highly offensive" requirement common in Australia, Canada, and the US, which inappropriately narrows privacy tort law.[63] The resulting reasonable person standard is a better fit with how social norms define the contours of privacy's social value.[64] Courts can likewise expand public disclosure of private facts by relaxing the requirement that the information is published, including situations where information is harmfully shared with a few people, expanding the information's audience. Common law courts, occasionally, can even create new torts that align with tort law's normative values.[65] Courts in Canada and New Zealand did so as late as the 2000s by developing a general privacy tort.[66] Identifying the type of probabilistic privacy loss that relates more closely to each tort facilitates expanding them so they can adapt to technological change.[67]

Courts can likewise expand torts related to privacy, such as breach of confidentiality.[68] Breach of confidentiality relates to breaches of trust, which scholars identify as an element of privacy invasions.[69] Trust encourages us to share information with others and, when people inappropriately reveal it to third parties, they breach our trust.[70] In the common law, breach of confidence requires misusing information to another person's detriment.[71] Detriment includes the "emotional or psychological distress that would result from the disclosure of intimate information."[72] A categorization of privacy harm as emotional harm suffered by a reasonable person can help ground this expansion. This tort fits doctrinally and normatively with inappropriate data sharing, and it may be possible to expand it to insufficient security leading to a breach.[73]

Most importantly, courts can and should focus on privacy harm, rather than consequential harms, produced by data practices that breach statutory rules or privacy policies, – that is, taking the opposite direction of the US Supreme Court in the TransUnion case. The GDPR has variable success on this front. Almost all cases stem from tangible, consequential data harms – which the GDPR calls material. Immaterial harm, such as privacy harm, received little recognition in private sector litigation, mostly in Austria, Germany, Portugal, and The Netherlands.[74] British small claims courts have also incorporated it, particularly for information collected absent a lawful basis.[75] Doing so is essential for capturing inferences, as illustrated by the cases of wrongly collected partial credit card information discussed in a previous chapter.[76] By dismissing privacy harm based on isolated data points, courts divest people of protection from inferential harm.

An Illustration: Grindr's Oversharing

In 2021, Grindr faced a historic fine for selling its users' personal information to third parties, which included sexual orientation and HIV status – an investigation mentioned in a prior chapter.[77] As a defense, Grindr's lawyers argued that "sexual orientation, a specially protected category of data, wasn't exposed by selling its users' data, since some of them may be straight."[78] In other words, because not every man who has sex with a man identifies as gay, they argued that exposing those who were considering having sex with a man they may find on Grindr didn't reveal their sexual orientation. A stretch, to say the least.

Examining Grindr's argument through the lens of probabilistic privacy loss explains why the argument is misleading. While having a Grindr account certainly doesn't provide conclusive evidence of sexual orientation (rather, only of potential interest in a sexual activity), it profoundly matters probabilistically. Someone with a Grindr account is more likely to be LGBTQ than someone without one. So every Grindr user who had their information shared with third parties faced a statistical privacy loss about their sexual orientation to those third parties. Grindr's argument is incorrect because people don't lose privacy only when someone produces conclusive evidence about them: their loss of privacy is probabilistic because privacy isn't binary. Probabilistic beliefs affect privacy because probabilistic knowledge (such as improving estimations of whether someone is likely LGBTQ) is also knowledge.[79] Information inferred probabilistically is both powerfully privacy-eroding and highly profitable.

Users' privacy loss, coupled with a GDPR breach, is sufficient for a data protection authority to sanction the company. What would happen if users sued can follow two of the three pathways.

One path courts could take is basing liability on statutory breach. This option makes courts enforce the regulation like data protection agencies do, and it makes Grindr's responsibility dependent on a procedural breach. Under laws that make

individual agreement a legitimizing basis for data practices, the company's liability then becomes largely dependent on whether it collected agreement from its users. The Norwegian authority considered that Grindr didn't, but it easily could have gone the other way. For example, according to some sources, the company has been selling user information since 2017 based on those agreements without regulatory authorities objecting to it.[80]

The second path is tort law. However, none of the common law privacy torts as currently considered apply to these users. Public disclosure of private facts requires publishing the information to the public, not just selling it. The tort, as currently interpreted, can't adequately deal with the problems of the information economy. If users sued in Norway, the civil code has a provision that protects private life, but it would be challenging to argue it in court if the data practice falls under the GDPR and a GDPR violation is absent.[81]

A better alternative is to make liability dependent on the harm that the company caused through a new-found standard. If users sued under this standard, for example in a class action, they would have to show privacy loss and privacy harm. Having established statistical loss, privacy harm requires interference with privacy's social value.

Grindr users who had their sexuality and HIV status shared had their intimacy violated. The type of information shared (sexuality and HIV status) required confidentiality that the company didn't keep – particularly considering that many users live in countries where the information could put them in physical danger. Most Grindr users share their sexuality with other users. In doing so, inadvertently or not, they also share such information with the app. But the reason for users to share information with each other doesn't extend to the app, and much less to third parties. Privacy interactions involve building relationships of trust, and some level of social trust is implied when sharing sensitive information with other people on dating apps.[82] Users choose with whom to share their information and with whom to interact based on the information the other users share – a reflection of reciprocity discussed earlier in the book that the company exploited when it shared that information with third parties.[83]

The company's decision to share the information with third parties harmed its users' privacy. It affected their intimacy, contravened social expectations, inhibited trust, and obstructed communications that LGBTQ people may want to have with each other.[84] Courts should acknowledge the consequential data harms that these users may have faced, such as reputational and discriminatory harm. But these harms are difficult to prove and they vary from user to user. To provide systemic protection, the law must remedy Grindr's informational exploitation, which all users whose information was illegitimately disclosed shared.

* * *

The law would improve protection and internal coherence by focusing accountability on the consequences of data practices, rather than its methods. One way to do so is with a new legal standard that imposes civil liability for privacy harm. Once a private right of action based on privacy harm standard is established, the next question to address is what liability covers.

B THE BASIS FOR PRIVACY LIABILITY

A question raised by realities such as Equifax's data breach and Grindr's data misuse is which basis for liability works better for privacy: negligence or no-fault. Negligence allows companies to engage in data practices without incurring liability as long as they comply with a certain level of care. Under no-fault liability, they can't: people can recover damages for data practices that caused them harm regardless of whether fault was involved. Given the social and economic factors underlying the information economy, the most suitable basis depends on whether the harm is a consequential data harm or privacy harm, and on whether the harmful activity is data misuse (like Grindr's) or a data breach (like Equifax's).

Statutory No-fault Liability for Consequential Harms

To determine the most effective basis for liability, considering who can minimize the likelihood and magnitude of harm is crucial. Effective liability regimes deter harm by placing responsibility on those who can prevent or mitigate it.[85] The likelihood and magnitude of harm chiefly depend on two factors: levels of care and levels of activity. The level of activity refers to how much of the potentially risky behavior one engages in, such as the number of hours spent driving. The level of care refers to how much effort one puts into preventing harm, such as driving carefully. For data harms, "level of activity" is the amount of data collection, processing, and sharing. "Level of care" is corporate efforts to prevent data misuse, such as how the information is used and shared, and to prevent data breaches, such as effective security measures.

Liability has a trade-off when it comes to its ability to deter. Negligence doesn't encourage adequate levels of activity from perpetrators, while no-fault liability doesn't encourage adequate care or activity from victims.[86] In other words, negligence incentivizes both parties to act with an adequate level of care, but not necessarily an adequate level of activity, while no-fault liability incentivizes perpetrators to act with an adequate level of care and activity, but not necessarily victims.[87]

Which liability basis is most appropriate given that tradeoff depends on the type of harm. It depends on whether its likelihood and magnitude are equally determined by both perpetrators' and victims' behavior or mostly by one of them.[88] Imagine a factory that emits pollutants into a river every month where the owner knows they won't be liable because they satisfy requirements to keep contamination

at a specified level per unit of production (level of care). Why would they try to reduce them further? On the other hand, under no-fault liability, perpetrators must remedy harm no matter how it took place. Perpetrators are more likely to reduce harm under no-fault liability than under negligence, where only under certain circumstances they're held responsible for the harm.[89] No-fault liability better reduces harm in cases like this one, when perpetrators can control the probability and magnitude of harm better than victims can.[90] This incentive-aligning happens because no-fault liability turns the externalities that perpetrators can impose on victims into a cost for those perpetrators.[91] The right type of liability for the factory would be no-fault.

The factory situation is unusual. For example, looking both ways when crossing the street helps us prevent being hit by a car, even if we only cross when the light is green. In Montreal, where I live, walking carefully over the icy sidewalks in winter helps us not slip when the city and homeowners fail to de-ice them properly. When biking, watching for cars opening their doors and wearing a helmet reduces our chances of getting injured. In these situations, victims can mitigate the amount of harm by taking precautions. Accordingly, they're governed by negligence.

The prevention of data harms is dissimilar. They're closer to the factory that produces pollution harm with a probability that people living next to the river can't affect. Data harms are different from most others because victims can't prevent them from happening by taking precautions. People can't control the probability or size of harms stemming from data practices that companies choose.[92] Similarly, self-protection measures after data are disclosed have a negligible influence on the likelihood and magnitude of data breaches compared with the security measures that companies can implement.[93] Corporations have control over how they use and how they protect people's personal information.[94] Only they can significantly change the likelihood and magnitude of data harms, for example through types of processing and level of database security.[95] Negligence's benefit of optimizing victims' behavior isn't helpful for data harms because these harms depend on corporate data practices much more than on anything people can do.

Further, both the levels of care and activity of corporations determine the likelihood and magnitude of data harms, making it important for liability to capture both. As the amount of financial data collected by any company rises, so does the risk of fraud.[96] For example, the risk of social security numbers being leaked depends on third parties' and data brokers' data practices.[97] As Chris Hoofnagle explains, "[t]he relationship is so asymmetric that the individual is literally at the mercy of the risk preferences of companies with which no relationship has even been established."[98] The amount of data collection and number of data transfers (activity levels) affect the likelihood of those whose information they hold being harmed – and the magnitude to which they are. Far from the costs of activity levels being fully internalized, for some consequential harms, such as financial harms stemming from identity theft, corporate costs from data harms are socialized. For

example, in the US, banks can write down losses from fraud against taxes. So the amount of identity theft for its clients that a business decides to tolerate is subsidized by taxpayers.

No-fault liability may do more than deter. It may provide incentives for companies to prioritize data protection and improve security measures, ultimately reducing data harm, in a context where they know how to do it better than regulators do.[99] A no-fault liability regime puts the economic onus of profitable activities on those that profit from and understand data and security practices. No-fault liability incentivizes companies to prioritize data protection and implement measures to reduce harm that are compatible with their business models.[100] For data practices, it provides incentives for appropriate privacy measures to be built into products' design.

No-fault liability has an additional advantage: the cost of searching for the optimal level of care is taken by the entity with most information about it. In the information economy, where there's an information imbalance between injurers and injured parties, injurers have a better understanding of the activity that can cause harm and the precautions needed to prevent it.[101] No-fault responds to information asymmetries between companies and regulators or courts on risk-reduction dependent on each technology and business model. Relieving difficult-to-meet proof of fault in a context of no information also makes recovery more feasible, reducing the uncertainty of engaging with the information economy.[102] It removes the onus, significant under privacy's moral hazard, for people to monitor data practices that comply with negligence to know when they can sue.

An objection to no-fault liability is that it might overdeter valuable data practices.[103] No-fault liability is appropriate when an activity has expected harm and the company internalizes all benefits. According to the objection, data practices often produce little harm and they benefit many people. The objection is mistaken in two ways. If it's true that data practices create little harm, the cost of no-fault liability would be low.[104] Further, as long as companies internalize benefits, no-fault liability doesn't overdeter, absent punitive damages, because it merely internalizes harm, concentrating data practices' costs and benefits in one party.[105] Socially valuable activities are compatible with no-fault liability for harm.[106] The only data practices that would shut down under no-fault liability would be those that produce more harm than profit. The objection is correct in one way. Some data practices have social benefits that companies don't capture. Most of these, although not all, exist outside the information economy, which is the focus of this analysis – companies in the information economy are successful at internalizing benefits through data-driven profit.[107] To capture all others, courts can introduce an exception to no-fault liability for socially beneficial data uses and sharing, which Yafit Lev-Aretz refers to as "data philanthropy."[108] Laws (and courts) can establish burden of proof of demonstrating data philanthropy that moves a corporate data practice from no-fault liability to negligence, avoiding overdeterrence.

Tortious Strict Liability

No-fault liability for consequential harms can be achieved through tort law with the doctrine of strict liability. Strict liability holds a person or entity responsible for any harm they cause. In common law jurisdictions, strict liability is typically applied to inherently dangerous activities and products liability. The rationale for inherently dangerous activities is based on principle, while the argument for defective products is based on incentivizing appropriate precautions. Both rationales apply to data practices.

The head of the legal department of an airline once told me: "the question isn't who's going to be hacked; the question is when each company will get hacked." Collecting and holding enormous amounts of personal data invites security breaches.[109] So the principle-driven argument for strict liability applies to the consequential harms of corporate data practices and data breaches. Tort law uses strict liability for inherently dangerous activities or things, such as storing fireworks or owning wild animals. Those cases share an understanding that perpetrators do something inevitably dangerous, though not necessarily wrongful. The inevitability of data breaches justifies applying the doctrine of strict liability for abnormally dangerous activities because it makes data practices an inherently dangerous activity.[110] The inevitability of data harm and corporations' knowledge advantage extends to deliberate data practices.[111] Similar to dangerous activities, the harm that results from data practices and breaches is potentially severe. It affects people's personal and professional lives daily.

Traditional strict liability doctrine provides a related analogy. The doctrine is that someone who brings and keeps in their property anything that's likely to do a mischief if it escapes must pay for all damage produced by its escape – such as a flood.[112] This doctrine can and should be applied to situations beyond physical property. The high-risk and high-profit nature of "cyber-reservoirs" – where security breaches are inevitable and where data leaks cause profound, widespread damages – lends itself to strict liability.[113] People whose data are leaked aren't unlike those whose land is flooded: they're victims of an event outside their control and for which they couldn't have been expected to prepare. Addressing the constant and inevitable risk of data harm with strict liability ensures a remedy.

Another form of well-recognized strict liability is products liability. Products liability has a strict liability regime because manufacturers have more control over the safety of their products than consumers do, so manufacturers' behavior is what's most important to regulate through liability. It establishes solidary liability (also called joint and several) for the supply chain because it would be difficult for consumers to identify which part of the supply chain caused the harm and sue entities they haven't interacted with. Data are analogous to these products in both dimensions.[114] Data misuses and hacks are vexing incidents that victims can't predict well; corporations have a better understanding of what they do with data and how much

security they put in place. For data breaches, corporations could attempt recovery from hackers after compensating victims, as they're in a better position to do so than victims are.

Products liability's reasoning tracks with policy arguments in favor of no-fault liability, allowing courts to better achieve tort law's aims to compensate victims and deter harmful behavior. Providing redress without having to prove corporations' negligence internalizes the costs of data practices.[115] Strict liability for data harms doesn't create significant risk of reckless victim behavior. Even if there were a risk of people misbehaving under strict liability because they could be compensated for any harm (there isn't), that risk would be lower than the risk of having companies misbehave because they have limited liability for their products' harm – both in products liability and data harms.[116]

Profit matters as well as principle and policy. In other areas of law, such as environmental law, the argument that the polluter should be strictly liable is made on the basis that they benefit from their polluting undertaking.[117] For-profit data practices and profitable lack of data security fall under this consideration. Strict liability doesn't imply that collecting, processing, or sharing data is wrongful. It just concentrates risks and benefits of an activity on the same entity.

Tortious strict liability, like statutory no-fault liability, responds to information asymmetries. It simplifies liability analyses by removing the need to determine fault.[118] Negligence introduces problems for data security because the correct level of due care may be uncertain.[119] In data breaches such as Desjardins' and Equifax's, it can be challenging for courts and victims to determine whether companies were negligent. In corporate data practices, determining fault is even more difficult given the context-dependence of precautions. For instance, it may be unclear for outsiders whether it was risky for a company to share certain data.

A strict liability regime for data harms stemming from data practices and data breaches would induce appropriate levels of care and activity more effectively than would negligence. It would force companies to consider the risks they create while profiting from people's data, incentivizing corporations to reduce harm, rather than on finding the level of care to get away with it. The alternative to strict liability is that victims bear the harms of data practices that they didn't choose, they couldn't anticipate, and they didn't profit from, when neither they nor companies behaved negligently. That's what's truly strict.

Intentional and Negligence Liability for Privacy Harm

Privacy harm is also closer to pollution from a factory than to a car accident. It's ubiquitous and inescapable, for example with mass facial recognition. It's mostly harmful in aggregation, such as when inferences are made. And its systemic aspects are invisible.[120] As discussed in a previous chapter, informational exploitation and data harms often occur as a result of the abuse of permitted activities.[121] Perfect

compliance with procedural rules wouldn't eradicate all harms.[122] Victims can't do much to prevent or mitigate it either.

Exploitative data practices require intention (or recklessness) over the data collection, processing, or sharing. Although the behavior itself must be intentional or reckless, the outcome doesn't need to be.[123] This framing makes it consistent with privacy tort law and other information torts.[124] Damages for defamation, for example, amount to liability for the outcomes of publishing false information, even though the act of publishing false material is intentional or negligent: damages are not capped at how much reputational harm the wrongdoer tried to inflict.[125] Intentional infliction of emotional distress requires intention for the distress-inflicting behavior, but produces liability for its consequences because damages aren't capped if a victim is distressed more than a wrongdoer could foresee.[126] The requirement would broadly increase consistency between what we require from each other through tort law and what we require from corporations through statutory privacy and security law.

Exploitation through lack of data security requires, instead, negligence over the security measures that led to a breach. This form of negligence works best as a standard of best industry practices, consistent with the standard many jurisdictions follow for data harms. Absorbing industry best practices to inform standards when creating legal duties has been effective in countless areas of the law, and seems to be emerging in US data security law.[127] For data security's negligence basis, courts should shift the burden of proof to defendants. Corporations being sued for privacy harm would have to provide evidence of their security measures, as they have better information than victims or courts about them.

Data security outcomes that weren't foreseeable while engaging in exploitation should likewise be included. This distinction follows the difference between excuses and justifications in private law. One uses excuses when one did something that didn't meet a standard of conduct, but one shouldn't be blamed for all its consequences.[128] One uses justifications to say that one's behavior met the standard of conduct, even if it caused harm.[129] Considering informational exploitation, data security law should accept justifications, but not excuses. It should have a standard of sufficient measures to exempt hacked companies from responsibility for privacy harm, but not free them from responding for consequences they couldn't anticipate that resulted from wrongful behavior. Not taking excuses increases consistency between data security law and privacy tort law, which is fitting for the harms they share.

An adherent of the traditionalist paradigm would object to this line of argument. They may say that there's inherent risk to having your personal information online, so it's unfair to place the risk on corporations and not the people who use a service. Corporations would argue that some risks from digitized data should be borne by users. Why shouldn't one think of privacy harms as risks people accept in exchange for services? The answer is the unknowability of the risks involved discussed earlier in the book.[130]

Incentive-setting is crucial to curbing informational exploitation. Companies taking security into consideration from the beginning, and how they should do the same with privacy, is at the core of modern accountability proposals such as privacy by design and information fiduciaries. Further, the fairness theory of tort law justifies the proposed approach. It stipulates that corporations should compensate individuals fully whenever they engage in profitable activities that are risky for others for which those others don't derive the same amount of benefit as the corporation.[131] Privacy harm falls in this scenario.[132]

Since the 90s, corporate accountability has expanded in various areas of the law to increasingly hold corporations responsible for types of harm they create and were previously unaccountable for, including health hazards and environmental harm.[133] Under current laws (and with current courts), similar liability claims for intangible privacy harm would be mostly unsuccessful. The hope is that, with a fuller notion of the pervasive immaterial harms that the information economy creates, this dissonance among legal areas may eventually subside.

Mixed Private–Public Enforcement

In 2022, the Director of the Federation of German Consumer Organizations, Jutta Gurkmann, stated in response to a case against Meta: "It is no secret that some European data protection authorities have difficulties to combat the rampant data collection by big technology companies. In the past, the lack of enforcement has increasingly weakened the acceptance of the GDPR."[134]

Enforcement is necessary for any privacy or data protection legislation to be effective.[135] The EU has been successful at converging public and private enforcement to the benefit of individuals by having neither of them depend on the other.[136] Enforcement would work better yet if private and public enforcement shifted to increase complementarity.

Both public and private enforcement mechanisms are needed in practice to overcome the information and power asymmetries that exist in data collection, processing, and sharing.[137] Lawsuits allow individuals to have a say about which cases are brought, bring out facts about blameworthy security practices, and provide redress to victims while acting as a deterrent against rule-breaches.[138] Lawsuits can be a bigger deterrent than administrative fines if compensation is estimated adequately, particularly in jurisdictions without large fines.[139] Private rights of action alleviate regulatory burden on administrative agencies, reduce the risk of agency capture, and pressure companies to comply with the law.[140] This dynamic has been called hybrid enforcement.

Mixed public–private enforcement, where liability is based on a harm standard, would go a step further. In existing hybrid enforcement systems, private rights of action and public enforcement both sanction breaches of data protection rules. Mixed enforcement departs from them because it doesn't add public and private

enforcement to statutory violations. Instead, the two mechanisms take different roles. It avoids duplicated (private and public) damages for a single wrong and it covers gaps that hybrid enforcement doesn't cover: harmful behavior that complies with data protection law. Private enforcement based on a harm standard would maximally complement the proposed public enforcement focused on reducing systemic risk.[141]

Regulators and courts have different institutional advantages. Public enforcement is better positioned than courts to address systemic problems. If coupled with investigatory and sanctioning powers, public enforcement can address widely dispersed externalities and harms to public goods, such as the harms to democracy seen with Cambridge Analytica.[142] Public enforcement can take a proactive approach to risk that courts can't take. For example, regulatory proposals have suggested that the FTC should regulate the use of the word "free" when companies use it for monetizing our data and the use of "privacy policy" when no baseline protection is offered.[143] The court system can't appropriately deter widespread, systemic social risks, even with mechanisms of collective redress.[144] It's impossible, for example, to constitute a class for the harms to democracy of Cambridge Analytica.

Courts, on the other hand, can address harm to individuals or groups. Courts are better positioned than regulators to deter unpredictable harm. Governments don't always know how to effectively determine procedures made in advance, so it's productive to make (outcome-based) private enforcement align corporations' capacity to address risk with incentives for them to do so. Inevitable budget constraints, in addition, render it impossible for public enforcement authorities to investigate everything, making it wise for them to focus resources on aspects courts can't pick up.

Mixed enforcement responds to comparative asymmetric information.[145] There's an often-overlooked information problem in public–private enforcement dynamics. Because informational exploitation is difficult to detect, enforcers and victims necessarily have different types of information about different privacy violations. Consider cases of viral nonconsensual distribution of intimate images.[146] It's impossible for administrative agencies to detect when someone's pictures are plastered across websites. But at some point, victims may. Even if agencies found the images, it would be difficult for them to know whether they were shared without consent. The victim would know. Many instantiations of data harms are most salient to their victims.

The process of discovery is an information benefit of private rights of action. Fact-finding, in particular, often uncovers data practices that differ from what companies declared they do. It helps increase transparency for the public and for enforcing agencies.[147] Prohibited physical behavior, such as material dumping or driving with a broken light, can be seen by administrative officers. The outcomes of data practices, on the other hand, are opaque. Most of the time, we learn the details of how our personal information was being processed after harm occurs. This invisibility makes administrative sanctions for harm difficult to enforce.

A mixed enforcement system wouldn't be unique to privacy. It's common for administrative and tort law to be combined. For example, traffic authorities sanction individuals for driving with a broken light even if they didn't get into a car accident; and one can sue based on tort law when injured in a car accident even if the driver's lights were working.[148] Countless regulations don't rule out compensation when harm occurs absent a procedural violation. And they keep public enforcement when a risk-creating violation occurs without harm materializing. For example, the US Congress partially relies on private enforcement for public environmental law objectives.[149] While environmental law is far from perfect in addressing harms to the environment, it has consistently benefited from compatible public–private enforcement.[150]

Compatibility can be improved with minor legal reforms. In the US, courts interpreting privacy laws should make room for FTC sanctions for statutory breach while giving people a remedy for harm. In countries with similar data protection law to the GDPR, national tort law should complement data protection authorities' sanctioning power by operating independently of it, as it does in many parts of the EU. Similarly, enforcement authorities themselves would increase compatibility by focusing efforts and resources on prioritizing systemic aspects of their laws aimed at risk-reduction, such as privacy by design and data minimization, deprioritizing procedural aspects or individual control rights.

***

Privacy harm liability should include liability for all negative consequences of engaging in informational exploitation: profiting from an intentional or reckless data practice or a negligent lack of data security. The proposed harm-based standard with negligence or intention for privacy harm and strict liability for data harms can unify statutory privacy law (in Europe, data protection), tort law, and data security in curbing exploitation in the information economy. It would capture the main appeal of other popular accountability proposals, such as information fiduciaries and privacy by design.

C PROCEDURAL ASPECTS OF HARM-BASED PRIVACY LIABILITY

Imagine trying to sue Equifax or Desjardins individually, investing years and thousands of dollars to get a small amount in return. Litigation can be uncertain and expensive, and the recoverable amounts can be paltry. Low awards and infrequent lawsuits limit liability's power to constrain exploitation, like they did when Ford made the business decision to allow its Pinto cars to explode. Many who object to privacy liability argue that it's not worth bothering with. This common objection is the direct opposite of another common objection, discussed in the last chapter, of risking a flood of meritless lawsuits.[151]

The lack of incentives to sue problem requires a two-step institutional response. First, it requires legal actors to recognize privacy harm together with consequential data harms to develop better frameworks for evidence and compensation. Second, class actions, which group together similar harms experienced by several people, can address harms in the information economy, which frequently affect large groups of people. For most people, it's either impossible or impractical to litigate privacy harms individually. But a group can.

Evidence and Compensation

Think of Perrin Davis, who sued Facebook because it kept tracking him after he logged off.[152] Once the facts were established, the court didn't require Davis to prove reputational, financial, or discriminatory harm based on privacy torts. These harms aren't elements of the tort of intrusion upon seclusion because they aren't privacy values. They're other important social values that may be harmed when people's personal information is wrongfully collected, processed, or shared. The same value distinction applies to statutory privacy cases.

Privacy statutes can take elements from privacy torts to build a harm-based compensation system. Compensating immaterial harm has historically been an uphill battle in common law countries.[153] But, over time, immaterial harm started to be recognized. For example, many courts consider medical and psychological diagnoses as useful but not necessary for their recognition, compensating for sorrow and emotional distress.[154] Today, courts distinguish privacy torts from related torts, such as defamation, in one important way: privacy torts don't require the plaintiff to prove a consequential harm other than a harm to their privacy.[155] This evidentiary evaluation mirrors those of other torts. People must prove psychological harm in a claim of intentional infliction of emotional distress and must prove reputational harm in an action for defamation, but not financial or physical harm in either.

Privacy claims outside tort law shouldn't require an additional element either. Privacy harm isn't an intrinsic element of privacy torts. Rather, it's a characteristic of the privacy values that privacy torts protect. Like privacy torts, privacy laws protect privacy values by regulating data practices. To consider that a nonprivacy value must be violated to ground a legal action on a privacy statute implies misunderstanding the purpose of a privacy statute – to protect people's privacy. Requiring it mischaracterizes what harming privacy means.

Identifying relevant social values sheds light on evidence questions. Applying the proposed new standard in a statutory privacy case, courts shouldn't assume that privacy harm is present. Yet courts shouldn't require consequential harms. Instead, courts should examine whether there was a probabilistic privacy loss and determine whether the plaintiff's privacy loss is harmful. They can do so by examining whether the data practice that produced the privacy loss was appropriate or it constituted

informational exploitation.[156] Their determination should be guided by whether the loss violated privacy's values, like Grindr did.

Distinguishing between privacy loss and privacy harm, which is the cornerstone of the proposed liability regime, guides compensation. In these claims, courts should require evidence of informational exploitation by showing the intentional or negligent violation of the proposed standard, rather than relying on evidence of financial or physical harm. Although evidence rules differ jurisdiction to jurisdiction, courts can apply the local evidence requirements of either of the two doctrinal categories that align with intrinsic harm: those for emotional harm as suffered by a reasonable person or those for dignitary harm. By using these categories, courts can provide compensation in recognition that people's privacy warrants protection while avoiding damage awards that are disproportionate to their jurisdiction – and mitigating frivolous litigation.

Two factors can further inform the appropriate quantum of compensation. In quantum determinations, courts across jurisdictions should consider contextual factors that are relevant to the level of interference with social values: whether the privacy harm is intentional or negligent, whether it's severe, whether it's persistent or a one-time occurrence, and whether it was motivated by victims' identity or characteristics.[157] Although the precise quantum ranges will differ among jurisdictions, the doctrinal category under which privacy harm is considered would provide direction. They provide, at least, three avenues for estimating damages.

A first option is for each court to grant amounts they normally grant for emotional harm. For example, that would be the approach of British courts following *Vidal-Hall*. Courts recognize that emotional distress is sufficient to establish harm in nondigital contexts.[158] Common law courts have awarded as much as $100,000 for emotional distress claims.[159] Courts can also base compensation on other forms of intangible harm to which they're receptive, such as those for assault and battery.[160] Similarly, liability for failure to notify data breaches in the US, while specific in its cause of action, can include emotional distress – something not yet extended to other data breach compensations.[161]

A second option is for courts to grant amounts they normally grant for dignitary harm. For example, outside the information economy, the European Court of Human Rights developed case law on nonpecuniary harms for privacy claims against state actors.[162] The court, focused on the dignitary value of privacy rather than on material consequences, awarded dignity-based nonpecuniary damages with an average individual amount of €16,000 in about two-thirds of the cases where it found a privacy violation, in addition to other damages.[163]

A conservative third option is to establish a set amount of damages, either by statute or precedent.[164] For example, when the Court of Appeal of Ontario in Canada developed its privacy tort, it set individual damages for up to $20,000.[165] This amount may seem low, but it could pair with compensation for consequential harms. Absent evidence of consequential harms, it adds to build a deterrent effect if considered as part of a system of collective redress.

Group Privacy Harms

To delineate the scope of harm-based liability, one should distinguish between data practices (including the practice of establishing insufficient security) that harm groups and data practices that produce systemic effects, undifferentiated between all members of society. Doing so is correlative to focusing public enforcement on systemic (undifferentiated) effects to increase its effectiveness.

Legal systems usually require that harm is attributable to anyone seeking remedy before a court.[166] Privacy-reducing data practices where everyone in society faces their effects in an undifferentiated way are thus a bad candidate for lawsuits.[167] However, not all widespread privacy losses are undifferentiated. Many data practices harm a large group of people, sometimes by small amounts, in a way that they don't harm the general population. The task is to differentiate between systemic (privacy) effects, which produce undifferentiated privacy *losses*, and mass interferences with privacy values, which produce group privacy *harms*.[168]

Dismissing mass privacy harms as undifferentiated effects is inappropriate. Widespread harms are socially relevant precisely because they're pervasive.[169] The lack of a reliable way to distinguish between widespread privacy harms and undifferentiated effects leads to a two-sided problem. It makes it difficult for courts to consistently identify cases that warrant redress and makes it difficult for political actors to identify undifferentiated effects that will escape courts. Courts are well positioned to take on mass harms to compensate victims and deter harmful behavior.[170] Regulators are well positioned to address systemic effects, such as anti-privacy design, overcollection of data, and lack of algorithmic transparency.

In analogous areas of law, courts consider widespread harms in their determinations of the right to sue and compensation. In environmental law, courts recognize harm to people's environmental interests without separate physical or financial harm due to the enormous social interest in quality of life and the difficulties to provide individual proof.[171] Plaintiffs suing to protect the environment in the US sometimes do so on the basis that the harm is to an aesthetic or recreational interest that they hold.[172] The US Supreme Court has, for example, noted that "environmental well-being, like economic well-being, are important ingredients of the quality of life in our society, and the fact that particular environmental interests are shared by the many rather than the few doesn't make them less deserving of legal protection through the judicial process."[173] US courts have considered people's reasonable concerns about environmental degradation sufficient.[174] Similarly, some Canadian courts in environmental law cases deem proof of general harm to society, such as harm to the atmosphere, sufficient.[175] Those harms are more dispersed than mass privacy harms that are dismissed.

Environmental harm is analogous to algorithmic privacy harm.[176] Widespread privacy harm negatively affects people's well-being like environmental harm does.[177] Although privacy harm and environmental harm have countless differences, they're

similar regarding their pervasiveness, their importance for social life, their unpredictability for victims, and the difficulty in quantifying their long-term harm.[178] Leaving data practices that produce mass privacy harm unaddressed by writing them off as undifferentiated leaves large groups of victims uncompensated and fails to internalize significant social harm.

The enormity of social privacy interests and the difficulty in providing proof in a networked society are two significant challenges for privacy law.[179] Both challenges benefit from a notion of intrinsic privacy harm based on statistical information gains. A new standard fits this continuous view of privacy because standards allow the application of force proportional to the gravity of harm.[180] Consistent with a social norms analysis, such a standard can incorporate relevant contextual considerations such as the cost of precautions not taken and the type of information involved.[181]

Widespread harms aren't a bad candidate for redress. They're just procedurally challenging because, without adequate mechanisms in place, people have insufficient incentive to sue.[182]

The Importance of Collective Redress

The harms caused by corporations in the information economy often impact a large number of people. They often affect larger groups than the economic harms that the law is used to addressing. In individual interpersonal relations, most interferences with privacy happen when someone discloses the personal information of just one person to the wrong source or misuses the information of just one person. In the information economy, harm comes from the fact that corporations collect, process, and share personal information from many.

The lack of cost-efficient options to bring individual privacy claims disadvantages victims. Claims for mass privacy harms are worth little on an individual basis. In the US, for example, financial data harms litigated under federal law entitle people to recover between $100 and $1,000 per violation.[183] The hassle and expense of litigating meritorious causes doesn't always exceed their benefit. Even under the GDPR, cases have mostly reached small individual amounts.[184] Only grave data harms provide people with enough reason to individually go through a costly and lengthy judicial process. Only those who can afford it litigate harms that aren't debilitating. Individual private actions poorly address data harms that uniquely affect the most disadvantaged, such as unfair insurance premium increases or algorithmic discrimination in securing housing.

The lack of cost-efficient options to bring privacy claims presents a systemic problem too. Insufficient private enforcement is also ineffective at ensuring deterrence, since corporations aren't deterred from harmful data practices if liability is hypothetical.[185] Because of their low compensation coupled with the costs of litigation, private rights of action in privacy law work best as part of a mechanism of collective redress, such as class actions.

By aggregating similar individual actions, class actions increase the number and types of claims that can be litigated.[186] They reduce the legal cost for each individual, which improves affordability and therefore the number of meritorious victims who can bring claims. Collective mechanisms provide redress that would otherwise be unavailable to people who are harmed but can't afford litigation, either because of the cost of litigation or the low potential rewards. In most cases, lawyers are paid on a contingency fee basis with no upfront cost for class members.[187] Affordability is of particular importance in privacy claims, where success is uncertain and the remedy is likely to be low on a per-person basis. Class actions are additionally helpful for informational reasons. Individuals who are harmed may not have the resources or knowledge required to seek legal recourse in privacy.

Laws and courts across jurisdictions began to certify privacy class actions, both based on tort law and regulatory breaches. For example, when activist Max Schrems sued Facebook to prevent it from sending his data to the US, the Austrian Supreme Court ruled that claims based on the GDPR can be pursued through class actions.[188] Davis' lawsuit against Facebook, similarly, was a class action.[189]

Collective private rights of action in privacy and data security, however, so far fail on two fronts. First, they frequently fail to recognize harm required for people to sue, leaving victims' claims unrecognized.[190] Second, awards tend to be so low that they don't compensate victims, making individual litigation not worth the hassle.[191] This dynamic undermines their usefulness.

The first hurdle class actions need to overcome is adequate compensation. In the Equifax breach, compensation worked out, as previously mentioned, to $3 per victim. In Canada, a case that reviewed class actions found that the maximum individual payout was $500, with some of them being under $14.[192] When based on consequential harms alone, class actions may provide insufficient incentives to sue for meritorious claims. Those amounts may be sufficient for a mass harm class action, but they're insufficient to motivate small to medium groups. Consequential harms' causation problems partly drive those low amounts. These difficulties result from judicial skepticism over harm in privacy claims. Adequate compensation requires an added notion of privacy harm.

Growing privacy class actions numbers parallel prior developments in environmental law and competition law, where private rights of action now often manifest in collective redress. If the trend in privacy law continues, coupled with a recognition of privacy harm, class actions could change how people find redress in the information economy.

Why Privacy Claims Fit Class Actions

To increase access to justice, privacy class actions must overcome a double obstacle. Together with the difficulty in proving compensable harm (a difficulty from privacy

law), they must overcome the difficulty of obtaining class certification (a difficulty from civil procedure).

Class actions are often undermined because individuals in the group suffer different data harms that prevent courts from unifying their claims. This problem is caused by identifying only consequential data harms (or risk thereof), while neglecting privacy harm, which is the unifying element between class members. Information unjustly sold, released in a data breach, or misused is poised to have a similar effect on each user's privacy. It would be common that, in addition to that harm, a subset of victims suffer consequential harms. For example, some could be subjected to identity theft as a result of a data breach, but not all, as was the case with the Equifax breach. These consequential harms don't erase the privacy harm they have in common.

Intrinsic privacy harm provides identification over commonality needed to sue as a class. Recall the TransUnion case, where thousands of people were mistakenly flagged as terrorists. Their privacy loss caused consequential data harms for some of them in the form of reputational and financial harms.[193] What plaintiffs had in common was the privacy harm that TransUnion caused them.[194] That central commonality justifies their grouping in a class. The US Supreme Court failed to see this common element, noting that some but not all class members suffered reputational harm equivalent to defamation.[195] In the Equifax and Desjardins data breaches, focusing on consequential harms would undermine their grouping: some but not all victims had their credit card copied and their identities stolen.[196] Richard Lloyd lost against Google at the UK Supreme Court because the court failed to see any harm the 4 million users had in common.[197]

The loss and harm distinction similarly applies to distinguishing among groups of plaintiffs. It may be difficult to identify whether people share a privacy harm or they suffered different privacy harms, particularly when people are harmed in different magnitudes. But losing something by different magnitudes is dissimilar from suffering different harms. Privacy loss is the remaining piece of the puzzle, as a notion of privacy loss uncovers unifying aspects. Privacy loss is the cause of privacy and data harms that plaintiffs can claim. Identifying commonality through loss applies to both data breaches, such as the Equifax incident, and data practices, such as the TransUnion case. For example, class members in the TransUnion case shared an inferential privacy loss from TransUnion's mislabeling them as terrorists, based on their (unjustified) loss of control over their information.[198]

Certification requires a common privacy harm, rather than just a shared privacy loss that led to disjointed harms. However, a shared privacy loss resulting from the same data practice or breach should be seen as establishing a presumption that their harm is shared. For example, in the hypothetical Grindr class action discussed above, all class members suffered privacy harm resulting from the unauthorized disclosure of their information, in addition to different consequential harms.[199] They share this harm because they shared the unjustified loss that constituted it.

Traditional class actions address equivalent group harms linked by a single misbehavior, such as when the US National Football League was sued for failing to protect players against head injuries and when Volkswagen was sued for misrepresenting its diesel emissions.[200] Identifying shared privacy harm through a recognition of losses provides consistency in allowing people to sue as a group.

Collective action based on intrinsic privacy harm better responds to the reality of inferences.[201] Because synergies among collected data points from different people lead to harmful inferences, fragmenting redress into individual lawsuits leads to replicated efforts from plaintiffs, defendants, and the court system. Harms produced by probabilistic privacy losses due to relational data share this concern. Inferential and relational privacy harms (and data harms) are often group harms, so grouping their claims is more fitting than dividing them into individual actions.

In an ideal system, encouraging class actions would be coupled with a departure from the contractual paradigm. A consequence of such a departure is deeming any clauses compelling arbitration or forbidding claim aggregation as unenforceable. These clauses impede deserving compensation, thwart deterrence, and stifle the development of the law.[202]

Overcoming Objections through Representative Actions

There are two implementation concerns with privacy class actions. The first is that class actions can create a misalignment of incentives between lawyers and clients. Class action attorneys may prioritize quick settlements to obtain a contingency fee, rather than engaging in the private costs of a litigation process.[203] As a second concern, one might worry that class actions impose administrative burdens on people similar to those of individual control mechanisms.

Equipped with a notion of how to quantify intrinsic privacy harm, courts can moderate lawyer-client misalignment because it provides a basis to evaluate the reasonableness of settlement amounts. Courts can then reject settlements if they significantly undervalue their claim.[204] Absent that possibility, although this misalignment can result in lower than optimal settlement amounts, it's unclear whether class actions disadvantage any individual with the right to sue.[205] A class action mechanism with an incentive misalignment is worse than one without it, but it's better than having only individual actions – or no right to sue.

While class actions place some onus on people, the class action mechanism removes the onus of anticipation of harm and self-protection imposed by control mechanisms, such as data rights, and the lowered onus of individual action imposed by individual litigation. Further, if private rights of action depend on privacy harm, individuals who sue aren't reacting to an abstraction but to being unfairly disadvantaged, so liability would avoid much of the information-finding administrative burden on people that procedural rules impose. Moreover, this mechanism would better deter harm than existing ones. By improved deterrence, in the long term,

there may be less need for litigation than there currently is. This would further alleviate the burden.

These concerns are specific to class actions, not to all forms of collective redress. The GDPR provides an alternative form of collective redress through representative actions. These are opt-in collective redress, meaning that plaintiffs have to actively choose to join them.[206] For example, the Federation of German Consumer Organizations sued Facebook for how it hosts third-party apps and games in its App Center – the mechanism that led to the Cambridge Analytica scandal.

Representative actions brought by interest groups are helpful in bringing collective claims. Private rights of action for privacy harm gain effectiveness when structured under any form of collective redress. The procedural benefits of collective redress and their fit with privacy harm apply to different types of collective claims that group harmed victims. Representative actions, such as those recognized in the GDPR, provide many benefits of class actions while avoiding both objections.

The GDPR clause has a weakness: procedural law is local, so each country can decide whether and how to incorporate the mechanism.[207] The Court of Justice of the European Union ruled that consumer groups can file representative actions, but only as long as national law allows it.[208] One helpful form of GDPR-stipulated representative action, allowing people to join after the court issues its judgment, is absent in most countries' procedural laws.[209] A 2023 EU directive addresses this weakness, allowing qualified nonprofit groups in all EU countries to launch collective redress claims.[210] Representative actions, while overcoming both implementation concerns, face equivalent obstacles of compensation and grouping than those identified for class actions, requiring an equivalent solution.

A cohesive view of privacy values provides further reason to group privacy claims in class and representative actions. A policy goal of class actions is to increase access to justice.[211] Obstacles to private rights of action lead to a tension between the right of access to justice and the rigid right to sue in the information economy.[212] The tension can be mitigated by reforming laws to have a clear standard that reckons with privacy harm or by encouraging courts to identify, among data practices without (yet) materialized consequential harms, those that cause privacy harm.

Private rights of action in the information economy, in sum, are most useful as part of a collective redress mechanism. Class actions and representative actions can provide redress to group harms and mass harms in a way that complements public enforcement targeted at high-risk, systemic privacy losses. For them to be effective, a notion of intrinsic privacy harm is needed, so courts can address access to justice obstacles specific to the collection, processing, and sharing of people's information.

* * *

Liability can introduce meaningful accountability in the information economy with new laws that incorporate private rights of action based on a standard to avoid

immaterial privacy harm. An incremental alternative, without major legal reform, is for courts to expand the scope of private law liability to develop such a standard and apply it in parallel to statutes.

What separates this proposal from calls for liability in law reform circles and public policy is the basis for liability. Crucially, liability shouldn't depend on breach of procedural rules established in advance or broken promises in privacy documents that people agreed to. It also shouldn't hinge on negative material consequences that happen years later. For liability to reduce informational exploitation, private rights of action must depend on the creation of privacy or other data harm. The cause of action must be one that courts apply on a standards basis, where liability depends on intrinsic privacy harm.

The proposed liability system applies to both corporate data practices and breaches. Both activities produce privacy harm for profit, as both involve the intentional collection of personal information with resulting harmful exploitation, either through misuse or exposure. Despite their doctrinal differences, liability, particularly in the form of class actions, can address harm in both domains. Ideally, people who suffered the same privacy harm should be able to scale up their claims to a class action because this is the most effective way to seek redress. It's also the most socially efficient way to grant it.

Companies that collect, process, and distribute personal information are in a better position to understand their potential for harm and how to prevent it than their users and regulators are. Currently, corporations have little incentive to minimize the likelihood and magnitude of privacy harm. A regime where corporations are responsible for the cost of those harms responds to the pervasive harms that they must take accountability for and to the power they currently hold to avoid it.

Conclusion

Privacy law needs an update. It's older than the Internet – let alone AI. But the issue isn't that there are new technologies that it didn't foresee. Rather, the issue is that it's built on rules for a society that no longer exists. Privacy in the information economy is about regulating relationships of power.[1] And, to regulate power, one needs meaningful accountability for the powerful.[2]

When you log into your social network of choice, you're likely aware that it tracks what you "like" or "share" to form a profile about you for advertisers who wish to spend their budgets targeting those they're most likely to influence. What you're likely unaware of is the sheer amount of collected and inferred information that the social network and other corporations it trades with already have about you. Parts of it you expressly or inadvertently provided, and parts of it were inferred using algorithms and behavioral tracking. You also have no idea what the future uses of your data may be. Some pieces of data that appear innocuous today will be significant and harmful in the future, but you can't know which ones.

Personal data exchanges occur second by second and their consequences never leave you. They're different from traditional two-party consumer experiences, where a transaction begins when you approach the cash register and ends when you leave it. Every time we use a new app, we quickly click "I agree" to its privacy policy. In an instant, we're taken to have consented to the collection of countless data points for various corporate actors, who will go on to create detailed profiles of us that they may subsequently sell to marketers and to each other.[3] This process is inordinately opaque. And it certainly doesn't provide us with an opportunity to realistically assess the risk of each "I agree" click. Under these circumstances, privacy law can't rely on even the most sophisticated versions of individual consent provisions.

Privacy law is built on false behavioral assumptions that treat it, for the most part, like traditional two-party commercial exchanges. The rules that dictate what happens with our data are thus built on a misguided understanding of the social and economic interactions that involve those data. These assumptions lead to major misunderstandings: that people don't care about their privacy anymore, that they have nothing to lose if they have nothing to hide, and that they can take other options if

dissatisfied with how their data are handled. I call this the traditionalist approach. Modern economists moved past the simplified nineteenth-century paradigm that inspired it. But privacy law hasn't. When people click "I agree" to data practices that yield them little benefit and expose them to great harm, contrary to what laws assume they'll do, individual users aren't to blame. Our regulatory landscape is, perpetuating constant agreement without a clear sense of what harm can follow the data practices that people agree to.

As long as the traditionalist approach acts as the cornerstone of privacy law, our digital landscape will perpetuate a dynamic where tech companies garner tremendous profits and power at our expense. Companies have perverse incentives to misuse our personal data in ways that create risks and harms for us. Data aggregators, for example, are risk amplifiers.[4] Their business model is based on accumulating as much data as possible from as many people as possible.[5] Traditionalist regulations focus on giving people individual control over their data and establishing procedural safeguards.[6] These safeguards, though, provide marginal improvements over a free data market. In their worst forms, they perpetuate corporate profitability while forgetting the people they're supposed to protect. As a result, people receive little more than expensive lip service through a discourse of control and rights they can rarely use.

Harms fall through the cracks. "Move fast and break things" was an internal Facebook motto abandoned in 2014 that turned into a Silicon Valley mantra, taken as synonymous with innovation and tech disruption.[7] The motto made it to a letter to shareholders when Facebook went public, where Mark Zuckerberg clarified: "The idea is that if you never break anything, you're probably not moving fast enough."[8] It shows how data profiteers had and continue to have impunity for the harms they create – the "things" they break. Making them responsible for these harms is at the core of accountability.

Informational exploitation is pervasive. To exploit someone is to take advantage of their vulnerability or weakness for one's own benefit.[9] Wrongful exploitation adversely affects the dignity of the exploited person because they're treated as an object for someone else's ends.[10] This exploitative dynamic is reflected when corporations misuse our personal information for profit or profit from our information without keeping it safe, exposing us to data harms for surveillance dividends.[11]

Philosophers explain that exploitation entails exerting power over others for self-enrichment.[12] This dynamic is perceptible in the information economy. In it, power relationships exceed asymmetric bargaining or information. They extend into shaping the systems through which we communicate and into making decisions about our lives based on our data – such as our credit score to determine loan opportunities and what options of housing and employment we're exposed to.[13] And corporations that take, infer, and share our data are ever-present. This dynamic widely exceeds contractual or consumer relations. Some of these are companies we've never heard of.[14] There's an incongruity in applying contract law remedies, such as defaults and unconscionability, to address abuse of power and discretion.

The dynamic of power and discretion is one in which entities that profit from us have the ability to unilaterally inflict harm on us. Corporations in the information economy have the power to exercise harms with significant impunity. Traditionalist laws, by establishing procedural, box-ticking compliance divorced from consequences, entrench this power.[15] So do traditionalist regulators when they defer to these symbolic compliance mechanisms, performing privacy without protecting people.[16] The unenviable result is socially costly mechanisms that don't rein in harms created by the information economy's business model and don't effectively curb corporate power. Procedural measures and sanctions for eventual noncompliance lead to large compliance costs that big players can withstand but small players can't.[17] In that way, they keep power in the information economy unaccountable.[18] The only way out is for legislators, regulators, and courts to shift attention toward individual and social privacy harms.

The privacy fallacy results from such a misunderstanding, where we see the intrinsic value of privacy but not the possibility of harming it. We fall prey to it when we believe that, while privacy is valuable in itself and it's worth protecting, that value can't be harmed in and of itself and we only need to be protected from tangible consequences. Saying that if there's no tangible harm from a data practice there's nothing to worry about ("If you have nothing to hide, you have nothing to lose") runs into the problem of being systemically exposed to exploitation.

Duties that survive "I agree" moments, such as those established by the GDPR, are crucial to enhanced protection. But procedural rules paired with reinforcing individual control tend to replicate, rather than resolve, the information economy's moral hazard that enables exploitation. On the books, consent is a minimum threshold in most regulations, under which people have other rights after consenting. But, in practice, you can agree to data practices that override almost every substantive protection, and most remaining data protection rights you can't waive depend on you being able to exercise them.[19] Abandoning individual consent provisions is the first step in creating accountability for privacy harm. Consent provisions should be removed from our privacy laws because, in practice, consent provisions swallow everything else.[20] An arbitration clause, for example, can undo much of the good that liability does.[21]

These provisions aren't merely a relic from the past. They play an outsized role in emerging privacy legislation too.[22] Google's former CEO Eric Schmidt once confessed to *The Atlantic*: "The average American doesn't realize how much of the laws are written by lobbyists … and it's obvious that if the system is organized around incumbencies writing the laws, the incumbencies will benefit from the laws that are being written."[23] The numbers add up. There are almost twice as many Amazon lobbyists registered in the US as there are senators in the US Congress.[24] In 2021, Alphabet (Google), Amazon, and Meta (Facebook) spent $50 million just in their Washington DC lobbying efforts.[25] The tech industry together spends about €100 million per year in lobbying EU institutions.[26]

For the most part, people feel that their privacy is protected with the options afforded by individual control rights. This feeling of protection makes us trust the system, makes us navigate the Internet comfortably, and gives us a (false) sense of wellbeing guarantees as we engage in the economy. The false feeling of protection is beneficial to regulated companies: we're online more than we otherwise would be, we create more ad revenue, we spend more money, we use more products, and we embed the system in our social life more, making it more difficult to escape from it for others.

Part of the traditionalist approach's perpetuation takes place because providing people with control and autonomy has an intuitive appeal.[27] So people may accept control-based measures even if they're bad for them. Framing privacy and data protection as questions of formal autonomy in a context of power imbalance and ease of manipulation is, in itself, a successful exercise of power and manipulation.[28]

A significant achievement of the traditionalist paradigm is successfully presenting itself as the natural way of running things. People are told that they deserve to have control over their information – that it belongs to them – as a gold standard.[29] Politicians talk about patching market failures as if it were a novel and tough approach to big tech.[30] When someone asks why a regulatory framework isn't working, legislators often think it's because the framework isn't neoclassical enough. If people are clicking "I agree" too easily, then regulators often think it must be that, to solve the problem, one needs to tack on the word "meaningful" or "informed" before "consent" in the statute as a harbinger of individual control.[31] Or, if corporations offer extractive and extortive terms of service that are eerily similar to each other, then one should use antitrust law because it must be simply a manifestation of abuse of market power and, if we split them up, we would solve the problem.[32]

Protecting people from exploitation, though, preserves their autonomy. Exploitation is marked by impaired consent and unfair distributive outcomes.[33] Protecting people's autonomy means sheltering them from exploitation even when they would agree to it.[34] People are also harmed by exploitation, online and offline, when they formally agree to how they're treated, much like thousands of sweatshop workers do because they have no better options.[35] Exploitation harms also take place when choices exist but people can't evaluate the harm involved.[36] Under such conditions, it's still exploitative when someone agrees to – or even is content with – the treatment they receive.[37] Recognizing people's autonomy means considering people capable of living their lives in ways that assume some risks. It doesn't mean taking their blanket before-the-fact agreement to an activity to mean they accepted all resulting harm and are immunized from being exploited by it.[38] Even if one believed that individual control over personal information is what privacy law ought to protect because decisional autonomy is the only relevant value, the traditionalist paradigm crumbles under the power dynamics that make individual control impossible. Protecting people's autonomy when they can't understand what they agree to means protecting them from the moral hazard of the growing influence of

corporate actors that shape how we communicate and have the power to manipulate an increasing number of aspects of our lives.

Mark Zuckerberg thinks that "[i]n a lot of ways Facebook is more like a government than a traditional company."[39] Tech giants hold so much power in the information economy that scholars also believe they have equivalent powers to state actors.[40] One reason is size. These are some of the largest companies in the world, with billions of users, enormous resources at their disposal, and more money than some governments.[41] Their size includes an actual airline (Prime Air), airports (Air Hubs), and spacecrafts (SpaceX, technically owned by Elon Musk, not Twitter). Another reason is control over interactions. Designing the platforms that we use to communicate, access information, and share information grants influence over private behaviors and public opinion.[42] Meta brags about its ability to nudge democratic outcomes.[43] They even have systems of dispute resolution – some call it a "Supreme Court."[44] A third reason is reach. Tech giants operate globally, with the ability to exert influence across almost all national borders.[45] On one occasion, they influenced those very borders.[46] These factors combined bestow an amount of power that's unprecedented.[47] Not even the Dutch East India Company could do this much.

Reckoning with informational exploitation explains why tech companies can be similarly powerful to state actors. The source of their power is our data. Tech giants hold power over us based on the data they have about us, even independent of their market position.[48] They exercise this power not through money but through data. Because they collect and infer vast data about their users and others, they can turn our personal information against us. They can, for example, use data about activities and preferences to manipulate behavior in ways that benefit the company but aren't in its users' best interests, with consequences as varied as inflating purchasing behavior, enabling discrimination, and swaying presidential elections.[49] Their growing power, crystalized in their ability to produce harms with significant impunity, leads to a growing need to curb the harms that it causes.

Privacy law needs accountability for the consequences of data practices. At the center of accountability, there should be liability based on duties not to harm, including harms of informational exploitation and the consequences that accrue from them. To achieve accountability, laws need to redirect back to the corporations the cost of the harms that they produce while making a profit. This proposal aligns with broader accountability efforts advanced by various scholars, which include information fiduciaries, privacy by design, and relationships of trust.[50] It departs from existing liability regimes and proposals, which are unhelpfully triggered by breach of procedural rules or promises in privacy policies. Anchoring liability on a concept of intrinsic privacy harm, such as informational exploitation, can overcome problems of standing, causation, class certification, and damages that liability provisions face under current law.

Accountability efforts have ample precedent. The FIPs document from the FTC, which inspired much of today's privacy law, discussed corporations' responsibility

to prevent data misuse.[51] The GDPR has a declared focus on accountability.[52] The Canadian FIPs also include accountability.[53] The idea of accountability, however, weakened as it slowly faded into responsibility to comply with procedural rules and corporate promises. Laws shouldn't ignore the data misuse that takes place under these rules. Because of the information economy's moral hazard, "responsibility" must mean accountability for the outcomes of how corporations use (or misuse) people's personal information.

This proposal doesn't impede other forms of regulation. It reinforces other forms of accountability, such as information fiduciaries and privacy by design. These accountability mechanisms provide a duty not to exploit (fiduciaries) and mechanisms to prevent exploitation (privacy by design); they're reinforced by liability based on a notion of what it is to exploit. This proposal can operate absent legislatures mandating these other mechanisms because it creates structural economic incentives for corporations to implement them. Due to being tethered to a theory of harm, it avoids critiques issued to other accountability mechanisms, such as risk of becoming too crystalized into specific rules,[54] risk of impeding working business models,[55] and risk of becoming too expansive or vague for courts to apply.[56] This proposal also doesn't impede the existing data protection rights and procedural system – as long as these mechanisms don't pull resources away from meaningful changes.

Law reform is needed on multiple fronts. Accountability requires new legal standards, rather than procedural rules. Liability for individual and group harms should be combined with regulatory standards for systemic risks. Publicly enforceable legal standards are well suited to address systemic privacy problems, complementing civil liability. A combination of procedure-independent duties and prohibitions can reduce systemic risk and mitigate widespread social harms. Harm identification can't be done by legislators in advance, so the best regulatory regimes are those that minimize risk and make room for harm to be identified after the fact.

The reform extends to enforcement. Data protection authorities are best positioned to address systemic issues for which liability is ineffective – undifferentiated privacy losses that don't produce individual or group harms but produce widespread risk. Group harms can be addressed through privacy class actions. But class actions can't deter widespread, systemic social risks.[57] In countries where, by contrast, authorities focus on enforcing individual control rights, they extend consent problems and remove attention from systemic effects.[58] Enforcement systems with that focus fail to equip people with tools to pursue common interests, obscure systemic harm, and perpetuate conditions for widespread exploitation.[59]

Accountability for data practices' consequences requires distinguishing between losses and harms. Tyler Clemente, the teenager mentioned in the Introduction who died by suicide after being secretly filmed during an intimate encounter and outed, faced a privacy loss (data collection) that constituted privacy harm because his identity was exploited for amusement. His humiliation and death were consequences of this harm. His story illustrates privacy's distributional effect, as the

same information (intimate encounters) is often more harmful to Queer people and women than to others. Monica Lewinsky, whose well-known story was also mentioned in the Introduction, faced a privacy loss (data sharing) that constituted privacy harm because her intimate life was exploited for clicks and used for profit. Her public humiliation and harm to her career were consequences of the informational exploitation she was put through. Often, harmful losses such as these are probabilistic, when based on inferred or group data.

To achieve meaningful accountability, liability must include more than the financial or physical consequences of data practices. It must also include privacy harm. If the only problematic aspect of the information economy were its tangible consequences, it would follow that we would have a better society with no privacy at all, provided that it could be achieved without causing negative financial and physical consequences. In that hypothetical society, we would allow people to be manipulated and exploited based on their personal information for profit, while protecting their finances and physical integrity. If this doesn't sound desirable to you, it's because you see some intrinsic value in privacy.

The intrinsic view of privacy explains why privacy is a human right in so many countries. Reducing privacy to its negative tangible consequences implies, by extension, that privacy can be overridden by desirable tangible consequences such as economic gain. Breaking the binary in which privacy is often put by distinguishing between losses and normative harms leads to a better framework. Privacy loss can be subjected to cost–benefit analyses, where appropriately acquiring and using information for economic gain is acceptable – and even desirable. Privacy harm shouldn't. Legitimate data practices should be pursued while avoiding privacy harm and including accountability for harm when they create it.

Liability for data practices' outcomes would preserve the information economy. It would even improve it. It wouldn't halt innovation or the tech industry because it creates space for the industry to engage in any data practice that produces more profit than harm.[60] Creating liability for the consequences of their data practices provides needed incentives to develop data practices that are high-profit and low-harm. Conversely, it makes low-profit and high-harm activities more expensive. To be fair, companies that produce harm would be less profitable with liability than without it. Yet profitability at all costs is unacceptable from a public policy perspective.[61] Focusing regulatory costs on consequences rather than tying corporations to procedure-focused regulations may even present lower costs for those companies that carry the safest data practices for those whose data they profit from. Unlike procedural rules, which have high regulatory costs and introduce entry barriers that disadvantage new, small players to the benefit of incumbents with large legal and compliance departments, liability has lower costs for those with lower risk. With the current system, privacy-protective services need the same safeguards as privacy-invasive services. Shifting attention to liability would help nonexploitative services to flourish.

The surge of AI in our daily lives accentuates the need to curb privacy harm. AI inferences facilitate significant influence over our daily lives by making decisions about us in areas as diverse as finances, employment, health, housing, and speech. In a society where our information can be used to exploit us and where our wellbeing is influenced by how our information is turned into credit scores, risk assessments, and employability, developing functional protection against privacy harm is urgent. To fix it, we need to hold corporations responsible for the consequences their data practices create. That's what legal systems do for any other valuable activity that produces pervasive intended and unintended harm to others.

Notes

INTRODUCTION

1 Ian Parker, "The Story of a Suicide" *The New Yorker* (6 February 2012) <https://perma.cc/8BW7-ZSXA>.

2 Kate Zernike, "After Gay Son's Suicide, Mother Finds Blame in Herself and in Her Church" *The New York Times* (24 August 2012) <https://perma.cc/2N8E-HB4Q>.

3 Danielle Keats Citron, *The Fight for Privacy: Protecting Dignity, Identity, and Love in the Digital Age* (WW Norton 2022) 183.

4 Ahmar Khan, "Trans Woman, Twitch Streamer Keffals Doxxed, Arrested at Gunpoint by London, Ont. Police" (*Global News*, 9 August 2022) <https://perma.cc/CZ9H-YVJL>; Kate Dubinski, "Trans Star on Twitch Fears for Her Life after Someone Sent Police to Her London, Ont., Home" (*CBC*, 9 August 2022) <https://perma.cc/8XJC-ATD8>.

5 Margaret Pless, "Kiwi Farms, the Web's Biggest Community of Stalkers" *New York Magazine Intelligencer* (19 July 2016) <https://perma.cc/3EUV-TPZG>.

6 Donie O'Sullivan and Richa Naik, "Trans Activist Celebrates Rare Victory against Online Trolls after Kiwi Farms Deplatforming" (*CNN*, 6 September 2022) <https://perma.cc/HBJ4-UK2F>.

7 David Gilbert, "Inside Keffals' Battle to Bring Down Kiwi Farms" (*Vice*, 7 September 2022) <https://perma.cc/2GRT-BFVL>.

8 Ahmar Khan and Amy Simon, "Twitch Streamer and Transgender Activist Doxxed in Northern Ireland after Leaving Canada" (*Global News*, 31 August 2022) <https://perma.cc/7P6A-YF3R>.

9 See *R. v. Manoux*, 2017 ONCJ 58 para 5 [Canada]; *R v DRW*, 2016 ONCJ 171 [Canada]; *R. v. Taylor*, 2015 ONCJ 741 para 1 [Canada]; *R. v. Jarvis*, 2019 SCC 10 para 2 [Canada]; *R. v. Bursey*, 2017 NLTD(G) 62 paras 5–6 [Canada]; *R. v. Gardiner*, 2017 ONSC 3904 para 4 [Canada]; *R. v B.H.*, 2017 ONCJ 377 para 3 [Canada]; *R. c. D.R.*, 2018 QCCQ 80 paras 1–8 [Canada].

10 Danielle Keats Citron, "A New Compact for Sexual Privacy" (2020) 62 *William & Mary Law Review* 1763, 1783. Danielle Keats Citron, "Sexual Privacy" (2019) 128 *Yale Law Journal* 1870, 1904–1928. Ryan Calo, "Digital Market Manipulation" (2014) 82 *George Washington Law Review* 995, 999, 1003–1008; Solon Barocas and Andrew Selbst, "Big Data's Disparate Impact" (2016) 104 *California Law Review* 671, 677–694.

11 Evan Selinger and Judy Hyojoo Rhee, "Normalizing Surveillance" (2021) 22 *Northern European Journal of Philosophy* 49, 59–60. Jamie Luguri and Lior Jacob Strahilevitz,

"Shining a Light on Dark Patterns" (2021) 13 *Journal of Legal Analysis* 43, 47; Ari Ezra Waldman, "Cognitive Biases, Dark Patterns, and the 'Privacy Paradox'" (2020) 31 *Current Opinion in Psychology* 105, 108.

12 Julie E Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (Oxford University Press 2019) 5–7; Shoshana Zuboff, *The Age of Surveillance Capitalism* (1st ed., PublicAffairs 2019) 8–12, 35–36.

13 See Michelle Dean, "The Story of Amanda Todd" *The New Yorker* (18 October 2012) <https://perma.cc/5ZEB-4MFZ>. See also Chapter 1B.

14 Citron, *The Fight for Privacy* (n 3) 3–23, 47–49. See also Clare McGlynn and Erika Rackley, "Image-Based Sexual Abuse" (2017) 37 *Oxford Journal of Legal Studies* 534, 537–540.

15 Julia Angwin and Terry Parris Jr, "Facebook Lets Advertisers Exclude Users by Race" (*ProPublica*, 28 October 2016) <https://perma.cc/48UB-9A4Y>.

16 *National Fair Housing Alliance v Facebook Inc* SDNY 18 Civ. 2689 (JGK), 18 Civ 2689 JGK. See also "Statement of Interest of the US Opposing Facebook's Motion to Dismiss" (*SDNY*) 2–17 <https://perma.cc/3XV8-KUQV>.

17 "Improving Enforcement and Promoting Diversity: Updates to Ads Policies and Tools" (*Meta*, 8 February 2017) <https://perma.cc/33BB-V6HW>.

18 Till Speicher and others, 'Potential for Discrimination in Online Targeted Advertising', *Proceedings of the 1st Conference on Fairness, Accountability and Transparency* (PMLR 2018) 2 <https://perma.cc/U5KP-WQXM>.

19 Ariana Tobin, "Facebook Promises to Bar Advertisers from Targeting Ads by Race or Ethnicity. Again" (*ProPublica*, 25 July 2018) <https://perma.cc/MC3F-A2GK>; Ariana Tobin and Jeremy B Merrill, 'Besieged Facebook Says New Ad Limits Aren't Response to Lawsuits' (*ProPublica*, 23 August 2018) <https://perma.cc/VU2Z-Z3K7>.

20 Pauline Kim and Sharion Scott, "Discrimination in Online Employment Recruiting" (2019) 63 *St. Louis University Law Journal* 93, 95.

21 Omri Ben-Shahar and Lior Jacob Strahilevitz, "Contracting over Privacy: Introduction" (2016) 45 *The Journal of Legal Studies* S1, 1.

22 Woodrow Hartzog, "The Case against Idealising Control" (2018) 4 *European Data Protection Law Review* 423; Iris van Ooijen and Helena U. Vrabec, "Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective" (2019) 42 *Journal of Consumer Policy* 91.

23 Solon Barocas and Helen Nissenbaum, "Big Data's End Run around Anonymity and Consent" in Julia Lane and others (eds), *Privacy, Big Data, and the Public Good: Frameworks for Engagement* (Cambridge University Press 2014).

24 Ari Ezra Waldman, "Outsourcing Privacy" (2020) 96 *Notre Dame Law Review Reflection* 194, 195; Ari Ezra Waldman, "Privacy, Practice, and Performance" (2022) 110 *California Law Review* 1221.

25 Ari Ezra Waldman, *Industry Unbound: The Inside Story of Privacy, Data, and Corporate Power* (Cambridge University Press 2021) 99–160.

26 Tort deals with wrongdoings committed by one person against another. It aims to provide compensation for harm suffered because of these wrongdoings, known as "torts." It makes people accountable for their actions by holding them financially responsible for harm they cause.

27 Katherine Strandburg, "Free Fall: The Online Market's Consumer Preference Disconnect" (2013) 430 *University of Chicago Legal Forum* 95, 131.

28 Thomas Kadri, "Brokered Abuse" [2023] *Journal of Free Speech* 1; Chris Jay Hoofnagle, "Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers

Collect and Package Your Data for Law Enforcement" (2003) 29 *North Carolina Journal of International Law and Commercial Regulation* 595.

29 See Julie E Cohen, "How (Not) to Write a Privacy Law" (*Knight First Amendment Institute at Columbia University*, 23 March 2021) <https://perma.cc/2TTH-8BK5>; Daniel J Solove, "The Limitations of Privacy Rights" (2023) 98 *Notre Dame Law Review* 975, 987; Ari Ezra Waldman, "Privacy's Rights Trap" (2022) 117 *Northwestern University Law Review* 88.

30 Cohen, *Between Truth and Power* (n 12) 145.

31 Jack M Balkin, "Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation" (2018) 51 *U.C. Davis Law Review* 1149, 1167–1168; Jack Balkin, "2016 Sidley Austin Distinguished Lecture on Big Data Law and Policy: The Three Laws of Robotics in the Age of Big Data" (2017) 78 *Ohio State Law Journal* 1217, 1234–1235.

32 See Jack Balkin, "Information Fiduciaries and the First Amendment" (2016) 49 *U.C. Davis Law Review* 1183; Woodrow Hartzog, *Privacy's Blueprint: The Battle to Control the Design of New Technologies* (Harvard University Press 2018); Ari Ezra Waldman, *Privacy as Trust: Information Privacy for an Information Age* (Cambridge University Press 2018); Neil Richards, *Why Privacy Matters* (Oxford University Press 2021); Citron (n 3).

33 Monica Lewinsky, "The Price of Shame" (*TED*, 20 March 2015) <https://perma.cc/HQ9B-UZL8>.

34 Ibid.

35 Gary Anthes, "Data Brokers Are Watching You" (2015) 58 *Communications of the ACM* 28.

36 Richards, *Why Privacy Matters* (n 32) 207–213; Citron, *Fight for Privacy* (n 3) 106–128; Waldman, *Privacy as Trust* (n 32) 34–45; Helen Nissenbaum, *Privacy in Context: Technology, Policy and the Integrity of Social Life* (Stanford University Press 2010) 127–150.

37 Woodrow Hartzog, "What Is Privacy? That's the Wrong Question" (2021) 88 *University of Chicago Law Review* 1677, 1687; Danielle Keats Citron and Daniel J Solove, "Privacy Harms" (2022) 102 *Boston University Law Review* 793, 830; Daniel J Solove, "A Taxonomy of Privacy" (2005) 154 *University of Pennsylvania Law Review* 477, 486; Daniel Solove, "Conceptualizing Privacy" (2002) 90 *California Law Review* 1087, 1089.

38 Richards, *Why Privacy Matters* (n 32) 111–206; Nissenbaum, *Privacy in Context* (n 36) 67–88.

39 See British Data Protection Act 2018, Part 1, 3(5) ("'Data subject' means the identified or identifiable living individual to whom personal data relates.")

40 Cohen, *Between Truth and Power* (n 12) 25–47; Carissa Véliz, *Privacy Is Power: Why and How You Should Take Back Control of Your Data* (Bantam Press 2021) 50–82; Daniel Solove, "Privacy and Power: Computer Databases and Metaphors for Information Privacy" (2001) 53 *Stanford Law Review* 1393, 1413–1430; Lisa M Austin, "Enough about Me: Why Privacy Is about Power, Not Consent (or Harm)" in Austin Sarat (ed), *A World Without Privacy?: What Can/Should Law Do* (2014) 134 <https://perma.cc/EPK4-HCRJ>; Orla Lynskey, "Grappling with 'Data Power': Normative Nudges from Data Protection and Privacy" (2019) 20 *Theoretical Inquiries in Law* 189, 192.

41 Anita L Allen, *Why Privacy Isn't Everything: Feminist Reflections on Personal Accountability* (Rowman & Littlefield Publishers 2003) 26.

42 Jonathan Taplin, *Move Fast and Break Things: How Facebook, Google, and Amazon Cornered Culture and Undermined Democracy* (Little, Brown and Company 2017). See also Herman Taneja, "The Era of 'Move Fast Break Things' Is Over", Harvard Business Review (22 January 2019).

1 THE TRADITIONALIST APPROACH TO PRIVACY

1 Martha T McCluskey, Frank Pasquale, and Jennifer Taub, "Law and Economics: Contemporary Approaches" (2016) 35 *Yale Law & Policy Review* 297, 299–300.
2 Rush, "Freewill" (1980).
3 Jean-Paul Sartre, *Existentialism Is a Humanism* (Yale University Press 2007) ("In one sense choice is possible, but what is not possible is not to choose. I can always choose, but I must know that if I do not choose, that is still a choice").
4 "AWS Service Terms" (*Amazon Web Services, Inc.*, 4 November 2022) <https://perma.cc/S4CN-KKZA>. See also Samuel Gibbs, "Amazon Updates Its Terms of Service to Cover the Zombie Apocalypse" *The Guardian* (11 February 2016) <https://perma.cc/8FZF-6HGE>. This provision was removed after this book went through copyediting, on 3 May 2023.
5 Daniel J Solove, "Introduction: Privacy Self-Management and the Consent Dilemma" (2012) 126 *Harvard Law Review* 1880, 1880. See Federal Trade Commission, "Privacy Online: Fair Information Practices in the Electronic Marketplace – A Report to Congress" (2000) 7–9 <https://perma.cc/7CB9-RHKA>; Federal Trade Commission, "Final Report of the Federal Trade Commission Advisory Committee on Online Access and Security" <https://perma.cc/X8QS-VWA4>.
6 See Chapter 5A.
7 Julia Fioretti, "Europeans to Be 'Masters' of Their Personal Data: Senior Official" *Reuters* (London, 16 December 2015) <https://perma.cc/78KL-7VG6>.
8 Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Business and Policymakers" (2012) <https://perma.cc/Z39C-NUSB>.
9 "Consumer Data Privacy in a Networked World" (*The White House*, 2012) i <https://perma.cc/K8LX-RWYN>.
10 'Government Moves to Protect Privacy in Private Sector' (*Office of the Privacy Commissioner of Canada*, 1 October 1998) <https://perma.cc/WQ47-SPYA>.
11 Baptiste Chatain, "MEPs Highlight the Potential of the Data Economy for Jobs" (*European Parliament*, 25 March 2021) <https://perma.cc/Q76Z-GR8B>.
12 A29WP, "Opinion 2/2013 on Providing Guidance on Obtaining Consent for Cookies" (2013) 2–3.
13 Navdeep Bains, Digital Charter Implementation Act, 2020 [Bill C-11 (Historical)].
14 'Consumer Consent and Authorisation' (*Office of the Australian Information Commissioner*) <https://perma.cc/4FXF-JAMW>. See also 'Explanatory Paper: Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021' (*Australian Government*, October 2021) 9 <https://perma.cc/YU29-HS4B>.
15 Solove, "Introduction: Privacy Self-Management and the Consent Dilemma" (n 5) 1884–1885.
16 Ibid 1882–1883.
17 United States Department of Health Education and Welfare, "Records, Computers and the Rights of Citizens" (MIT Press, 1973) III <https://perma.cc/W65E-BB4M>.
18 Ibid vi.
19 "Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data" (*OECD*, 23 September 1980) <https://perma.cc/R7CC-BTJA>. Privacy Act of 1974, Pub. L. No. 93-579 (codified at 5 U.S.C. 552a (2012)); Family Educational Rights and Privacy Act of 1974, Pub. L. No. 93-380 (codified at 20 U.S.C. 1232g (2012)); Cable Communications Policy Act of 1984, Pub. L. No. 98-549 (codified at 47 U.S.C. 551 (2012)).

20 Jonathan Zittrain, *The Future of the Internet: And How to Stop It* (Yale University Press 2008) 201; Przemyslaw Palka, "Data Management Law for the 2020s: The Lost Origins and the New Needs" (2020) 68 *Buffalo Law Review* 559, 584–589; Marc Rotenberg, "Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)" [2001] *Stan. Tech. L. Rev.* 1, 13–17; Woodrow Hartzog, "The Inadequate, Invaluable Fair Information Practices" (2016) 76 *Maryland Law Review* 952, 953–954, 958–961. See also Abraham L Newman and David Bach, "Privacy and Regulation in a Digital Age" in Brigitte Preissl, Harry Bouwman, and Charles Steinfield (eds), *E-Life after the Dot Com Bust* (Springer-Verlag Berlin Heidelberg 2004) 254.

21 Regulation (EU) 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 (General Data Protection Regulation); Personal Information Protection and Electronic Documents Act, SC 2000, c 5 (Canada); Act on the Protection of Personal Information Act No. 57 of 2003 (Japan); Personal Data Protection Act, Act No. 25.326 of 2000 (Argentina); Personal Information Protection Act, Act No. 14839 of 2017 at art. 3 (South Korea); Privacy Act 2020, No. 31 of 2020 at Part 3 (New Zealand); Privacy Act 1988, Act No. 119 of 1988 at schedule 1 (Australia); Data Privacy Act of 2012, Republic Act 10173 of 2012 at s 11 (Philippines); Personal Data Protection Act 2010, Act No. 709 of 2010 at s 5 (Malaysia); Data Protection Act 2018, c 12 (UK); Personal Data Protection Act, Act No. 2012 of 2020 at Schedule 3 (Singapore); and US state statutory privacy legislation, such as the California Consumer Privacy Act, AB-375 of 2018.

22 Federal Trade Commission (n 5) i.

23 GDPR Article 5(1) – Principles relating to processing of personal data (lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, and integrity and confidentiality).

24 OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data 1980 (Collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and enforcement).

25 The original US Department of Health, Education, and Welfare FIPs were transparency of records, notice, purpose limitation, accuracy, and responsibility to prevent misuse. For the Canadian Personal Information Protection and Electronic Documents Act, they're ten: accountability, identifying purposes, consent, limiting collection, limiting use, disclosure, and retention, accuracy, safeguards, openness, individual access, and challenging compliance. See "PIPEDA Fair Information Principles" (*Office of the Privacy Commissioner of Canada*, 16 September 2011) <https://perma.cc/QNE9-W47T>.

26 Daniel J Solove and Paul M Schwartz, "ALI Data Privacy: Overview and Black Letter Text" (2022) 68 *UCLA Law Review* 1252, 1262–1263.

27 Hartzog, "The Inadequate, Invaluable Fair Information Practices" (n. 20) 965; Fred H Cate, "The Failure of Fair Information Practice Principles," *Consumer Protection in the Age of the Information Economy* (2006) 343–344. See also Article 29 Working Party, "Opinion 15/2011 On the Definition of Consent (WP187)" (*European Commission*, 13 July 2011) 8 <https://perma.cc/2CW9-L67C>.

28 Federal Trade Commission, "Privacy Online: Fair Information Practices in the Electronic Marketplace" (n 5) 7–8.

29 Federal Trade Commission Act of 1914–2006 (15) 41. 15 U.S.C. s 45 (a)(1),(2).

30 Marcia Hofmann, "Federal Trade Commission Enforcement of Privacy" in Christopher Wolf (ed), *Proskauer on Privacy* (Practicing Law Institute 2008); Aleecia McDonald and Lorrie Faith Cranor, "The Cost of Reading Privacy Policies" (2008) 4 *I/S: Journal of Law*

and Policy for the Information Society 543, 545–546; Woodrow Hartzog and Daniel J Solove, "The FTC and the New Common Law of Privacy" (2014) 114 *Columbia Law Review* 583.

31 Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change" (n 8) 48–60; Woodrow Hartzog, "The New Price to Play: Are Passive Online Media Users Bound By Terms of Use?" (2010) 15 *Communication Law and Policy* 405, 415; Lindsey Barrett and others, "Illusory Conflicts: Post-Employment Clearance Procedures and the FTC's Technological Expertise" (2020) 35 *Berkeley Technology Law Journal* 793, 814–815.

32 Paula J Dalley, "The Use and Misuse of Disclosure as a Regulatory System" (2006) 34 *Florida State University Law Review* 1089, 1090–1091; Robert S Adler and R David Pittle, "Cajolery or Command: Are Education Campaigns an Adequate Substitute for Regulation?" (1984) *Yale Journal on Regulation* 159, 159–160. Other examples are the Securities Act, the Truth in Lending Act, and the ABA's Model Court Rule on Insurance Disclosure.

33 Allyson W Haynes, "Online Privacy Policies: Contracting Away Control over Personal Information" (2007) 111 *Penn State Law Review* 587, 600.

34 Ryan Calo, "Against Notice Skepticism in Privacy (and Elsewhere)" (2012) 87 *Notre Dame Law Review* 1027, 1032; Hartzog and Solove, "The FTC and the New Common Law of Privacy" (n 30) 592–593.

35 'Fair Information Practice Principles' (*Federal Trade Commission*, 31 March 2009) <https://perma.cc/8EUH-9SFD>; Robert Pitofsky and others, "Privacy Online: A Report to Congress" [1998];Federal Trade Commission 64, 7, 41.

36 Calo, "Against Notice Skepticism in Privacy" (n 34) 1048.

37 Matthew Crain, "A Critical Political Economy of Web Advertising History" in Niels Brügger and Ian Milligan (eds), *The SAGE Handbook of Web History* (2019) 340.

38 Omri Ben-shahar and Carl E Schneider, "The Failure of Mandated Discourse" (2011) 159 *University of Pennsylvania Law Review* 647, 682; Florencia Marotta-Wurgler, "Even More than You Wanted to Know about the Failures of Disclosure" (2015) 11 *Jerusalem Review of Legal Studies* 63, 63–64.

39 Dalley, "The Use and Misuse of Disclosure as a Regulatory System" (n 32) 1090–1093; Calo, "Against Notice Skepticism in Privacy" (n 34) 1028.

40 Calo, "Against Notice Skepticism in Privacy" (n 34) 1048.

41 Neil Richards, *Why Privacy Matters* (Oxford University Press 2021) 174–176.

42 See Directive (EC) 2019/770 of 20 May 2019 on Certain Aspects Concerning Contracts for the Supply of Digital Content and Digital Services [2019] OJ L 136/1, art 3,7 <https://perma.cc/E75D-VS99>.

43 Daniel Solove, *The Digital Person: Technology and Privacy in the Information Age* (New York University Press 2004) 90–91.

44 Hartzog, "The Inadequate, Invaluable Fair Information Practices" (n 20) 952.

45 Lisa M Austin, "Reviewing PIPEDA: Control, Privacy and the Limits of Fair Information Practices" (2006) 44 *Canadian Business Law Journal* 21, 23–24; Lisa M Austin, "Is Consent the Foundation of Fair Information Practices Canada's Experience under Pipeda" (2006) 56 *University of Toronto Law Journal* 181, 182–183; Cate, "The Failure of Fair Information Practice Principles" (n 27) 343; Hartzog, "The Inadequate, Invaluable Fair Information Practices" (n 20) 952–955.

46 McDonald and Cranor, "The Cost of Reading Privacy Policies" (n 30) 564. See also Alexis C Madrigal, "Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days" (*The Atlantic*, 1 March 2012) <https://perma.cc/JK7V-UYA9>.

47 George Milne and Mary Culnan, "Strategies for Reducing Online Privacy Risks: Why Consumers Read (or Don't Read) Online Privacy Notices" (2004) 18 *Journal of Interactive Marketing* 15, 20–21. See also Ben-shahar and Schneider, "The Failure of Mandated

Discourse" (n 38) 671–672; Florencia Marotta-Wurgler, "Will Increased Disclosure Help – Evaluating the Recommendations of the ALI's Principles of the Law of Software Contracts" (2011) 78 *University of Chicago Law Review* 165, 178; Yannis Bakos, Florencia Marotta-Wurgler, and David R Trossen, "Does Anyone Read the Fine Print? Consumer Attention to Standard-Form Contracts" (2014) 43 *The Journal of Legal Studies* 1, 31–32; Jonathan A Obar and Anne Oeldorf-Hirsch, "The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services" (2020) 23 *Information, Communication & Society* 128, 140–142.

48 Andrew Malcolm, "Top of the Ticket: Chief Justice Roberts on Tiny Type" *Los Angeles Times* (20 October 2010) <https://perma.cc/9F2X-MRSJ>.

49 Joel R Reidenberg and others, "Disagreeable Privacy Policies: Mismatches between Meaning and Users' Understanding" (2015) 30 *Berkeley Technology Law Journal* 39, 69.

50 Richards, *Why Privacy Matters* (n 41) 174–176.

51 Calo, "Against Notice Skepticism in Privacy" (n 34) 1062–1063; William M Sage, "Regulating through Information: Disclosure Laws and American Health Care" (1999) 99 *Columbia Law Review* 1701, 1803–1804.

52 Solon Barocas and Helen Nissenbaum, "On Notice: The Trouble with Notice and Consent" [2009] Proceedings of the engaging data forum 5–6; Kirsten Martin, "Do Privacy Notices Matter? Comparing the Impact of Violating Formal Privacy Notices and Informal Privacy Norms on Consumer Trust Online" (2016) 45 *The Journal of Legal Studies* s191, s195. See also McDonald and Cranor, "The Cost of Reading Privacy Policies" (n 30) 546.

53 Omri Ben-Shahar and Adam Chilton, "Simplification of Privacy Disclosures: An Experimental Test" (2016) 45 *The Journal of Legal Studies* S41, S54–S55; Lior Jacob Strahilevitz and Matthew B Kugler, "Is Privacy Policy Language Irrelevant to Consumers?" (2016) 45 *The Journal of Legal Studies* S69, S87–S92.

54 Omri Ben-Shahar and Carl E Schneider, *More Than You Wanted to Know: The Failure of Mandated Disclosure* (Princeton University Press 2016) 71–86.

55 Andy Greenberg, "An AI That Reads Privacy Policies So That You Don't Have To" *Wired* (9 February 2018) <https://perma.cc/8238-RBVN>.

56 Florencia Marotta-Wurgler, "Self-Regulation and Competition in Privacy Policies" (2016) 45 *Journal of Legal Studies* S13, 18; John A Rothchild, "Against Notice and Choice: The Manifest Failure of the Proceduralist Paradigm to Protect Privacy Online (or Anywhere Else)" (2018) 66 *Cleveland State Law Review* 559, 629.

57 Martin, "Do Privacy Notices Matter?" (n 52) S193, S209; Kevin E Davis and Florencia Marotta-Wurgler, "Contracting for Personal Data" (2019) 94 *New York University Law Review* 662, 681.

58 Barocas and Nissenbaum, "On Notice: The Trouble with Notice and Consent" (n 52) 4.

59 Alan F Westin, *Privacy and Freedom* (Atheneum 1967) 419–422. See also Stacy-Ann Elvy, "Commodifying Consumer Data in the Era of the Internet of Things" (2018) 59 *Boston College Law Review* 423, 475; Chris J Hoofnagle and Jennifer M Urban, "Alan Westin's Privacy Homo Economicus" (2014) 49 *Wake Forest Law Review* 261.

60 Frank Pasquale, "Two Narratives of Platform Capitalism" (2016) 35 *Yale Law & Policy Review* 309, 312.

61 Chris Jay Hoofnagle, "Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement" (2003) 29 *North Carolina Journal of International Law and Commercial Regulation* 595, 598–618.

62 Danielle Keats Citron and Frank Pasquale, "The Scored Society: Due Process for Automated Predictions Essay" (2014) 89 *Washington Law Review* 1, 8–18.

63 Alessandro Acquisti, "Privacy and Market Failures: Three Reasons for Concern, and Three Reasons for Hope" (2012) 477 *Journal on Telecommunications and High Technology Law* 227, 228.
64 See Chapter 3B.
65 Solove, "Introduction: Privacy Self-Management and the Consent Dilemma" (n 5) 1880.
66 Ibid.
67 James P Nehf, "Shopping for Privacy Online: Consumer Decision Making Strategies and the Emerging Market for Information Privacy" (2005) *University of Illinois Law Review, Technology & Policy* 1, 14–17.
68 Oren Bar-Gill, Omri Ben-Shahar, and Florencia Marotta-Wurgler, "Searching for the Common Law: The Quantitative Approach of the Restatement of Consumer Contracts" (2017) 84 *The University of Chicago Law Review* 7, 28; Thomas Haley, "Illusory Privacy" (2023) 98 *Indiana Law Journal* 75, 82–91; Gregory Klass, "Empiricism and Privacy Policies in the Restatement of Consumer Contract Law" (2019) 36 *Yale Journal on Regulation* 45, 85.
69 Nancy Kim, "Adhesive Terms and Reasonable Notice" (2022) 53 *Seton Hall Law Review* 2, 112.
70 Bar-Gill, Ben-Shahar and Marotta-Wurgler (n 68) 28. See also Scott Killingsworth, "Minding Your Own Business: Privacy Policies in Principle and in Practice" (1999) 7 *Journal of Intellectual Property Law* 57, 91–92.
71 *Douez v Facebook, Inc* (33 SCC) [8]; *Douez v Facebook, Inc* (BCCA 279) [9].
72 Jared S. Livingston, "Invasion Contracts: The Privacy Implications of Terms of Use Agreements in the Online Social Media Setting" (2011) 21 *Albany Law Journal of Science & Technology* 591, 601–604; Mark R Patterson, "Standardization of Standard-Form Contracts: Competition and Contract Implications" (2010) 52 *William and Mary Law Review* 327, 332; Shmuel I Becher and Esther Unger-Aviram, "The Law of Standard Form Contracts: Misguided Intuitions and Suggestions for Reconstruction" (2010) 8 *DePaul Business & Commercial Law Journal* 199, 212–214.
73 See Chapters 3B and 4B.
74 Michelle Cumyn, "Standard Form Contracts and the Erosion of Consent: Is There No Turning Back?" (draft).
75 Stefan Grundmann, "A Modern Standard Contract Terms Law from Reasonable Assent to Enhanced Fairness Control" (2019) 15 *European Review of Contract Law* 148, 153–154.
76 Ben-Shahar and Schneider, *More Than You Wanted to Know* (n 54) 73.
77 Tina Piper, "The Personal Information Protection and Electronic Documents Act: A Lost Opportunity to Democratize Canada's Technological Society" (2000) 23 *Dalhousie LJ* 253, 276–277.
78 Matt Brennan, "Timeline: Pamela Anderson and Tommy Lee's Sex Tape Saga, as It Happened" *Los Angeles Times* (2 February 2022) <https://perma.cc/29CE-HTYA>.
79 Marie-Claire Chappet, "What Pam & Tommy Teaches Us about the Double Standards of Celebrity" *Harper's BAZAAR* (3 February 2022) <https://perma.cc/G67W-H4F9>.
80 Pamela Anderson, *Love, Pamela: A Memoir of Prose, Poetry, and Truth* (Dey Street Books 2023) 127–129.
81 Ibid 129–133. *Pamela, a Love Story* (dir. Ryan White, 2023), min 53:00–56:00.
82 Shauna Snow, "Arts and Entertainment Reports from The Times, National and International News Services and the Nation's Press" *Los Angeles Times* (Los Angeles, 22 March 1997) <https://perma.cc/GD5W-JMUQ>; Brennan, "Timeline" (n 78).
83 Mary-Anne Franks, "Revenge Porn Reforms: A View from the Front Lines" (2017) 69 *Florida Law Review* 1251, 1267–1268; 'History / Mission / Vision' (*Cyber Civil Rights Initiative*) <https://perma.cc/P2ZV-WKUM>.

84 Andrea Slane and Ganaele Langlois, "Debunking the Myth of 'Not My Bad': Sexual Images, Consent, and Online Host Responsibilities in Canada" (2018) 30 *Canadian Journal of Women and the Law* 42, 58–63. See also Suzie Dunn and Alessia Petricone-Westwood, "More than 'Revenge Porn' Civil Remedies for the Nonconsensual Distribution of Intimate Images" *CCLA* (2018) 8. See *R v AC* [2017] ONCJ 317 [Canada].
85 Danielle Keats Citron, *The Fight for Privacy: Protecting Dignity, Identity, and Love in the Digital Age* (WW Norton 2022) 41–42.
86 *Walls v City of Petersburg* [1990] Court of Appeals, 4th Circuit 89-2357, 895 F 2d 188.
87 Ignacio Cofone and Adriana Robertson, "Privacy Harms" (2018) 69 *Hastings Law Journal* 1039, 1052–1053.
88 Richards, *Why Privacy Matters* (n 41) 21–34. See also Chapter 6B.
89 Danielle Citron and Mary Anne Franks, "Criminalizing Revenge Porn" (2014) 49 *Wake Forest Law Review* 345, 348; Ari Ezra Waldman, "Law, Privacy, and Online Dating: 'Revenge Porn' in Gay Online Communities" (2019) 44 *Law & Social Inquiry* 987, 1004; Caille Millner, "Public Humiliation over Private Photos" (*SFGate*, 10 February 2013) <https://perma.cc/7E33-JWDH> (quoting site operator as saying, "When you take a nude photograph of yourself and you send it to this other person, or when you allow someone to take a nude photograph of you, by your very actions you have reduced your expectation of privacy"); 'Civil Lawsuit on Revenge Porn' *The New York Times* (New York, 29 January 2015) <https://perma.cc/3GAP-BNC9?type=image>.
90 Amanda Levendowski, "Using Copyright to Combat Revenge Porn" (2013) 3 *New York University Journal of Intellectual Property and Entertainment Law* 422, 431–437.
91 *State v VanBuren* [2019] 214 A3d 791 (VT 95) [97].
92 *R v NN* [2019] ONCJ 18-34150; 18-37714, 512 [341–347] ("certainly there is a risk that when someone provides such images, as Mr. Connolly indicated in his submissions, that those images may find their way out into the public, and that is a cautionary tale").
93 See Tegan S Starr and Tiffany Lavis, "Perceptions of Revenge Pornography and Victim Blame" (2018) 12 *International Journal of Cyber Criminology* 427, 434–535; Tahlee Mckinlay and Tiffany Lavis, "Why Did She Send It in the First Place? Victim Blame in the Context of 'Revenge Porn'" 27 *Psychiatry, Psychology, and Law* 386, 391.
94 Citron, *Fight for Privacy* (n 85) 76–80.
95 Kashmir Hill, "The Secretive Company That Might End Privacy as We Know It" *The New York Times* (New York, 18 January 2020) <https://perma.cc/B2JF-547D>.
96 Scott Skinner-Thompson, "Agonistic Privacy & Equitable Democracy" (2021) 131 *Yale Law Journal Forum* 454, 459–461.
97 Julie E Cohen, *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice* (Yale University Press 2012) 111–114; Scott Skinner-Thompson, "Performative Privacy" (2017) 50 *U.C. Davis Law Review* 1673, 1678–1689.
98 Woodrow Hartzog, "The Public Information Fallacy" (2019) 99 *Boston University Law Review* 459, 518.
99 Scott Skinner-Thompson, *Privacy at the Margins* (Cambridge University Press 2020) 8.
100 See the infamous *Sipple v Chronicle Publishing Co* [1984] Court of Appeal, 1st Appellate Dist, 4th Div AO11998, 154 Cal App 3d 1040 [US].
101 Andrew E Taslitz, "Privacy as Struggle" (2007) 44 *San Diego Law Review* 501, 507; Scott Skinner-Thompson, "Privacy's Double Standards" (2018) 93 *Washington Law Review* 2051, 2061–2063.
102 Virginia Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor* (St Martin's Press 2018) 5–7.
103 Richards (n 41) 33.

104 Daniel Solove, *Nothing to Hide: The False Tradeoff Between Privacy and Security* (Yale University Press 2011) 1.

105 "Google's Schmidt Roasted for Privacy Comments" (*PCWorld*, 11 December 2009) <https://perma.cc/DDC7-M8QF>; "Google CEO On Privacy (VIDEO): 'If You Have Something You Don't Want Anyone To Know, Maybe You Shouldn't Be Doing It'" *Huffington Post* (New York, 18 March 2010) <https://perma.cc/PAQ4-7SWN>; Richard Esguerra, "Google CEO Eric Schmidt Dismisses the Importance of Privacy" (*Electronic Frontier Foundation*, 10 December 2009) <https://perma.cc/D4QP-2AMJ>.

106 Solove, *Nothing to Hide: The False Tradeoff Between Privacy and Security* (n 104); Daniel Solove, "'I've Got Nothing to Hide' and Other Misunderstandings of Privacy" (2007) 44 *San Diego Law Review* 745, 764–771.

107 Solove, *Nothing to Hide: The False Tradeoff Between Privacy and Security* (n 104) 747. See also Daniel Solove, "Why Privacy Matters Even If You Have 'Nothing to Hide' – The Chronicle of Higher Education" *The Chronicle Review* (15 May 2011) <https://perma.cc/3USQ-TM57>.

108 Bruce Schneier, "The Eternal Value of Privacy" (*Schneier on Security*, 18 May 2006) <https://perma.cc/6RQ5-JN8R>. See also Elizabeth Stoycheff, "Mass Surveillance Chills Online Speech Even When People Have 'Nothing to Hide'" *Slate* (3 May 2016) <https://perma.cc/DC2T-JQ29>; Geoffrey R Stone, "Freedom and Public Responsibility" *Chicago Tribune* (Chicago, 21 May 2006) 11 <https://perma.cc/522V-YE3T>.

109 Ramzi Kassem and Diala Shamas, "Rebellious Lawyering in the Security State" (2017) 23 *Clinical Law Review* 671, 688.

110 Rónán Duffy, "'If You Have Nothing to Hide, You Have Nothing to Fear': MP Accused of Quoting Nazi Leader" *TheJournal.ie* (Dublin, 4 November 2015) <https://perma.cc/3V3L-PAU2> (quote from MP Richard Graham defending the Investigatory Powers Act 2016). See also Jeffrey Rosen, *The Naked Crowd: Reclaiming Security and Freedom in an Anxious Age* (Reprint edition, Random House Trade Paperbacks 2005) 35–36.

111 "Investigation of Communist Activities in the State of Michigan, Part 6: Hearing before the H Comm on Un-American Activities" 5357.

112 See "Caller-ID Technology: Hearing before the Sub on Technology and the Law of the Comm on the Judiciary"; "US Customs Service Passenger Inspection Operations: Hearing before the Sub on Oversight of the H Committee on Ways and Means" 33–35.

113 Eugene Volokh, "Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking about You" (2000) 52 *Stanford Law Review* 1049, 1052–1059; Charles M Kahn, James McAndrews, and William Roberds, "Money Is Privacy" (2005) 46 *International Economic Review* 377; Jin-Hyuk Kim and Liad Wagman, "Screening Incentives and Privacy Protection in Financial Markets: A Theoretical and Empirical Analysis" (2015) 46 *The RAND Journal of Economics* 1.

114 Natasha Singer, "Sharing Data, but Not Happily" *The New York Times* (New York, 4 June 2015) <https://perma.cc/9KXW-GY8B>; Julia Angwin and Surya Mattu, "Facebook Doesn't Tell Users Everything It Really Knows…" (*ProPublica*, 27 December 2016) <https://perma.cc/R8B8-DJVE>; Siva Vaidhyanathan, "Don't Delete Facebook. Do Something about It" *The New York Times* (New York, 8 June 2018) <https://perma.cc/K7BD-JKWJ>; Dylan Curran, "Are You Ready? This Is All the Data Facebook and Google Have on You" *The Guardian* (London, 30 March 2018) <https://perma.cc/4YZ4-TUW9>.

115 Shoshana Zuboff, *The Age of Surveillance Capitalism* (1st ed., PublicAffairs 2019) 74–85.

116 Richard A Posner, *The Economics of Justice* (Harvard University Press 1983) 271.

117 Richard A Posner, *Economic Analysis of Law* (5th ed., Aspen 1998) 46.

118 Richard Posner, "The Right of Privacy" (1978) 12 *Georgia Law Review* 393, 404–405; Richard Posner, "An Economic Theory of Privacy" (1978) 2 *American Enterprise Institute Journal of Government and Society (Regulation)* 19, 21–22; Richard Posner, "The Economics of Privacy" (1981) 71 *The American Economic Review P&P* 405.

119 See generally Jeremias Prassl, *Humans as a Service: The Promise and Perils of Work in the Gig Economy* (1st ed., Oxford University Press 2018) 119–133.

120 Alex Rosenblat and Luke Stark, "Algorithmic Labor and Information Asymmetries: A Case Study of Uber's Drivers" (2016) 10 *International Journal of Communication* 3758.

121 See Karen Levy, *Data Driven: Truckers, Technology, and the New Workplace Surveillance* (Princeton University Press 2022) 52–76; Pauline T Kim and Matthew T Bodie, "Artificial Intelligence and the Challenges of Workplace Discrimination and Privacy" (2021) 35 *Journal of Labor and Employment Law* 289, 301–315.

122 Ifeoma Ajunwa, Kate Crawford and Jason Schultz, "Limitless Worker Surveillance" (2017) 105 *California Law Review* 735, 740–747; Ifeoma Ajunwa, "Algorithms at Work: Productivity Monitoring Applications and Wearable Technology as the New Data-Centric Research Agenda for Employment and Labor Law" (2018) 63 *Saint Louis University Law Journal* 21, 34–49.

123 Claudia Goldin and Cecilia Rouse, "Orchestrating Impartiality: The Impact of 'Blind' Auditions on Female Musicians" (2000) 90 *The American Economic Review* 715.

124 Ibid 715–716.

125 Ibid 738.

126 Jessica L Roberts, "Protecting Privacy to Prevent Discrimination" (2014) 56 *William & Mary Law Review* 2097, 2127–2140, 2157–2158; Ignacio Cofone, "Antidiscriminatory Privacy" (2019) 72 *SMU Law Review* 139, 156.

127 Patrik S Florencio and Erik D Ramanathan, "Secret Code: The Need for Enhanced Privacy Protections in the United States and Canada to Prevent Employment Discrimination Based on Genetic and Health Information" (2001) 39 *Osgoode Hall Law Journal* 77, 111–112; Rudy Kleysteuber, "Tenant Screening Thirty Years Later: A Statutory Proposal to Protect Public Records" (2007) 116 *The Yale Law Journal* 1344, 1369–1372; Nicholas Caivano, "Inaccessible Inclusion: Privacy, Disclosure and Accommodation of Mental Illness in the Workplace" (2016) 5 *Canadian Journal of Human Rights* 97, 117–127. See also Roberts, "Protecting Privacy to Prevent Discrimination" (n 126) 2127–2140, 2157–2158; Cofone, "Antidiscriminatory Privacy" (n 126) 140–147.

128 Nikita Aggarwal, "The Norms of Algorithmic Credit Scoring" (2021) 80 *The Cambridge Law Journal* 42, 52–60; Ignacio Cofone, "Algorithmic Discrimination Is an Information Problem" (2019) 70 *Hastings Law Journal* 1389, 1406–1416.

129 U.S. House of Representatives, "Testimony of Carter Brown – Hearing on The Equality Act (H.R. 5)" (Committee on The Judiciary Subcommittee on the Constitution, Civil Rights, and Civil Liberties, 2 April 2019) <https://perma.cc/73Q4-KBTD>.

130 See also *Altitude Express, Inc v Zarda* [2020] 590 US 17 140 Ct 1739; *Bostock v Clayton County, Georgia* [2020] 140 Ct 1731 590 US 140.

131 After the EEOC supported Cox, the case was settled. "Randstad Will Pay $50,000 to Settle EEOC Disability Discrimination Lawsuit" (*US EEOC*, 2 August 2016) <https://perma.cc/8CPN-3X2H>; *US EEOC v Randstad et al* [2011] Dist Court Maryland Civil Action No. RDB 10-3472.

132 Pauline Kim and Sharion Scott, "Discrimination in Online Employment Recruiting" (2019) 63 *St. Louis University Law Journal* 93, 115–118.

133 Stacy Hickox, "It's Time to Rein in Employer Drug Testing" (2017) 11 *Harvard Law & Policy Review* 419, 421–425.

134 The signal is far from perfect: Plenty of people who use recreational drugs are excellent employees and lots of people who pass drug tests are poor employees. The signal's noisiness attenuates the value of testing, but it doesn't diminish its harm.
135 There are additional reasons why someone might be uncomfortable with drug testing. These include the risk of false positives – that the test might incorrectly indicate that someone had drugs in their system.
136 Ignacio Cofone, "Nothing to Hide, But Something to Lose" (2020) 70 *University of Toronto Law Journal* 64, 73–80.
137 Confidentiality over the results wouldn't solve the problem. Although confidentiality may reduce the likelihood of further harm by third parties, it does nothing about the immediate harm of revealing the bundled information.
138 Alaska Statute, s 23.10.615; Florida Statute, s 440.102; Ohio Administrative Code, s 4123-17-58.
139 Cofone, "Nothing to Hide, But Something to Lose" (n 136) 81.
140 Neil Richards, *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age* (Oxford University Press 2015) 95–108.
141 Cofone, "Nothing to Hide, but Something to Lose" (n 136) 82, 88.
142 Richards, *Why Privacy Matters* (n 41) 111–163; Citron, *Fight for Privacy* (n 85) 105–130. See also Chapter 6A.
143 Andrea Peterson, "How Washington's Last Remaining Video Rental Store Changed the Course of Privacy Law" *Washington Post* (Washington, DC, 28 April 2014) <https://perma.cc/4E6M-8UCE>; Note, "The Video Privacy Protection Act as a Model Intellectual Privacy Statute" (2018) 131 Harvard Law Review 1766.
144 Video Privacy Protection Act of 1988, Pub. L. 100–618 (codified as 18 U.S.C. 2710-2711 (2012)).
145 Frank Pasquale and Arthur J Cockfield, "Beyond Instrumentalism: A Substantivist Perspective on Law, Technology, and the Digital Persona" (2018) *Michigan State Law Review* 821, 841–842.
146 See Chapter 3B.
147 See Omri Ben-Shahar, "Data Pollution" (2019) 11 *Journal of Legal Analysis* 104, 138–143.
148 See Chapter 2A.
149 Ibid.

2 PRIVACY MYTHS: RATIONALITY AND APATHY

1 Max Witysnki, "Behavioral Economics, Explained" *UChicago News* <https://perma.cc/3U5A-AS4W>.
2 Forbrukerrådet, "Deceived by Design" (27 June 2018) 31 <https://perma.cc/2WXM-6EAP>.
3 Ibid 32–34.
4 Alan L Chaikin, Valerian J Derlega, and Sarah J Miller, "Effects of Room Environment on Self-Disclosure in a Counseling Analogue" (1976) 23 *Journal of Counseling Psychology* 479, 481. See also John W Thibaut and Harold H Kelley, *The Social Psychology of Groups* (1st ed., Wiley 1959) 69.
5 Alessandro Acquisti and Jens Grossklags, "What Can Behavioral Economics Teach Us About Privacy ?" in Alessandro Acquisti and others (eds), *Digital Privacy: Theory, Technologies and Practices* (Auerbach Publications 2008) 363–369.
6 See eg, Myong Jin Won-Doornink, "Self-Disclosure and Reciprocity in Conversation: A Cross-National Study" (1985) 48 *Social Psychology Quarterly* 97, 100–103.

7 Alessandro Acquisti, Leslie John, and George Loewenstein, "The Impact of Relative Standards on the Propensity to Disclose" (2012) 49 *Journal of Marketing Research* 160, 172–174.
8 Youngme Moon, "Intimate Exchanges: Using Computers to Elicit Self-Disclosure from Consumers" (2000) 26 *Journal of Consumer Research* 323, 328–329.
9 Monika Taddicken, "The 'Privacy Paradox' in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure" (2014) 19 *Journal of Computer-Mediated Communication* 248, 267.
10 Adam Joinson and others, "Privacy, Trust, and Self-Disclosure Online" (2010) 25 *Human-Computer Interaction* 1, 17–19, 24–27.
11 Naresh K Malhotra, Sung S Kim, and James Agarwal, "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model" (2004) 15 *Information Systems Research* 336, 350. See also Craig Van Slyke and others, "Concern for Information Privacy and Online Consumer Purchasing" (2006) 7 *Journal of the Association for Information Systems* 415, 433–435; Tamara Dinev and Paul Hart, "An Extended Privacy Calculus Model for E-Commerce Transactions" (2006) 17 *Information Systems Research* 61, 63–64; David Gefen and others, "EGovernment Adoption" (2002) 83 *AMCIS 2002 Proceedings* 569, 571–572.
12 Joey F George, "The Theory of Planned Behavior and Internet Purchasing" (2004) 14 *Internet Research* 198, 204–207.
13 Heng Xu and others, "The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services" (2009) 26 *Journal of Management Information Systems* 135, 154–158.
14 Francesco Massara, Francesco Raggiotto, and W Gregory Voss, "Unpacking the Privacy Paradox of Consumers: A Psychological Perspective" (2021) 38 *Psychology & Marketing* 1814, 1816–1818.
15 Carlos Jensen, Colin Potts, and Christian Jensen, "Privacy Practices of Internet Users: Self-Reports versus Observed Behavior" (2005) 63 *International Journal of Human-Computer Studies* 203, 223. See also Rahul Gadekar and Saumya Pant, "Exploring Facebook Users' Privacy Knowledge, Enactment and Attitude: A Study on Indian Youth" (2015) 5 *International Journal of Communication Research* 273, 278.
16 Patrick Gage Kelley, Lorrie Faith Cranor, and Norman Sadeh, "Privacy as Part of the App Decision-Making Process," *SIGCHI Conference on Human Factors in Computing Systems* (Association for Computing Machinery 2013) 3401.
17 Yong Jin Park, "Digital Literacy and Privacy Behavior Online" (2011) 40 *Communication Research* 215, 223–225; Carlos Jensen and Colin Potts, "Privacy Policies as Decision-Making Tools: An Evaluation of Online Privacy Notices," *SIGCHI Conference on Human Factors in Computing Systems* (Association for Computing Machinery 2004) 475–476; Joel R Reidenberg and others, "Disagreeable Privacy Policies: Mismatches between Meaning and Users Understanding" (2015) 30 *Berkeley Technology Law Journal* 39, 87–88.
18 Alessandro Acquisti, Curtis Taylor, and Liad Wagman, "The Economics of Privacy" (2016) 54 *Journal of Economic Literature* 442, 449, 477–478.
19 Acquisti and Grossklags, "What Can Behavioral Economics Teach Us about Privacy?" (n 5) 367.
20 Joseph Turow and others, "Americans Reject Tailored Advertising and Three Activities That Enable It" (2009) 21.
21 Iris van Ooijen and Helena U. Vrabec, "Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective" (2019) 42 *Journal of*

Consumer Policy 91, 99; Kirsten Martin, "Privacy Notices as Tabula Rasa: An Empirical Investigation into How Complying with a Privacy Notice Is Related to Meeting Privacy Expectations Online" (2015) 34 *Journal of Public Policy & Marketing* 210, 211.

22 Chris Jay Hoofnagle and Jennifer King, "Research Report: What Californians Understand About Privacy Online" (3 September 2008) 4 <https://perma.cc/A4EP-Y7YT>.

23 Chris J Hoofnagle and Jennifer M Urban, "Alan Westin's Privacy Homo Economicus" (2014) 49 *Wake Forest Law Review* 261, 281–282.

24 Kirsten Martin, "Do Privacy Notices Matter? Comparing the Impact of Violating Formal Privacy Notices and Informal Privacy Norms on Consumer Trust Online" (2016) 45 *The Journal of Legal Studies* s191, 204–206. See also Bettina Berendt, Oliver Günther, and Sarah Spiekermann, "Privacy in E-Commerce: Stated Preferences vs. Actual Behavior" (2005) 48 *Communications of the Association for Computing Machinery* 101, 104 (finding no statistically significant impact).

25 Acquisti and Grossklags, "What Can Behavioral Economics Teach Us About Privacy ?" (n 5) 370–371.

26 Alessandro Acquisti, Leslie John, and George Loewenstein, "What Is Privacy Worth?" (2013) 42 *Journal of Legal Studies* 249, 267–269. See also Cass R Sunstein, "Valuing Facebook" (2020) 4 *Behavioural Public Policy* 370.

27 A. G. Winegar and C. R. Sunstein, "How Much Is Data Privacy Worth? A Preliminary Investigation" (2019) 42 *Journal of Consumer Policy* 425, 426.

28 Aleecia M McDonald and Lorrie Faith Cranor, "Americans' Attitudes about Internet Behavioral Advertising Practices," *Proceedings of the 9th Annual ACM Workshop on Privacy in the Electronic Society* (Association for Computing Machinery 2010) 70–71. See also Aleecia McDonald and Lorrie Faith Cranor, "Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising," *Telecommunications Policy Research Conference* (2010) 25–27.

29 Jens Grossklags and Alessandro Acquisti, "When 25 Cents Is Too Much: An Experiment on Willingness-to-Sell and Willingness-to-Protect Personal Information," *Workshop on the Economics of Information Security* (2007) 3, 12.

30 Han Li, Rathindra Sarathy and Heng Xu, "Understanding Situational Online Information Disclosure as a Privacy Calculus" (2010) 51 *Journal of Computer Information Systems* 62, 68.

31 Russell Korobkin, "The Endowment Effect and Legal Analysis" (2003) 97 *Northwestern University Law Review* 1227, 1228.

32 Alessandro Acquisti, Leslie John, and George Loewenstein, "What Is Privacy Worth?" (2013) 42 *The Journal of Legal Studies* 249, 267.

33 Winegar and Sunstein, "How Much Is Data Privacy Worth?" (n 27) 429–430.

34 Greg Glassman, "Understanding CrossFit" *CrossFit Journal* (1 April 2007) <https://perma.cc/N767-LFKK>.

35 F. H. Knight, "Risk, Uncertainty and Profit" (Hart, Schaffner & Marx: Houghton Mifflin Company 1921); Julia Köhn, *Uncertainty in Economics: A New Approach* (Springer International Publishing 2017).

36 Laura Brandimarte, Alessandro Acquisti, and George Loewenstein, "Misplaced Confidences: Privacy and the Control Paradox" (2012) 4 *Social Psychological and Personality Science* 340, 345–346.

37 Acquisti and Grossklags, "What Can Behavioral Economics Teach Us About Privacy?" (n 5) 369.

38 Bernardo Reynolds and others, "Sharing Ephemeral Information in Online Social Networks: Privacy Perceptions and Behaviours" in Pedro Campos and others (eds), *Human-Computer Interaction (INTERACT)* (Springer 2011) 204.

39 Joseph Turow, "Americans and Online Privacy: The System Is Broken," *The University of Pennsylvania Annenberg Public Policy Center Report* (2003) 25.

40 Alessandro Acquisti and Jens Grossklags, "Privacy and Rationality in Individual Decision Making" (2005) 3 *Institute of Electrical and Electronics Engineers Security and Privacy Magazine* 7 (comparing survey data with data from the United States Federal Trade Commission).

41 George Milne and Mary Culnan, "Strategies for Reducing Online Privacy Risks: Why Consumers Read (or Don't Read) Online Privacy Notices" (2004) 18 *Journal of Interactive Marketing* 15, 20–21; Canada, "Privacy Enhancing Technologies – A Review of Tools and Techniques" (*Office of the Privacy Commissioner of Canada*, 15 November 2017) <https://perma.cc/G4GP-9ME8>.

42 Acquisti and Grossklags, "What Can Behavioral Economics Teach Us about Privacy ?" (n 5) 368.

43 Emmanuel Sebastian Udoh and Abdulwahab Alkharashi, "Privacy Risk Awareness and the Behavior of Smartwatch Users: A Case Study of Indiana University Students," *Future Technologies Conference (FTC)* (IEEE 2016) 929.

44 Haein Lee, Hyejin Park, and Jinwoo Kim, "Why Do People Share Their Context Information on Social Network Services? A Qualitative Study and an Experimental Study on Users' Behavior of Balancing Perceived Benefit and Risk" (2013) 71 *International Journal of Human-Computer Studies* 862, 867.

45 Susanne Barth and others, "Putting the Privacy Paradox to the Test: Online Privacy and Security Behaviors among Users with Technical Knowledge, Privacy Awareness, and Financial Resources" (2019) 41 *Telematics and Informatics* 55, 64.

46 See eg, Cory Doctorow, "Why Is It so Hard to Convince People to Care about Privacy?" *The Guardian* (London, 2 October 2015) <https://perma.cc/54QK-5R4U>.

47 Stephen J. Dubner, "Why Are There So Many Bad Bosses?" (*Freakonomics*, 2 March 2022) <https://perma.cc/KXB4-3W3B> ("There is a lot of discussion about privacy and privacy regulation these days. And you hear a lot of people saying how their privacy is important to them. And then you turn to them and say, 'Here's a Snickers bar. Could I have your mother's maiden name?' And they say yes. So it's a little bit confusing when you tell me that you really care about privacy, and then you just scroll down on every app you download and click yes, yes, yes. That doesn't tell me that you really care about privacy.")

48 Daniel J Solove, "The Myth of the Privacy Paradox" (2021) 89 *George Washington Law Review* 1, 4–11. See eg, Nick Ismail, "People Don't Care about Privacy (and That's Ok, Probably)" (*Information Age*, 20 July 2017) <https://perma.cc/R5B8-QBNE>.

49 Susanne Barth and Menno DT de Jong, "The Privacy Paradox – Investigating Discrepancies between Expressed Privacy Concerns and Actual Online Behavior – A Systematic Literature Review" (2017) 34 *Telematics and Informatics* 1038, 1039; Nina Gerber, Paul Gerber, and Melanie Volkamer, "Explaining the Privacy Paradox: A Systematic Review of Literature Investigating Privacy Attitude and Behavior" (2018) 77 *Computers & Security* 226, 227.

50 See Chapter 1B.

51 Ruwan Bandara, Mario Fernando, and Shahriar Akter, "Explicating the Privacy Paradox: A Qualitative Inquiry of Online Shopping Consumers" (2020) 52 *Journal of Retailing and Consumer Services* 1, 5–6.

52 Sarah Spiekermann, Jens Grossklags, and Bettina Berendt, "E-Privacy in 2nd Generation E-Commerce: Privacy Preferences versus Actual Behavior" in Michael Wellman and Yoav Shoham (eds), *Proceedings of the Third ACM Conference on Electronic Commerce* (ACM Press 2001) 45.

53 Berendt, Günther, and Spiekermann, "Privacy in E-Commerce: Stated Preferences vs. Actual Behavior" (n 24) 104.
54 Alessandro Acquisti and Jens Grossklags, "Privacy and Rationality in Individual Decision Making" (2005) 3 *IEEE Security and Privacy Magazine* 26, 31.
55 Spyros Kokolakis, "Privacy Attitudes and Privacy Behaviour: A Review of Current Research on the Privacy Paradox Phenomenon" (2017) 64 *Computers & Security* 122, 123–126; Allison Woodruff and others, "Would a Privacy Fundamentalist Sell Their DNA for $1000 … If Nothing Bad Happened as a Result? The Westin Categories, Behavioral Intentions, and Consequences," *10th Symposium On Usable Privacy and Security* (2014) 12 <https://perma.cc/KDW4-B7SG>.
56 Alessandro Acquisti and Ralph Gross, "Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook," *Proceedings of the Sixth Workshop on Privacy Enhancing Technologies* (Robinson College, Cambridge University 2006) 11.
57 Ibid 15.
58 Manuel Rudolph, Denis Feth, and Svenja Polst, "Why Users Ignore Privacy Policies – A Survey and Intention Model for Explaining User Privacy Behavior" in Masaaki Kurosu (ed), *Human-Computer Interaction. Theories, Methods, and Human Issues*, vol. 10901 (Springer 2018) 591.
59 Emily Christofides, Amy Muise, and Serge Desmarais, "Information Disclosure and Control on Facebook: Are They Two Sides of the Same Coin or Two Different Processes?" (2009) 12 *CyberPsychology & Behavior* 341.
60 Nicola Jentzsch, Sören Preibusch, and Andreas Harasser, "Study on Monetising Privacy: An Economic Model for Pricing Personal Information" (*European Network and Information Security Agency*, 2012) 5 <https://perma.cc/3Z3V-RMG4>.
61 Alastair Beresford, Dorothea Kübler, and Sören Preibusch, "Unwillingness to Pay for Privacy: A Field Experiment" [2012] *Economics Letters* 25, 26–27.
62 Garrett Glasgow, Sarah Butler, and Samantha Iyengar, "Survey Response Bias and the 'Privacy Paradox': Evidence from a Discrete Choice Experiment" (2020) 28 *Applied Economics Letters* 625, 627–628.
63 Kirsten Martin, "Manipulation, Privacy, and Choice" (2022) 23 *North Carolina Journal of Law & Technology* 452, 502. See also Solove, "The Myth of the Privacy Paradox" (n 48) 27–31.
64 Paul Hitlin, Lee Rainie, and Kenneth Olmstead, "Facebook Algorithms and Personal Data" (*Pew Research Center*, 16 January 2019) <https://perma.cc/47UY-KKML>.
65 Brooke Auxier and others, "Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information" (*Pew Research Center*, 15 November 2019) <https://perma.cc/YBL6-Q3QB>.
66 Steven Englehardt and Arvind Narayanan, "Online Tracking: A 1-Million-Site Measurement and Analysis" (*Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 2016) 1399 <https://perma.cc/V4JZ-BLLL>.
67 Matt Warman, "EU Fights 'Fierce Lobbying' to Devise Data Privacy Law" *The Telegraph* (London, 9 February 2012) <https://perma.cc/UBU3-D5N3>.
68 Paul Schwartz and Daniel Solove, "The PII Problem: Privacy and a New Concept of Personally Identifiable Information" (2011) 86 *NYU Law Review* 1814, 1853;
Blase Ur and others, "Smart, Useful, Scary, Creepy: Perceptions of Online Behavioral Advertising Perceptions of Online Behavioral Advertising," *SOUPS* (ACM Press 2012) 6.
69 Katherine Strandburg, "Free Fall: The Online Market's Consumer Preference Disconnect" (2013) 430 *University of Chicago Legal Forum* 95, 131.
70 Acquisti and Grossklags, "What Can Behavioral Economics Teach Us about Privacy?" (n 5) 4; Acquisti and Grossklags, "Privacy and Rationality in Individual Decision Making" (n 54) 30.

71 Luc Wathieu and Allan Friedman, "An Empirical Approach to Understanding Privacy Valuation" (2007) No. 07-075 HBS Marketing Research Paper https://perma.cc/LNL4-9R7P; Leslie John, Alessandro Acquisti, and George Loewenstein, "Strangers on a Plane: Context-Dependent Willingness to Divulge Sensitive Information" (2011) 37 *Journal of Consumer Research* 858, 868.

72 Julia Gideon and others, "Power Strips, Prophylactics, and Privacy, Oh My!" (2006) Symposium on Usable Privacy and Security (SOUPS) <https://perma.cc/E7A6-DYAD>; Janice Tsai and others, "The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study" (2011) 22 *Information Systems Research* 254, 263.

73 Zeynep Tufekci, "Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites" (2008) 28 *Bulletin of Science, Technology & Society* 20, 31–34.

74 Kirsten Martin and Helen Nissenbaum, "What Is It about Location?" (2020) 35 *Berkeley Technology Law Journal* 251, 301–302; Kirsten Martin and Helen Nissenbaum, "Measuring Privacy: An Empirical Test Using Context to Expose Confounding Variables" (2016) 18 *Columbia Science and Technology Law Review* 176, 215. See also Giles D'Souza and Joseph E Phelps, "The Privacy Paradox: The Case of Secondary Disclosure" (2009) 7 *Review of Marketing Science* 1, 20–21.

75 Kirsten Martin and Helen Nissenbaum, "Privacy Interests in Public Records: An Empirical Investigation" (2017) 31 *Harvard Journal of Law & Technology (Harvard JOLT)* 111, 140.

76 Kirsten Martin, "Breaking the Privacy Paradox: The Value of Privacy and Associated Duty of Firms" (2020) 30 *Business Ethics Quarterly* 65, 87.

77 Bernhard Debatin and others, "Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences" (2009) 15 *Journal of Computer-Mediated Communication* 83, 94.

78 See Chapters 3A, 4B.

79 See Chapter 3C.

80 Peter Swire and Robert Litan, *None of Your Business: World Data Flows, Electronic Commerce and the European Privacy Directive* (1998) 8.

81 Hanbyul Choi, Jonghwa Park, and Yoonhyuk Jung, "The Role of Privacy Fatigue in Online Privacy Behavior" (2018) 81 *Computers in Human Behavior* 42, 44–48.

82 Bandara, Fernando and Akter, "Explicating the Privacy Paradox" (n 51) 4.

83 Antti Oulasvirta and others, "Long-Term Effects of Ubiquitous Surveillance in the Home," *Proceedings of the 2012 ACM Conference on Ubiquitous Computing* (Association for Computing Machinery 2012) 49; Sangmi Chai and others, "Internet and Online Information Privacy: An Exploratory Study of Preteens and Early Teens" (2009) 52 *IEEE Transactions on Professional Communication* 167, 171, 176.

84 Alessandro Acquisti, "Privacy in Electronic Commerce and the Economics of Immediate Gratification" in Jack Breese, Joan Feigenbaum, and Margo Seltzer (eds), *Proceedings of the Fifth ACM Conference on Electronic Commerce* (ACM Press 2004); Alessandro Acquisti and Jens Grossklags, "Privacy Attitudes and Privacy Behavior" in L Jean Camp and Stephen Lewis (eds), *The Economics of Information Security* (Kluwer 2004).

85 Acquisti, "Privacy in Electronic Commerce and the Economics of Immediate Gratification" (n 84) 27.

86 Christofides, Muise, and Desmarais, "Information Disclosure and Control on Facebook" (n 59) 343; Stephane Rothen and others., "Disentangling the Role of Users' Preferences and Impulsivity Traits in Problematic Facebook Use" (2018) 13 *Plos One* <https://perma.cc/S94T-ZAUS>; Acquisti and Grossklags, "Privacy and Rationality in Individual Decision Making" (n 54) 31–32; Kokolakis, "Privacy Attitudes and Privacy Behaviour" (n 55) 130.

87 Christopher F Chabris, David I Laibson, and Jonathon P Schuldt, "Intertemporal Choice" in Steven N Durlauf and Lawrence E Blume (eds), *The New Palgrave Dictionary of Economics* (2nd ed., Nature Publishing Group 2008) 537–538.
88 Ted O'Donoghue and Matthew Rabin, "Doing It Now or Later" (1999) 89 *The American Economic Review* 103, 120.
89 Shane Frederick, George Loewenstein, and Ted O'Donoghue, "Time Discounting and Time Preference: A Critical Review" (2002) 40 *Journal of Economic Literature* 351, 382.
90 Peter Sozou, "On Hyperbolic Discounting and Uncertain Hazard Rates" (1998) 265 *Proceedings of the Royal Society of Biological Sciences* 2015.
91 See generally Todd Rogers, Katherine L Milkman, and Kevin G Volpp, "Commitment Devices: Using Initiatives to Change Behavior" (2014) 311 *JAMA* 2065.
92 Ibid.
93 Partha Dasgupta and Eric Maskin, "Uncertainty and Hyperbolic Discounting" (2005) 95 *The American Economic Review* 1290, 1292–1294.
94 Yoram Halevy, "Strotz Meets Allais: Diminishing Impatience and the Certainty Effect" (2008) 98 *The American Economic Review* 1145, 1145–1146; Yoram Halevy, "Time Consistency: Stationarity and Time Invariance" (2015) 83 *Econometrica* 335, 328.
95 danah boyd and Eszter Hargittai, "Facebook Privacy Settings: Who Cares?" (2010) 15 *First Monday* <https://perma.cc/3BZ2-EAT6>.
96 Gideon and others, "Power Strips, Prophylactics, and Privacy, Oh My!" (n 72).
97 Wathieu and Friedman, "An Empirical Approach to Understanding Privacy Valuation" (n 71).
98 Tsai and others (n 72) 255.
99 Sonja Utz and Nicole Krämer, "The Privacy Paradox on Social Network Sites Revisited: The Role of Individual Characteristics and Group Norms" (2009) 3 *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* 10.
100 Tobias Dienlin and Sabine Trepte, "Is the Privacy Paradox a Relic of the Past? An in-Depth Analysis of Privacy Attitudes and Privacy Behaviors" (2015) 45 *European Journal of Social Psychology* 285, 289–295.
101 Leslie John, Alessandro Acquisti, and George Loewenstein, "Strangers on a Plane: Context-Dependent Willingness to Divulge Sensitive Information" (2011) 37 *Journal of Consumer Research* 858, 868.
102 Ralph Gross and Alessandro Acquisti, "Information Revelation and Privacy in Online Social Networks," *Proceedings of the 2005 ACM workshop on Privacy in the electronic society* (Association for Computing Machinery 2005) 78.
103 Michelle Madejski, Maritza Johnson, and Steven M Bellovin, "A Study of Privacy Settings Errors in an Online Social Network," *10th IEEE International Conference on Pervasive Computing and Communications (PERCOM Workshops)* (2012) 344; Reynolds and others, "Sharing Ephemeral Information in Online Social Networks" (n 38) 204, 211.
104 Wathieu and Friedman, "An Empirical Approach to Understanding Privacy Valuation" (n 71).
105 Ignacio Cofone, "A Healthy Amount of Privacy: Quantifying Privacy Concerns in Medicine" (2017) 65 *Cleveland State Law Review* 1, 4–7.
106 Neil Richards, *Why Privacy Matters* (Oxford University Press 2021) 45–47; Shoshana Zuboff, *The Age of Surveillance Capitalism* (1st ed., PublicAffairs 2019) 293–299.
107 Ari Ezra Waldman, "Privacy, Notice, and Design" (2018) 21 *Stanford Technology Law Review* 129, 134.

108 Ryan Calo, "Digital Market Manipulation" (2014) 82 *George Washington Law Review* 995, 999, 1003–1008.
109 Forbrukerrådet, "Deceived by Design" (n 2) 3.
110 Ibid.
111 Ibid 26.
112 Ibid 22.
113 See Gaia Bernstein, *Unwired: Regaining Control over Addictive Technologies* (forthcoming, Cambridge University Press 2023). See also Madelyn Rose Sanfilippo and Yafit Lev-Aretz, "Topic Polarization and Push Notifications" (2019) 24 *First Monday* 1.
114 Punam Keller and others, "Enhanced Active Choice: A New Method to Motivate Behavior Change" (2011) 21 *Journal of Consumer Psychology* 376, 379.
115 Arunesh Mathur and others, "Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites" (2019) 3 *Proceedings of the ACM on Human-Computer Interaction* 1, 4.
116 Johan Van Asch, "How to Delete a Duolingo Account?" (*AccountDeleters*, 7 August 2015) <https://perma.cc/Z6BS-T2KD>.
117 Waldman, "Privacy, Notice, and Design" (n 107) 169.
118 Idris Adjerid, Alessandro Acquisti, and George Loewenstein, "Choice Architecture, Framing, and Cascaded Privacy Choices" (2019) 65 *Management Science* 2267; Idris Adjerid and others, "Sleights of Privacy: Framing, Disclosures, and the Limits of Transparency," *Ninth Symposium on Usable Privacy and Security* (2013) 226.
119 Delphine Reinhardt, Franziska Engelmann, and Matthias Hollick, "Can I Help You Setting Your Privacy? A Survey-Based Exploration of Users' Attitudes towards Privacy Suggestions," *13th International Conference on Advances in Mobile Computing and Multimedia* (2015) 353–354.
120 Aleecia M. McDonald and others, "A Comparative Study of Online Privacy Policies and Formats" in Ian Goldberg and Mikhail J. Atallah (eds), *Privacy Enhancing Technologies* (Springer 2009) 49–51. See also Hana Habib and others, "An Empirical Analysis of Data Deletion and Opt-Out Choices on 150 Websites," *USENIX Symposium on Usable Privacy and Security (SOUPS)* (USENIX Association 2019) 396 <https://perma.cc/U7QH-BFFQ>; Hana Habib and others, "'It's a Scavenger Hunt': Usability of Websites' Opt-Out and Data Deletion Choices," *CHI Conference on Human Factors in Computing Systems* (2020) 2.
121 Erin Schroeder, "UX Dark Patterns: Manipulinks and Confirmshaming" (*UX Booth*, 4 June 2019) <https://perma.cc/VP3P-66W3>.
122 Jamie Luguri and Lior Jacob Strahilevitz, "Shining a Light on Dark Patterns" (2021) 13 *Journal of Legal Analysis* 43, 47; Yichen Wang and others, "Jump on the Bandwagon? – Characterizing Bandwagon Phenomenon in Online NBA Fan Communities" 410, 411.
123 Martin, "Manipulation, Privacy, and Choice" (n 63) 463–465.
124 Ibid 482–486.
125 William McGeveran, "The Law of Friction The Frontiers of Consumer Protection" (2013) 2013 *University of Chicago Legal Forum* 15, 45; Ido Kilovaty, "Legally Cognizable Manipulation" (2019) 34 *Berkeley Technology Law Journal* 449, 469; Brett Frischmann, "Nudging Humans" (2022) 36 *Social Epistemology* 129, 137–168.
126 Martin, "Manipulation, Privacy, and Choice" (n 63) 487–489.
127 Nitasha Tiku, "Welcome to the Next Phase of the Facebook Backlash" (*Wired*, 21 May 2017) <https://perma.cc/TPJ6-BG2B>; Darren Davidson, "Facebook Targets 'Insecure' Young People" *The Australian* (Surry Hills, 1 May 2017) <https://perma.cc/S9CU-HW33>; "Comments on Research and Ad Targeting" (*Meta*, 30 April 2017) <https://perma.cc/KKS5-36HT>.
128 Richards, *Why Privacy Matters* (n 106) 187.

129 Martin, "Manipulation, Privacy, and Choice" (n 63) 456–458, 509.
130 Richard H Thaler, "Nudge, Not Sludge" (2018) 361 *Science* 431. See also Cass R Sunstein, *Sludge: What Stops Us from Getting Things Done and What to Do about It* (The MIT Press 2021) 1–20.
131 Ian R Kerr, "The Devil Is in the Defaults" (2017) 4 *Critical Analysis of Law* 91, 103.
132 Brigitte Madrian and Dennis Shea, "The Power of Suggestion: Inertia in 401(k) Participation and Savings Behavior" (2001) 116 *Quarterly Journal of Economics* 1149, 1173.
133 Eric Johnson and Daniel Goldstein, "Medicine: Do Defaults Save Lives?" (2003) 302 *Science* 1338, 1338; Julie Downs, George Loewenstein, and Jessica Wisdom, "Strategies for Promoting Healthier Food Choices" (2009) 99 *American Economic Review* 159, 160. See also Eric Johnson and Daniel Goldstein, "Defaults and Donation Decisions" (2004) 78 *Transplantation* 1713.
134 See eg, David Cohen and Jack Knetsch, "Judicial Choice and the Disparities between Measures of Economic Values" (1992) 30 *Osgoode Hall Law Journal* 737, 747; Colin Camerer, "Prospect Theory in the Wild: Evidence from the Field" in Daniel Kahneman and Amos Tversky (eds), *Choices, Values and Frames* (Cambridge University Press 2000) 294–295; Downs, Loewenstein, and Wisdom, "Strategies for Promoting Healthier Food Choices" (n 133).
135 Eric Johnson, Steven Bellman, and Gerald Lohse, "Defaults, Framing and Privacy: Why Opting In-Opting Out" (2002) 13 *Marketing Letters* 5, 9.
136 Johnson and Goldstein, "Defaults and Donation Decisions" (n 133) 1714–1715.
137 Debatin and others, "Facebook and Online Privacy" (n 77) 93, 100.
138 Johnson, Bellman, and Lohse, "Defaults, Framing and Privacy: Why Opting In-Opting Out" (n 135) 13; Craig McKenzie, Michael Liersch and Stacey Finkelstein, "Recommendations Implicit in Policy Defaults" (2006) 17 *Psychological Science* 414, 418–419.
139 William Samuelson and Richard Zeckhauser, "Status Quo Bias in Decision Making" (1988) 1 *Journal of Risk and Uncertainty* 7, 8; Daniel Kahneman, Jack Knetsch, and Richard Thaler, "Anomalies: The Endowment Effect, Loss Aversion, and Status Quo Bias" (1991) 5 *Journal of Economic Perspectives* 193, 198.
140 Alessandro Acquisti, Laura Brandimarte, and George Loewenstein, "Privacy and Human Behavior in the Age of Information" (2015) 347 *Science* 509, 512.
141 Russell Korobkin, "The Status Quo Bias and Contract Default Rules" (1998) 83 *Cornell Law Review* 608, 625.
142 Russell Korobkin, "The Endowment Effect and Legal Analysis" (2003) 97 *Northwestern University Law Review* 1227, 1228; Cass Sunstein, "Switching the Default Rule" (2002) 77 *NYU Law Review* 106.
143 Aurelia Tamò-Larrieux, *Designing for Privacy and Its Legal Framework: Data Protection by Design and Default for the Internet of Things* (Springer 2018) 36.
144 Ibid.
145 Jill Bronfman and Johanna Gunawan, "Right at the Source: Privacy Manipulative Design in User Interfaces" (*Common Sense Education*, 13 October 2021) <https://perma.cc/WBF3-UYTL>.
146 Matt McKeon, "The Evolution of Privacy on Facebook" (2010) <https://perma.cc/LP7G-ET2V>.
147 Frederic D. Stutzman, Ralph Gross, and Alessandro Acquisti, "Silent Listeners: The Evolution of Privacy and Disclosure on Facebook" (2013) 4 *Journal of Privacy and Confidentiality* 7, 31.
148 Waldman, "Privacy, Notice, and Design" (n 107) 169.

149 Ari Ezra Waldman, *Industry Unbound: The Inside Story of Privacy, Data, and Corporate Power* (Cambridge University Press 2021) 161–209.
150 Zuboff, *Age of Surveillance Capitalism* (n 106) 130–155.
151 Woodrow Hartzog, *Privacy's Blueprint: The Battle to Control the Design of New Technologies* (Harvard University Press 2018) 160.
152 See eg, Mark Sullivan, "These Are the Deceptive Design Tricks and Dark Patterns That Steer Your Clicks Each Day" (*Fast Company*, 25 June 2019) <https://perma.cc/2TBE-EMBH>; Henry Wong, "Inside the Deceptive Design World of Dark Patterns" (*Design Week*, 9 March 2020) <https://perma.cc/XK9M-9T9Q>.
153 Daniel Susser, Beate Roessler, and Helen Nissenbaum, "Online Manipulation: Hidden Influences in a Digital World" (2019) 4 *Georgetown Law Technology Review* 1, 17.
154 Harry Bignull, "Dark Patterns: Fighting User Deception Worldwide" (*Dark Patterns*, 5 January 2017) <https://perma.cc/SSE5-A7NB>. Another definition is that they are "tricks used in websites and apps that make you do things that you didn't mean to, like buying or signing up for something." See Harry Bignull, "What Is Deceptive Design?" (*Deceptive Design*) <https://perma.cc/3MSF-UEQP>.
155 Luguri and Strahilevitz, "Shining a Light on Dark Patterns" (n. 122) 81.
156 Arunesh Mathur, Mihir Kshirsagar, and Jonathan Mayer, "What Makes a Dark Pattern … Dark? Design Attributes, Normative Considerations, and Measurement Methods," *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (ACM 2021) 7–8; Colin M Gray and others, "The Dark (Patterns) Side of UX Design," *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (2018) 5–7.
157 Reddit, "FT.Com, Making It Very Easy to Sign up for a Monthly Charge of 28 € Instead of Cancelling Subscription Which Was My Intended Purpose" <https://perma.cc/K3TC-L4ZE>.
158 Deceptive Design [@darkpatterns], "Cancelling NYT Tweet" (*Twitter*, 7 January 2022) <https://perma.cc/JXQ7-22EK>; "Cancel Your Subscription" *New York Times* <https://perma.cc/27MU-Q8Y5>; *Moses v The NY Times Co* [2021] United States District Court, SD New York Civil Action 1:20-cv-04658-RA, Civil Action 1:20-cv-04658-RA U S Dist Court SD N Y [16]–[20].
159 Forbrukerrådet, "Deceived by Design" (n 2) 34–39.
160 Gray and others, "The Dark (Patterns) Side of UX Design" (n 156) 3, 7.
161 Simon Gabriel [@SimonGabriel], "Dark Patterns Tweet" (*Twitter*, 28 June 2021) <https://perma.cc/3FSN-NHBD>.
162 Barclays UK Help [@BarclaysUKHelp], '@kimeshan_ Tweet' (*Twitter*, 6 January 2022) <https://perma.cc/2HAJ-PKLX>.
163 Gray and others, "The Dark (Patterns) Side of UX Design" (n 156) 6–7.
164 Reddit, "Booking.Com Pretends That It Has a Working Button for Delete Account" <https://perma.cc/9ZJJ-24EB>. See also "Interface Interference" (*UXP2: Dark Patterns*, 2022) <https://perma.cc/JLQ2-7VZQ>.
165 Mark Di Stefano [@MarkDiStef], "France Fining Facebook and Google Tweet" (*Twitter*, 6 January 2022) <https://perma.cc/7MWE-D52X>.
166 "How Do I Delete My Profile?" (*Bumble*, 2022) <https://perma.cc/V9LR-UJDE>.
167 Luguri and Strahilevitz, "Shining a Light on Dark Patterns" (n 122) 47.
168 Christoph Bösch and others, "Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns" (237AD) 4 *Proceedings on Privacy Enhancing Technologies* 237, 249, 251–252. See also Chapter 4A.
169 Deceptive Design [@darkpatterns], "Ebay.Co.Uk Tweet" (*Twitter*, 13 December 2021) <https://perma.cc/UD75-EVZF>.

170 Forbrukerrådet, "Deceived by Design" (n 2) 16.
171 Luguri and Strahilevitz, "Shining a Light on Dark Patterns" (n 122) 66.
172 Mathur and others, "Dark Patterns at Scale" (n 115) 14–19. See also Mathur, Kshirsagar, and Mayer, "What Makes a Dark Pattern … Dark?" (n 156) 7–8.
173 Joe Lanman [@joelanman], "@NewYorker Dark Pattern Tweet" (*Twitter*, 28 June 2021) <https://perma.cc/UHZ6-9V45>.
174 Gray and others, "The Dark (Patterns) Side of UX Design" (n 156) 4–5.
175 "Duolingo Push" (*Duolingo*) <https://perma.cc/K5MQ-3CKH>.
176 Linda Di Geronimo and others, "UI Dark Patterns and Where to Find Them: A Study on Mobile Applications and User Perception," *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (ACM 2020) 5.
177 GDPR Article 25.
178 European Data Protection Supervisor, "Preliminary Opinion on Privacy by Design" <https://perma.cc/7V3Z-8TF3> 1–6 (transparency), paras 33, 34, 42 (data minimization).
179 Midas Nouwens and others, "Dark Patterns after the GDPR: Scraping Consent Pop-Ups and Demonstrating Their Influence," *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Association for Computing Machinery Inc 2020) 1–2.
180 Ibid 5–6. It tested explicit consent, symmetry between accepting and rejecting, and no preselected boxes.
181 Justin Hurwitz, "Designing a Pattern, Darkly" (2020) 22 *North Carolina Journal of Law & Technology* 57, 95–100.
182 See Chapter 4A.
183 Gregory Day and Abbey Stemler, "Are Dark Patterns Anticompetitive?" (2020) 72 *Alabama Law Review* 1, 29. See also Lina M Khan and David E Pozen, "A Skeptical View of Information Fiduciaries" (2019) 133 *Harvard Law Review* 497, 528, 540–541.
184 Luguri and Strahilevitz, "Shining a Light on Dark Patterns" (n 122) 94.
185 See Chapter 4B.
186 Ari Ezra Waldman, "Cognitive Biases, Dark Patterns, and the 'Privacy Paradox'" (2020) 31 *Current Opinion in Psychology* 105, 108; Jack Balkin, "Information Fiduciaries and the First Amendment" (2016) 49 *U.C. Davis Law Review* 1183, 1186. See also Chapter 5C.
187 Jack M Balkin, "The Fiduciary Model of Privacy" (2020) 134 *Harvard Law Review Forum* 11, 14.
188 See Chapter 7A.
189 See Day and Stemler, "Are Dark Patterns Anticompetitive?" (n 183) 15. See also Susser, Roessler, and Nissenbaum, "Online Manipulation" (n 153) 17.
190 Luguri and Strahilevitz, "Shining a Light on Dark Patterns" (n 122) 82–102; Colin M Gray and others, "Dark Patterns and the Legal Requirements of Consent Banners: An Interaction Criticism Perspective," *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Association for Computing Machinery 2021) 3–4, 8–12.
191 See Chapter 4A–B.
192 See Chapter 5A–B.
193 See Chapter 5C.

3 THE CONSENT ILLUSION

1 Cade Metz, "Facial Recognition Tech Is Growing Stronger, Thanks to Your Face" *New York Times* (13 July 2019) <https://perma.cc/3ETY-4BWM>.
2 *Stein v Clarifai, Inc* (2021) 526 F Supp 3d 339 (Dist Court) [44].

3 GDPR Article 4(11). See also *Judgment of 1 October 2019 in Case C-673/17 Planet49 GmbH* ECLI:EU:C:2019:801.
4 Jeremy Wiener, "Deceptive Design and Ongoing Consent in Privacy Law" (2021) 53 *Ottawa Law Review* 133, 152.
5 Shantal R Marshall and Laura P Naumann, "What's Your Favorite Music? Music Preferences Cue Racial Identity" (2018) 76 *Journal of Research in Personality* 74, 88.
6 Daniel DellaPosta, Yongren Shi, and Michael Macy, "Why Do Liberals Drink Lattes?" (2015) 120 *American Journal of Sociology* 1473, 1474–1475.
7 Yannick Leo and others, "Socioeconomic Correlations and Stratification in Social-Communication Networks" (2016) 13 *Journal of The Royal Society Interface* 1, 2.
8 Przemyslaw Palka, "Data Management Law for the 2020s: The Lost Origins and the New Needs" (2020) 68 *Buffalo Law Review* 559, 564–566.
9 "Acxiom Global Data Navigator" (*Acxiom LLC*, 2022) 2 <https://perma.cc/88DJ-5HMX>; "Acxiom InfoBase" (*Acxiom LLC*, 2020) 1 <https://perma.cc/LF8L-R8D7>.
10 Solon Barocas and Helen Nissenbaum, "Computing Ethics Big Data's End Run Around Procedural Privacy Protections" (2014) 57 *Communications of the ACM* 31, 32.
11 Sandra Wachter and Brent Mittelstadt, "A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI" (2019) *Columbia Business Law Review* 494, 505–506.
12 *Meyers v Nicolet Restaurant of De Pere, LLC* (2016) 843 F 3d 724 (Court of Appeals, 7th Circuit) [725].
13 *Kirchein v Pet Supermarket, Inc* (2018) 297 F Supp 3d 1354 (Dist Court) [1356].
14 Daniel J Solove and Danielle Keats Citron, "Risk and Anxiety: A Theory of Data-Breach Harms" (2018) 96 *Texas Law Review* 737, 757.
15 Katherine Strandburg, "Free Fall: The Online Market's Consumer Preference Disconnect" (2013) 430 *University of Chicago Legal Forum* 95, 98.
16 Alicia Solow-Niederman, "Information Privacy and the Inference Economy" (2022) 117 *Northwestern University Law Review* 357, 414; Thomas D Haley, "Data Protection in Disarray" (2020) 95 *Washington Law Review* 1193, 1213–1216.
17 Joost Poort and Frederik Borgesius, "Does Everyone Have a Price? Understanding People's Attitude towards Online and Offline Price Discrimination" (2019) 8 *Internet Policy Review* 1, 2–5; Frederik Zuiderveen Borgesius and Joost Poort, "Online Price Discrimination and EU Data Privacy Law" (2017) 40 *Journal of Consumer Policy* 347, 348–353.
18 Ariana Tobin, "Facebook Promises to Bar Advertisers from Targeting Ads by Race or Ethnicity Again" (*ProPublica*, 25 July 2018) <https://perma.cc/MC3F-A2GK>; Ariana Tobin and Jeremy B. Merrill, "Besieged Facebook Says New Ad Limits Aren't Response to Lawsuits" (*ProPublica*, 23 August 2018) <https://perma.cc/VU2Z-Z3K7>. See also Introduction.
19 Solow-Niederman, "Information Privacy and the Inference Economy" (n 16) 414.
20 Ignacio Cofone and Adriana Robertson, "Consumer Privacy in a Behavioral World" (2018) 69 *Hastings Law Journal* 1471, 1489–1490; Strandburg, "Free Fall" (n 15) 130–152.
21 Strandburg, "Free Fall" (n 15) 131.
22 See Chapter 4B.
23 Cofone and Robertson, "Consumer Privacy in a Behavioral World" (n 20) 1489–1497.
24 Rob Bonta, "Opinion No. 20-303" 1, 10 <https://perma.cc/2PYU-JS7M>; Jordan M Blanke, "Protection for 'Inferences Drawn': A Comparison between the General Data Protection Regulation and the California Consumer Privacy Act" (2020) 1 *Global Privacy Law Review* 90.

25 *Peter Nowak v Data Protection Commissioner* [2017] C-43416 ECLIEUC2017994 (Europe (ECJ)) [58, 62].
26 California Civil Code s 1798.100 (a)(3), 1798.100 (c), 1798.105 (d)(2), 1798.140 (e), 1798.140 (e)(2); Jordan M Blanke, "The CCPA, 'Inferences Drawn,' and Federal Preemption" (2023) 29 *Richmond Journal of Law & Technology* 53, 67–73; Anupam Chandler, Margot Kaminski, and William McGeveran, "Catalyzing Privacy Law" (2021) 105 *Minnesota Law Review* 1733, 1752–1753. See also Act respecting the Protection of Personal Information in the Private Sector 1994 ss 4, 5, 8 (Quebec).
27 See eg, Rady Khuong, "Enquête Concernant Le Centre de Services Scolaire Du- Val- Des-Cerfs (Anciennement Commission Scolaire Du Val-Des-Cerfs) (1020040-S)" (*Commission d'accès à l'information du Québec*, 9 November 2022) paras 21–31 <https://perma.cc/FR7Q-WJW4> [Canada].
28 See eg, Abby Ohlheiser, "Facebook Is Trying to Get Its Users to Share More about Their Personal Lives" *Washington Post* (Washington, DC, 26 October 2021) <https://perma.cc/J625-PSU9>.
29 See Chapter 2A.
30 Salome Viljoen, "A Relational Theory of Data Governance" (2021) 131 *Yale Law Journal* 573, 609.
31 Neil Richards and Woodrow Hartzog, "A Relational Turn for Data Protection?" (2020) 4 *European Data Protection Law Review (EDPL)* 492, 493.
32 Article 29 Working Party, "Opinion 15/2011 On the Definition of Consent (WP187)" (*European Commission*, 13 July 2011) 8 <https://perma.cc/2CW9-L67C>.
33 Lanah Kammourieh and others, "Group Privacy in the Age of Big Data" in Linnet Taylor, Luciano Floridi, and Bart van der Sloot (eds), *Group Privacy: New Challenges of Data Technologies* (Springer International Publishing 2017) 52–55; Ugo Pagallo, "The Group, the Private, and the Individual: A New Level of Data Protection?" in Linnet Taylor, Luciano Floridi, and Bart van der Sloot (eds), *Group Privacy: New Challenges of Data Technologies* (Springer International Publishing 2017) 161–164.
34 Yaniv Erlich and others, "Identity Inference of Genomic Data Using Long-Range Familial Searches" (2018) 362 *Science* 690; Ellen Wright Clayton and others, "The Law of Genetic Privacy: Applications, Implications, and Limitations" (2019) 6 *Journal of Law and the Biosciences* 1, 35.
35 Madelyn Sanfilippo, Brett M Frischmann, and Katherine J Strandburg, "Privacy as Commons: Case Evaluation Through the Governing Knowledge Commons Framework" (2018) 8 *Journal of Information Policy* 116; Priscilla M Regan, "Privacy as a Common Good in the Digital World" (2002) 5 *Information, Communication & Society* 382; Madelyn Sanfilippo, Brett Frischmann, and Katherine Strandburg, "Privacy and Knowledge Commons" in Madelyn Sanfilippo, Brett M. Frischmann, and Katherine Strandburg (eds), *Governing Privacy in Knowledge Commons* (Cambridge University Press 2021) 5.
36 Joshua A. T. Fairfield and Christoph Engel, "Privacy as a Public Good" (2015) 65 *Duke Law Journal* 385, 421–433; Ignacio Cofone, "The Dynamic Effect of Information Privacy Law" (2017) 18 *Minnesota Journal of Law, Science and Technology* 517, 530–531.
37 Henrik Skaug Sætra, "Privacy as an Aggregate Public Good" (2020) 63 *Technology in Society* 5 <https://perma.cc/Y3N8-7UGM>.
38 Nadezhda Purtova, "Property Rights in Personal Data: Learning from the American Discourse" (2009) 25 *Computer Law & Security Review* 507, 519; Fairfield and Engel, "Privacy as a Public Good" (n 36).
39 Pamela Samuelson, "Privacy as Intellectual Property?" (2000) 52 *Stanford Law Review* 1, 1128, 1144–1145.

40 Simeon de Brouwer, "Privacy Self-Management and the Issue of Privacy Externalities: Of Thwarted Expectations, and Harmful Exploitation" (2020) 9 *Internet Policy Review* 7–8 <https://perma.cc/57BK-XHPA>; Jennifer Jiyoung Suh and others, "Distinguishing Group Privacy From Personal Privacy: The Effect of Group Inference Technologies on Privacy Perceptions and Behaviors" (2018) 2 *Proceedings of the ACM on Human-Computer Interaction* 168:1, 168:4.

41 Solow-Niederman, "Information Privacy and the Inference Economy" (n 16) 361–362; Palka, "Data Management Law for the 2020s" (n 8) 596–602.

42 Solon Barocas and Helen Nissenbaum, "Big Data's End Run around Anonymity and Consent" in Julia Lane and others (eds), *Privacy, Big Data, and the Public Good: Frameworks for Engagement* (Cambridge University Press 2014) 55–56.

43 Viljoen, "A Relational Theory of Data Governance" (n 30) 615–616.

44 Ibid.

45 Barocas and Nissenbaum, "Computing Ethics Big Data's End Run Around Procedural Privacy Protections" (n 10) 32.

46 Viljoen, "A Relational Theory of Data Governance" (n 30) 580, 604–613 ("a basic purpose of data production as a commercial enterprise is to relate people to one another based on relevant shared population features").

47 Lisa M Austin, "Enough About Me: Why Privacy Is About Power, Not Consent (or Harm)" in Austin Sarat (ed), *A World Without Privacy?: What Can/Should Law Do* (2014) 133 <https://perma.cc/EPK4-HCRJ>.

48 Lisa M Austin, "Reviewing PIPEDA: Control, Privacy and the Limits of Fair Information Practices" (2006) 44 *Canadian Business Law Journal* 21, 24–25; Lisa M Austin, "Is Consent the Foundation of Fair Information Practices Canada's Experience under Pipeda" (2006) 56 *University of Toronto Law Journal* 181, 188–194.

49 Felix T Wu, "Defining Privacy and Utility in Data Sets" (2013) 84 *University of Colorado Law Review* 1117, 1117.

50 Eg GDPR Art 6(1)(e); Regina Becker and others, "COVID-19 Research: Navigating the European General Data Protection Regulation" (2020) 22 *Journal of Medical Internet Research* e19799, 6.

51 Austin, "Reviewing PIPEDA: Control, Privacy and the Limits of Fair Information Practices" (n 48) 24–25; Austin, "Is Consent the Foundation of Fair Information Practices Canada's Experience under Pipeda" (n 48) 188–194; Viljoen, "A Relational Theory of Data Governance" (n 30) 608.

52 Paul Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization" (2010) 57 *UCLA Law Review* 1701, 1716–1730.

53 Sara Morrison, "This Outed Priest's Story Is a Warning for Everyone about the Need for Data Privacy Laws" (*Vox*, 21 July 2021) <https://perma.cc/3PTM-QZ5S>; "Pillar Investigates: USCCB Gen Sec Burrill Resigns after Sexual Misconduct Allegations" (*The Pillar*, 20 July 2021) <https://perma.cc/Z27N-TDQB>.

54 Gilad L Rosner, "De-Identification as Public Policy" (2020) 3 *Journal of Data Protection & Privacy* 250. See eg, Art 2 and 4(1) GDPR.

55 Woodrow Hartzog and Ira Rubinstein, "The Anonymization Debate Should Be about Risk, Not Perfection" (2017) 60 *Communications of the ACM* 22, 22; Ira S Rubinstein and Woodrow Hartzog, "Anonymization and Risk" (2016) 91 *Washington Law Review* 703, 710–711; Lisa M Austin and Andrea Slane, "Digitally Rethinking Hunter v Southam" (2022) 60 *Osgoode Hall Law Journal* 1, 11–12.

56 Arvind Narayanan and Vitaly Shmatikov, "Myths and Fallacies of 'Personally Identifiable Information'" (2010) 53 *Communications of the ACM* 24, 25–26; Melissa Gymrek and

others, "Identifying Personal Genomes by Surname Inference" (2013) 339 *Science* 321, 324.

57 Larry Hardesty, "How Hard Is It to 'de-Anonymize' Cellphone Data?" (*Massachusetts Institute of Technology News*, 27 March 2013) <https://perma.cc/XZ99-NWZ2>.

58 Ohm, "Broken Promises of Privacy" (n 52) 1746–1748.

59 Linnet Taylor, Bart van der Sloot, and Luciano Floridi, "Conclusion: What Do We Know About Group Privacy?" in Linnet Taylor, Luciano Floridi, and Bart van der Sloot (eds), *Group Privacy: New Challenges of Data Technologies* (Springer International Publishing 2017) 231–232.

60 Brent Mittelstadt, "From Individual to Group Privacy in Big Data Analytics" (2017) 30 *Philosophy & Technology* 475, 477–481, 485.

61 See Chapter 1B.

62 Palka, "Data Management Law for the 2020s" (n 8) 625–633.

63 Wu, "Defining Privacy and Utility in Data Sets" (n 49) 1162.

64 Omer Tene and Jules Polonetsky, "Big Data for All: Privacy and User Control in the Age of Analytics" (2012) 11 *Northwestern Journal of Technology and Intellectual Property* 239, 261.

65 Scott R Peppet, "Regulating the Internet of Things: First Steps toward Managing Discrimination, Privacy, Security and Consent" (2015) 93 *Texas Law Review* 85, 159.

66 Evan Selinger and Woodrow Hartzog, "The Inconsentability of Facial Surveillance" (2019) 66 *Loyola Law Review* 101, 108–116.

67 See Chapter 2B.

68 Tony Vila, Rachel Greenstadt, and David Molnar, "Why We Can't Be Bothered to Read Privacy Policies Models of Privacy Economics as a Lemons Market" (2003) Proceedings of the 5th international conference on Electronic commerce <https://perma.cc/73FB-HN94>.

69 Christine S. Wilson, "A Defining Moment for Privacy: The Time Is Ripe for Federal Privacy Legislation (Remarks at the Future of Privacy Forum)" (US Federal Trade Commission 2020) 3–4 <https://perma.cc/YQ6J-M4L7>.

70 Strandburg, "Free Fall" (n 15) 95.

71 Samuelson, "Privacy as Intellectual Property?" (n 39) 1128, 1145; Jessica Litman, "Information Privacy/Information Property" (2000) 52 *Stanford Law Review* 1283, 1284–1285.

72 Cofone and Robertson, "Consumer Privacy in a Behavioral World" (n 20) 1475, 1489–1490.

73 Maurice E Stucke and Ariel Ezrachi, *Competition Overdose: How Free Market Mythology Transformed Us from Citizen Kings to Market Servants* (Harper Business 2020).

74 "Facebook Products 'Harm Children' and 'Weaken Our Democracy,' Whistleblower Tells U.S. Senators" *CBC* (Ottawa, 5 October 2021) <https://perma.cc/B8JF-J3PD>.

75 Ryan Calo, "Digital Market Manipulation" (2014) 82 *George Washington Law Review* 995, 999, 1003–1018; Carlos Jensen and Colin Potts, "Privacy Policies as Decision-Making Tools: An Evaluation of Online Privacy Notices," *SIGCHI Conference on Human Factors in Computing Systems* (Association for Computing Machinery 2004) 475.

76 Aleecia McDonald and Lorrie Faith Cranor, "The Cost of Reading Privacy Policies" (2008) 4 *I/S: Journal of Law and Policy for the Information Society* 543, 544.

77 Ryan Calo, "Against Notice Skepticism in Privacy (and Elsewhere)" (2012) 87 *Notre Dame Law Review* 1027, 1047–1059; Paula J Dalley, "The Use and Misuse of Disclosure as a Regulatory System" (2006) 34 *Florida State University Law Review* 1089, 1092–1093; William M Sage, "Regulating through Information: Disclosure Laws and American Health Care" (1999) 99 *Columbia Law Review* 1701, 1715–1720.

78 Solon Barocas and Helen Nissenbaum, "On Notice : The Trouble with Notice and Consent" (2009) Proceedings of the engaging data forum. See also Chapter 1A.
79 Ari Ezra Waldman, "Habit and Performative Privacy" (2021) 10 *Social Epistemology Review and Reply Collective* 43, 47.
80 Cofone and Robertson, "Consumer Privacy in a Behavioral World" (n 20) 1475, 1489–1490. See also Chapter 4C.
81 See Elena Gil González and Paul de Hert, "Understanding the Legal Provisions that Allow Processing and Profiling of Personal Data – an Analysis of GDPR Provisions and Principles" (2019) 19 *ERA Forum* 597, 600.
82 Ari Ezra Waldman, *Privacy as Trust: Information Privacy for an Information Age* (Cambridge University Press 2018) 66.
83 "Remarks of Chair Lina M. Khan As Prepared for Delivery IAPP Global Privacy Summit" 6 <https://perma.cc/B4VL-BNYA>.
84 Sarah Spiekermann and others, "The Challenges of Personal Data Markets and Privacy" (2015) 25 *Electronic Markets* 161, 166–167.
85 Stacy-Ann Elvy, "Paying for Privacy and the Personal Data Economy" (2017) 117 *Columbia Law Review* 1369, 1405–1406.
86 Neil Richards, *Why Privacy Matters* (Oxford University Press 2021) 202.
87 Mark A Lemley, "The Benefit of the Bargain," *Stanford Law and Economics Olin Working Paper No. 575* (2022) 31–33, 55.
88 Ibid 1882–1883.
89 Neil Richards and Woodrow Hartzog, "Taking Trust Seriously in Privacy Law" (2016) 19 *Stanford Technology Law Review* 431, 444.
90 Daniel J Solove, "Introduction: Privacy Self-Management and the Consent Dilemma" (2012) 126 *Harvard Law Review* 1880, 1883–1888.
91 Strandburg, "Free Fall" (n 15) 131.
92 Article 7(4).
93 See Civil Liberties, Justice, and Home Affairs Committee (LIBE) version (12 March 2014) and Council-amended version (8 April 2016).
94 Neil Richards, "The Dangers of Surveillance" (2012) 126 *Harvard Law Review* 1934, 1935.
95 See also Woodrow Hartzog and Neil Richards, "Privacy's Constitutional Moment and the Limits of Data Protection" (2020) 61 *Boston College Law Review* 1687, 1736, 1745.
96 Neil Richards and Woodrow Hartzog, "Privacy's Trust Gap: A Review" (2017) 126 *Yale Law Journal* 1180, 1184.
97 Occupational Health and Safety Act, Ontario Regulation 213/91 2022.
98 Franklin P. Brannen Jr., Richard L. Sizemore, and Jacob E. Daly, "Product Liability" (2006) 58 *Mercer Law Review* 313, 347–348.
99 John F Blakney, Margot Patterson, and Andrew Lanouette, "The Canada Consumer Protection Safety Act: A Review" (2011) 51 *Canadian Business Law Journal* 211, 212.
100 Daniel Solove, *The Digital Person: Technology and Privacy in the Information Age* (New York University Press 2004) 51.
101 Neil Richards and Woodrow Hartzog, "The Pathologies of Digital Consent" (2018) 96 *Washington University Law Review* 1461, 1492–1498.
102 Ibid 1498–1502.
103 Finn Myrstad and Øyvind H. Kaldestad, "Historic Victory for Privacy as Dating App Receives Gigantic Fine" (*Forbrukerrådet*, 26 January 2021) <https://perma.cc/77RN-XJGA>.
104 "Norwegian DPA: Intention to Issue € 10 Million Fine to Grindr LLC" (*European Data Protection Board*, 26 January 2021) <https://perma.cc/DNQ4-3KKP>; "Out of Control:

Complaints and Follow Up" (*Forbrukerrådet*, 14 January 2020) <https://perma.cc/ZGX5-6L5Z>; "Administrative Fine – Grindr LLC" (*Datatilsynet*, 13 December 2021) <https://perma.cc/F9AG-T59K>.

105 Byron Tau and Georgia Wells, "Grindr User Data Was Sold Through Ad Networks" *Wall Street Journal* (2 May 2022) <https://perma.cc/JF5K-5TZZ>.

106 John Armour, Henry Hansmann, and Reinier Kraakman, "Agency Problems and Legal Strategies" in Reinier Kraakman and others (eds), *The Anatomy of Corporate Law: A Comparative and Functional Approach* (Oxford University Press 2017) 45.

107 Patrick W. Schmitz, "On the Interplay of Hidden Action and Hidden Information in Simple Bilateral Trading Problems" (2002) 103 *Journal of Economic Theory* 444, 444–447.

108 Mark Verstraete, "Inseparable Uses" (2020) 99 *North Carolina Law Review* 427, 466–467.

109 Paul Schwartz, "Property, Privacy, and Personal Data" (2004) 117 *Harvard Law Review* 2056, 2121.

110 Jean-Jacques Laffont, "Regulation, Moral Hazard and Insurance of Environmental Risks" (1995) 58 *Journal of Public Economics* 319, 322–324.

111 Jack M Balkin, "Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation" (2018) 51 *U.C. Davis Law Review* 1149, 1167–1168; Jack Balkin, "2016 Sidley Austin Distinguished Lecture on Big Data Law and Policy: The Three Laws of Robotics in the Age of Big Data" (2017) 78 *Ohio State Law Journal* 1217, 1234–1235.

112 Sugato Bhattacharyya and Francine Lafontaine, "Double-Sided Moral Hazard and the Nature of Share Contracts" (1995) 26 *The RAND Journal of Economics* 761, 766–775; Eva I Hoppe and Patrick W Schmitz, "Hidden Action and Outcome Contractibility: An Experimental Test of Moral Hazard Theory" (2018) 109 *Games and Economic Behavior* 544, 550–557.

113 Neil Richards and Woodrow Hartzog, "Trusting Big Data Research" (2017) 66 *DePaul Law Review* 579, 584.

114 See eg, Leonid Bershidsky, "End-to-End Encryption Isn't as Safe as You Think" (*Bloomberg*, 14 May 2019) <https://perma.cc/K5WM-GDTL>; Bruce Schneier, "Why 'Anonymous' Data Sometimes Isn't" (*Wired*, 12 December 2007) <https://perma.cc/9PHU-L2DD>.

115 See Chapter 1B.

116 Florencia Marotta-Wurgler, "Self-Regulation and Competition in Privacy Policies" (2016) 45 *Journal of Legal Studies* S13, 16–19.

117 Paulius Jurcys, "Privacy Icons and Legal Design" (*Towards Data Science*, 11 November 2021) <https://perma.cc/A8G7-75L4>; Kate O'Flaherty, "Apple Slams Facebook And Google With Bold New Privacy Ad" *Forbes* (25 May 2022) <https://perma.cc/5F7B-MK5X>.

118 Mark Verstraete and Tal Zarsky, "Optimizing Breach Notification" (2021) 2021 *University of Illinois Law Review* 803, 844–845.

119 "New Privacy and Cookie Policy" (*Grindr*, 2023) <https://perma.cc/J4AE-W7J7>.

120 See Chapter 7B.

121 Zack Friedman, "Stop Falling For This Facebook Scam" (*Forbes*, 19 August 2019) <https://perma.cc/93KD-T5GP>.

122 Staci Zaretsky, "Stop Posting This Facebook Privacy Notice – Your Pseudo-Legalese Means NOTHING!" (*Above the Law*, 31 January 2019) <https://perma.cc/JVL9-VMDT>.

123 Natasha Singer, "Sharing Data, but Not Happily" *New York Times* (New York, 4 June 2015) <https://perma.cc/9KXW-GY8B>.

124 Lee Rainie and Maeve Duggan, "Privacy and Information Sharing" (*Pew Research Center*, 14 January 2016) 23–25 <https://perma.cc/MXN5-PV23>.

125 Andrea Slane and Ganaele Langlois, "Debunking the Myth of 'Not My Bad': Sexual Images, Consent, and Online Host Responsibilities in Canada" (2018) 30 *Canadian Journal of Women and the Law* 42, 65–66.
126 Clare McGlynn and Erika Rackley, "Image-Based Sexual Abuse" (2017) 37 *Oxford Journal of Legal Studies* 534, 555–557.
127 Samuel Axon, "96% of US Users Opt out of App Tracking in IOS 14.5, Analytics Find" (*Ars Technica*, 5 July 2021) <https://perma.cc/6R8Y-RJ2R>.
128 Weicheng Cao and others, "A Large Scale Study of User Behavior, Expectations and Engagement with Android Permissions" (2021) 808, 815 <https://perma.cc/HVF5-WMXD>.
129 See eg, Florent Thouvenin and others, "Governance Mechanisms for Access and Use of Data in Public Health Crises: Call for Action" (*Digital Law Center*) 3–4 <https://perma.cc/7NDF-R2TD>.
130 See eg, Ignacio Cofone, "Immunity Passports and Contact Tracing Surveillance" (2020) 24 *Stanford Technology Law Review* 176, 193–204.
131 See eg, Ignacio Cofone, "Ethical Surveillance in Vaccine Passports" (2021) 45 *Fordham International Law Journal* 621, 623–627, 635–638.
132 Helen Nissenbaum, *Privacy in Context: Technology, Policy and the Integrity of Social Life* (Stanford University Press 2010) 140.
133 Ibid 133–140.
134 Helen Nissenbaum, "Privacy as Contextual Integrity" (2004) 79 *Washington Law Review* 119, 131–138.
135 See eg, "Law 29/2021, of 28 October Qualified as Protection of Personal Data" (*Andorra (Catalan)*, 28 October 2021) art 7 <https://perma.cc/BYW8-9H83>; "Personal Data Protection Act" (*Argentina*, 30 October 2000) ss 5, 11 <https://perma.cc/L8MA-399Y>; "Brazilian Data Protection Law (LGPD) (As Amended by Law No. 13,853/2019)" (*Brazil's National Congress*, 2019) arts 8, 18 <https://perma.cc/A3MV-SFYC>; "Act on the Protection of Personal Data (Data Protection Act)" (*Faroe Islands Prime Minister's Office*, 7 June 2020) art 9 <https://perma.cc/2XFK-E9SL>; "The Data Protection Law" (*Bailiwick of Guernsey*, 2017) art 10 <https://perma.cc/9HVT-2PWS>; "Personal Data Protection Act 2012" (*Singapore Statutes Online*, 2020) <https://perma.cc/FQ3N-N37F> Part 4 Division I; "Personal Information Protection Act (General Law)" (*Personal Data Protection Laws in Korea*, 5 August 2020) art 15 <https://perma.cc/H2JP-LXCK> (official translation); "Act on the Protection of Personal Information (Act No. 57)" (*Government of Japan*, 2003) art 16 <https://perma.cc/Y6A2-PVPS> (unofficial translation); "Law No. 18.331 on the Protection of Personal Data and Habeas Data Action" (*Uruguay*, 2008) art 9 <https://perma.cc/N43G-2QPH>; "Protection of Privacy Law, 5741" (*Israel*, 1981) art 1 <https://perma.cc/L65U-3DZ2>; "Ley Federal de Protección de Datos Personales En Posesión de Los Particulares" (*Mexico*, 5 July 2010) art 8 <https://perma.cc/6U94-BF3B>.
136 Nissenbaum, *Privacy in Context* (n 132) 141–145.
137 Ibid 67–126; Nissenbaum, "Privacy as Contextual Integrity" (n 134) 131–137.
138 Scott Hershovitz, "The Search for a Grand Unified Theory of Tort Law" (2017) 130 *Harvard Law Review* 942, 958.
139 Verstraete, "Inseparable Uses" (n 108) 466–467, 471–472. See also Maria Lillà Montagnani and Mark Verstraete, "What Makes Data Personal?" (2023) 56 *U.C. Davis Law Review*.
140 Verstraete, "Inseparable Uses" (n 108) 466–467, 471–472.
141 See Chapter 6B.

4 MANIPULATION BY DESIGN

1 Deceptive Design [@darkpatterns], "Just Fab Tweet" (*Twitter*, 21 February 2021) <https://perma.cc/9ZYE-KHEZ>; constanta rosca [@constanta_rosca], "Fabletics Tweet" (*Twitter*, 18 February 2021) <https://perma.cc/V4S4-P3NF>.
2 "Subscription Traps: 'No-Strings Attached' Trial Offers Could Leave You with Your Hands Tied" (*Competition Bureau Canada*, 11 March 2020) <https://perma.cc/QQ74-D2VB>.
3 Louise Matsakis, "The Subtle Tricks Shopping Sites Use to Make You Spend More" (*Wired*, 6 August 2020) <https://perma.cc/7RWV-Q5RR>.
4 Ari Ezra Waldman, "Privacy, Notice, and Design" (2018) 21 *Stanford Technology Law Review* 129, 132–133.
5 Ari Ezra Waldman, "A Statistical Analysis of Privacy Policy Design Essay" (2017) 93 *Notre Dame Law Review Online* 159, 163–171.
6 Carissa Véliz, *Privacy Is Power: Why and How You Should Take Back Control of Your Data* (Bantam Press 2021) 53–71.
7 "The Electronic Privacy Information Center (EPIC) Complaint In the Matter of Amazon.Com, Inc." (*Office of the Attorney General of the District of Columbia*, 23 February 2021) 5–8 <https://perma.cc/9TQU-Y53Q>; "You Can Log Out, but You Can Never Leave" (*Forbrukerrådet*, 14 January 2021) 14–27 <https://perma.cc/LNM4-VTSQ>.
8 Paras Chopra [@paraschopra], "Duolingo Tweet" (*Twitter*, 16 August 2022) <https://perma.cc/W2V4-5CU8>.
9 Solon Barocas and Helen Nissenbaum, "On Notice : The Trouble with Notice and Consent" (2009) *Proceedings of the Engaging Data Forum* 5.
10 Data Protection Directive 1995 (46/EC) art 6(a) and (b) & 2(h). See also Working Party on the Protection of Individuals with regards to the Processing of Personal Data, "Opinion 03/2013 on Purpose Limitation" (Brussels, 2 October 2013) 1 11, 14; Article 29 Working Party, "Opinion 15/2011 On the Definition of Consent (WP187)" (*European Commission*, 13 July 2011) 2 <https://perma.cc/2CW9-L67C>; A29WP, "Opinion 2/2013 on Providing Guidance on Obtaining Consent for Cookies" (2013) 3.
11 Weihong Peng and Jennifer Cisna, "HTTP Cookies. A Promising Technology" (2000) 24 *Online Information Review* 150, 150; Windows Development Center, "HTTP Cookies" <https://perma.cc/HE4G-HSSS>.
12 Art 14(a) and 14(b), *Data Protection Directive*.
13 Joasia Luzak, "Much Ado about Cookies: The European Debate on the New Provisions of the EPrivacy Directive Regarding Cookies" (2013) 21 *European Review of Private Law* 221, 227–228; Sylvia Mercado Kierkegaard, "How the Cookies (Almost) Crumbled: Privacy & Lobbyism" (2005) 21 *Computer Law & Security Review* 310, 316.
14 Council Directive (EC) 2002/58 of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L 201/37.
15 Working Party on the Protection of Individuals with regards to the Processing of Personal Data, "Opinion 2/2010 on Online Behavioral Advertising" (Brussels, 22 June 2010) 8, 16; Article 29 Working Party (n. 10) 9, 13, 30.
16 Working Party on the Protection of Individuals with regards to the Processing of Personal Data (n 15); Article 29 Working Party (n 10) 9,13, 30.
17 GDPR Article 7, Recital 32; *Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV v Planet49 GmbH* [2019] Judgment of the Court (Grand Chamber) ECLI:EU:C:2019:801, ECLI:EU:C:2019:801 [62–3].

18 Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V. v Planet49 GmbH. (n 17) paras 54–56; Case T-343/13, CN v Parliament [2015] ECLI:EU:T:2015:926 [61]; Michael Veale and Frederik Zuiderveen Borgesius, "Adtech and Real-Time Bidding under European Data Protection Law" (2022) 23 *German Law Journal* 226, 236. See also European Data Protection Board, "Guidelines 05/2020 on Consent under Regulation 2016/679" (2020) 19, 22–23 para 82 <https://perma.cc/8Q8Y-XUTU>; Iris van Ooijen and Helena U. Vrabec, "Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective" (2019) 42 *Journal of Consumer Policy* 91, 100; Eoin Carolan, "The Continuing Problems with Online Consent under the EU's Emerging Data Protection Principles" (2016) 32 *Computer Law & Security Review* 462, 467.
19 OPTA, "Veelgestelde Vragen over de Cookieregels" (2013).
20 K. J. Dearie, "GDPR Cookie Notice Banner Examples" (*Termly*, 8 November 2021) <https://perma.cc/LBC9-M38J>.
21 Natali Helberger, "Freedom of Expression and the Dutch Cookie-Wall" (2013) 2.
22 Matt Steinglass, "Dutch Cookie Law May Lead to Online Exodus" *Financial Times* (21 June 2011) <https://perma.cc/JA9B-V7E2>.
23 Jan Driessen and others, "Verzoek Tot Inhoudelijke Behandeling Wijziging van de Telcommunicatiewet" (3 July 2011).
24 GJ Zwenne and L Mommers, *Wetgever Maakt Surfen Onmogelijk* (Het Financiële Dagblad, 11 June 2010) <https://perma.cc/N5M8-2QLP>.
25 Freek Vos, "Waar Maakt Iedereen Zich Zo Druk over? Leve de Cookies!" *Volkskrant* (17 October 2012).
26 Stephan Loerke, "The Dutch Find a Lighter Touch on Internet Privacy Laws" (*AdAge*, 3 July 2013) <https://perma.cc/62UW-558M>.
27 Helberger, "Freedom of Expression and the Dutch Cookie-Wall" (n 21) 1.
28 Eg, Bart van der Sloot, "Je Geld of Je Gegevens: De Keuze Tussen Privacybescherming En Gratis Internetdiensten" (2011) 86 *Nederlands Juristenblad* 1493.
29 Arnoud Engelfriet, "Websites Negeren Massaal de Cookiewet" (*Ichrecht*, 13 July 2012) <https://perma.cc/PP5K-AZPP>.
30 Vincent Oord and Marjolein Kampschreur, "Dutch Political Parties Violate Their Own Cookie Law" (*Fleishman-Hillard*, 7 June 2012) <https://perma.cc/SAZ4-ZVF3>. See also "Opta Overtreedt Eigen Cookie-Regels" (October 2012) <https://perma.cc/E2MP-HNRB>.
31 "Kamer Wil Einde Pop-Ups Door Cookiewet" (*NU* 13 February 2013); "Meerderheid Tweede Kamer Wil Einde Aan Cookie-Popups" (*Tweakers*, 13 February 2013); "Kamp (EZ) Gaat Cookievoorstel D66 Bestuderen" (*Emerce*, 22 November 2012).
32 *Data Protection Directive article 2(h)*.
33 ICO, "Guidance on the Rules on Use of Cookies and Similar Technologies" (*Information Commissioner's Office*, May 2012) 6 <https://perma.cc/J9ER-4Q8Y>.
34 Ibid.
35 Department for Culture Media and Sport, "Open Letter on the UK Implementation of Article 5(3) of the e-Privacy Directive on Cookies" (2011) 2–3.
36 Ignacio Cofone, "The Way the Cookie Crumbles: Online Tracking Meets Behavioral Economics" (2016) 25 *International Journal of Law and Information Technology* 38, 45.
37 "Cookiewet Versoepeld: Verplichte Melding Voor Minder Cookies" *deVolkskrant* (20 December 2012) <https://perma.cc/JG8T-UV7S>.
38 European Data Protection Board, "Guidelines 05/2020 on Consent under Regulation 2016/679" (n 18).

39 "Cookies: The CNIL Fines GOOGLE a Total of 150 Million Euros and FACEBOOK 60 Million Euros for Non-Compliance with French Legislation" (*CNIL*, 6 January 2022) <https://perma.cc/EX8R-H5VP>; Sammit Adhya, "New Cookie Choices in Europe" (*Google: The Keyword*, 21 April 2022) <https://perma.cc/6P2U-F47N>.
40 Kirsten Martin, "Manipulation, Privacy, and Choice" (2022) 23 *North Carolina Journal of Law & Technology* 452, 458–459.
41 Philip Hausner and Michael Gertz, "Dark Patterns in the Interaction with Cookie Banners," *CHI Conference on Human Factors in Computing Systems* (2021) 1–2 <https://perma.cc/CD6Q-956Z>.
42 Joachim Vogt and others, "Website Operators Are Not the Enemy Either – Analyzing Options for Creating Cookie Consent Notices without Dark Patterns," *Mensch und Computer 2022 – Workshopband* (Gesellschaft für Informatik eV 2022) <https://perma.cc/E7N6-R6QP>.
43 Jan M Bauer, Regitze Bergstrøm, and Rune Foss-Madsen, "Are You Sure, You Want a Cookie? – The Effects of Choice Architecture on Users' Decisions about Sharing Private Online Data" (2021) 120 *Computers in Human Behavior* 106729, 5.
44 CCPA, s 1798.120(a)
45 "FCC Adopts Broadband Consumer Privacy Rules" (*Federal Communications Commission*, 27 October 2016) <https://perma.cc/RB4P-25XU>. FCC, Protecting the Privacy of Customers of Broadband and Other Telecommunications Services – Notice of Proposed Rulemaking 2016 [31 FCC Rcd 2500, 2501] para 2.
46 ISPs would have been required to obtain explicit opt-in consent for sensitive information, defined broadly, and opt-out consent for non-sensitive information. The Order established wide categories for sensitive information, such as location data, financial information, health information, children's information, social security numbers, web browsing history, app usage history, and content of communications. Nonsensitive information was defined as all personally identifiable information that didn't fall under sensitive information. See FCC, Protecting the Privacy of Customers of Broadband and Other Telecommunications Services – Notice of Proposed Rulemaking (n 45).
47 Public Law No: 115-22 2017. See also Steve Lohr, "Trump Completes Repeal of Online Privacy Protections From Obama Era" *New York Times* (New York, 3 April 2017) <https://perma.cc/G3LJ-MC6G>; 5 U.S.C. 802.
48 Paul Ohm, "The Rise and Fall of Invasive ISP Surveillance" (2009) *University of Illinois Law Review* 1417, 1420–1423.
49 See Chapter 3B.
50 See Chapter 3C.
51 Craig McKenzie, Michael Liersch, and Stacey Finkelstein, "Recommendations Implicit in Policy Defaults" (2006) 17 *Psychological Science* 414, 414. See also Gabriel Carroll and others, "Optimal Defaults and Active Decisions" (2009) 124 *Quarterly Journal of Economics* 1639.
52 Cass Sunstein and Richard Thaler, "Libertarian Paternalism Is Not an Oxymoron" (2003) 70 *The University of Chicago Law Review* 1159, 1181; Chapter 2C.
53 Cofone, "The Way the Cookie Crumbles" (n 36) 48.
54 Ian Ayres and Robert Gertner, "Filling Gaps in Incomplete Contracts: An Economic Theory of Default Rules" (1989) 99 *Yale Law Journal* 87, 107.
55 Ibid 128.
56 Ibid 128. See also Ian Ayres and Robert Gertner, "Strategic Contractual Inefficiency and the Optimal Choice of Legal Rules" (1992) 101 *Yale Law Journal* 729, 733–734.
57 Ayres and Gertner, "Filling Gaps in Incomplete Contracts: An Economic Theory of Default Rules" (n 54) 91; Jason Johnston, "Strategic Bargaining and the Economic Theory of Contract Default Rules" (1990) 100 *Yale Law Journal* 615, 635.

58 Ayres and Gertner, "Filling Gaps in Incomplete Contracts: An Economic Theory of Default Rules" (n 54) 106.
59 Jay Kesan and Rajiv Shah, "Setting Software Defaults: Perspectives from Law, Computer Science and Behavioral Economics" (2006) 82 *Notre Dame Law Review* 583, 621.
60 Ibid.
61 See Chapter 2.
62 "Protecting Your Privacy Online" (*The Privacy Sandbox*) <https://perma.cc/2CU2-PLLQ>.
63 "Topics: The New Privacy Sandbox Proposal for Interest-Based Advertising" (*Google Ads Help*, 22 February 2022) <https://perma.cc/VEU9-TMAD>.
64 Andrea Polonioli, "Zero Party Data between Hype and Hope" (2022) 5 *Frontiers in Big Data* <https://perma.cc/2HW2-PH93>.
65 Michal Kosinski, David Stillwell, and Thore Graepel, "Private Traits and Attributes Are Predictable from Digital Records of Human Behavior" (2013) 110 *Proceedings of the National Academy of Sciences* 5802, 5803.
66 Carter Jernigan and Behram FT Mistree, "Gaydar: Facebook Friendships Expose Sexual Orientation" (2009) 14 *First Monday*.
67 Jian Hu and others, "Demographic Prediction Based on User's Browsing Behavior" (2007) *Proceedings of the 16th International Conference on World Wide Web* 151, 151–152; Koen W De Bock and Dirk Van den Poel, "Predicting Website Audience Demographics for Web Advertising Targeting Using Multi-Website Clickstream Data" (2010) 98 *Fundamenta Informaticae* 49, 50–51; Sharad Goel, Jake Hofman, and M Sirer, "Who Does What on the Web: A Large-Scale Study of Browsing Behavior" (2012) 6 *Proceedings of the International AAAI Conference on Web and Social Media* 130, 135–136; Michal Kosinski and others, "Personality and Website Choice" (2012) *ACM Web Science Conference* 251.
68 See Chapter 2A.
69 Daniel Kahneman and Amos Tversky, "Subjective Probability: A Judgment of Representativeness" (1972) 3 *Cognitive Psychology* 430, 444.
70 Ignacio Cofone and Adriana Robertson, "Consumer Privacy in a Behavioral World" (2018) 69 *Hastings Law Journal* 1471, 1489.
71 Ibid 1505–1506.
72 Scott R Peppet, "Regulating the Internet of Things: First Steps toward Managing Discrimination, Privacy, Security and Consent" (2015) 93 *Texas Law Review* 85, 119; Jacob Kröger, "Unexpected Inferences from Sensor Data: A Hidden Privacy Threat in the Internet of Things" (2019) *Internet of Things. Information Processing in an Increasingly Connected World* 147.
73 Andrew Raij and others, "Privacy Risks Emerging from the Adoption of Innocuous Wearable Sensors in the Mobile Environment," *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Association for Computing Machinery 2011).
74 Peppet, "Regulating the Internet of Things" (n 72) 93, 115–16, 120.
75 Rob Nicholls, "Informed Consent to Online Standard Form Agreements" (2022) 3 *Global Privacy Law Review* 163, 171–173.
76 Because Brooklyn's data is more useful when aggregated with other user information, her data is also informative about others, as discussed in Chapter 3. Even if information overload didn't exist, Brooklyn might agree to too much collection in exchange for "free" or low-cost services because part of that risk is borne by others.
77 Cofone and Robertson, "Consumer Privacy in a Behavioral World" (n 70) 1496.
78 See Bill C-27, 44th Parliament, 1st session, 2022 (Canada); Personal Information Protection Act, Act No. 14839 of 2017, art 22(2) (South Korea); Personal Data Protection Act 2010, Act 709 of 2010, s 7(3) (Malaysia).

79 GDPR Recital 58. See also GDPR Art 12 ("concise, transparent, intelligible and easily accessible form, using clear and plain language").
80 Cofone and Robertson, "Consumer Privacy in a Behavioral World" (n 70) 1497.
81 Alessandro Acquisti and Ralph Gross, "Predicting Social Security Numbers from Public Data" (2009) 106 *Proceedings of the National Academy of Sciences* 10975, 10980; Paul Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization" (2010) 57 *UCLA Law Review* 1701, 1716–1722; A Narayanan and V Shmatikov, "De-Anonymizing Social Networks," *30th IEEE Symposium on Security and Privacy* (2009); A Narayanan and V Shmatikov, "Robust De-Anonymization of Large Sparse Datasets," *IEEE Symposium on Security and Privacy (SP 2008)* (2008) 111–125.
82 Katherine Strandburg, "Free Fall: The Online Market's Consumer Preference Disconnect" (2013) 430 *University of Chicago Legal Forum* 95, 131.
83 See Chapter 3A.
84 Solon Barocas and Helen Nissenbaum, "Big Data's End Run around Anonymity and Consent" in Julia Lane and others (eds), *Privacy, Big Data, and the Public Good: Frameworks for Engagement* (Cambridge University Press 2014) 46.
85 Omri Ben-Shahar and Carl E Schneider, *More Than You Wanted to Know: The Failure of Mandated Disclosure* (Princeton University Press 2016) 191–194.
86 Lauren Willis, "When Nudges Fail: Slippery Defaults" (2013) 80 *University of Chicago Law Review* 1155, 1160; Lauren Willis, "Why Not Privacy By Default?" (2014) 29 *Berkeley Technology Law Journal* 61, 99.
87 Oren Bar-Gill and Omri Ben-Shahar, "Optimal Defaults in Consumer Markets" (2016) 45 *The Journal of Legal Studies* S137, 136–139.
88 Omri Ben-Shahar and Lior Jacob Strahilevitz, "Contracting over Privacy: Introduction" (2016) 45 *The Journal of Legal Studies* S1, 8–9.
89 Willis, "When Nudges Fail: Slippery Defaults" (n 86) 1186–1187.
90 See Willis, "Why Not Privacy By Default?" (n 86) 94.
91 Luzak, "Much Ado about Cookies" (n 13) 239.
92 Willis, "When Nudges Fail: Slippery Defaults" (n 86) 1212–1213.
93 See Chapter 2C.
94 Colin M Gray and others, "Dark Patterns and the Legal Requirements of Consent Banners: An Interaction Criticism Perspective," *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Association for Computing Machinery 2021) 6–8.
95 Ibid 8; Christine Utz and others, "(Un)Informed Consent: Studying GDPR Consent Notices in the Field" (2019) CCS '19: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security 973. See also Bauer, Bergstrøm, and Foss-Madsen, "Are You Sure, You Want a Cookie?" (n 43).
96 Johanna Gunawan and others, "Toward an Understanding of Dark Pattern Privacy Harms" [2021] CHI'21, Online Virtual Conference 4 <https://perma.cc/VR75-BAT5>.
97 Yafit Lev-Aretz and Katherine J Strandburg, "Privacy Regulation and Innovation Policy" (2020) 22 *Yale Journal of Law and Technology* 256, 291.
98 See *Douez v Facebook, Inc* (33 SCC) [6] [Canada]; *Albayate v Bank of Montreal* (BCSC 695) [138] [Canada].
99 Russell Korobkin, "Bounded Rationality, Standard Form Contracts, and Unconscionability" (2003) 70 *The University of Chicago Law Review* 1203, 1204–1207, 1256; Jason Johnston, "The Return of Bargain: An Economic Theory of How Standard-Form Contracts Enable Cooperative Negotiation between Businesses and Consumers" (2006) *Michigan Law Review* 893; Shmuel I Becher, "Behavioral Science and Consumer Standard Form Contracts" (2007) 68 *Louisiana Law Review* 155.

100 *Uber Technologies Inc v Heller* (16 SCC) [64–79, 84, 89–91]; *Douez v. Facebook, Inc.* (n 98) paras 112–116.
101 Korobkin, "Bounded Rationality, Standard Form Contracts, and Unconscionability" (n 99) 1207.
102 Alan Schwartz, "Regulating for Rationality" (2015) 67 *Stanford Law Review* 1373, 1410.
103 Ben-Shahar and Schneider, *More Than You Wanted to Know* (n 85) 172. See also Cofone and Robertson, "Consumer Privacy in a Behavioral World" (n 70) 1490.
104 Martin, "Manipulation, Privacy, and Choice" (n 40) 459.
105 Arthur L Corbin and Joseph M Perillo, *Corbin on Contracts: Avoidance and Reformation*, vol 7, revised ed (West Publishing Company 2002) 255.
106 *Hume v United States* (1889) 132 US 406 (Supreme Court) 409–411.
107 Ibid 414–415.
108 Corbin and Perillo, *Corbin on Contracts* (n 105) 258.
109 *Frank v Gaos* (2019) 139 Ct 1041 (Supreme Court) [1044]. See also Stored Communications Act, 18 U.S.C. s 2701.
110 "How to Set Up and Install the Meta Pixel" (*Meta Business Help Center*) <https://perma.cc/JG2Y-PGVX>.
111 Omri Ben-Shahar and Adam Chilton, "Simplification of Privacy Disclosures: An Experimental Test" (2016) 45 *The Journal of Legal Studies* S41, S54–S55; Lior Jacob Strahilevitz and Matthew B Kugler, "Is Privacy Policy Language Irrelevant to Consumers?" (2016) 45 *The Journal of Legal Studies* S69, S87–S92. Aleecia M McDonald and others, "A Comparative Study of Online Privacy Policies and Formats" in Ian Goldberg and Mikhail J. Atallah (eds), *Privacy Enhancing Technologies* (Springer 2009) 49–51. Hana Habib and others, "An Empirical Analysis of Data Deletion and Opt-Out Choices on 150 Websites," *USENIX Symposium on Usable Privacy and Security (SOUPS)* (USENIX Association 2019) 396 <https://perma.cc/U7QH-BFFQ>; Hana Habib and others, "'It's a Scavenger Hunt': Usability of Websites' Opt-Out and Data Deletion Choices," *CHI Conference on Human Factors in Computing Systems* (2020) 2. See also Chapters 1A and 2C.
112 Cofone and Robertson, "Consumer Privacy in a Behavioral World" (n 70) 1502–1503.
113 Ibid 1503–1504.
114 Ibid 1504–1505.
115 'Facebook Pixel Integration' (*Calendly*) <https://perma.cc/5L2J-RRLD>.
116 For example, instead of adding a statement in a privacy notice stating that "we will collect data on location, web browsing history, app usage history, and content of communications," the disclosure could read "we will collect data on location, web browsing history, app usage history, and content of communications. For example, this will allow us to learn where you are every time you open the app, and what websites you looked at before and after you use the app. It will also allow us to record the details of your app usage habits, when you communicate with others through the app, and the full text of any conversations you have using the app platform."
117 Cofone, "The Way the Cookie Crumbles" (n 36) 55–56.
118 Ibid 56.
119 Helberger, "Freedom of Expression and the Dutch Cookie-Wall" (n 21) 3–4.
120 Cofone, "The Way the Cookie Crumbles" (n 36) 56–57.
121 Council Directive (EC) 2009/136 of 25 November 2009 amending Directive (EC) 2002/22 on universal service and users' rights relating to electronic communications networks and services, Directive (EC) 2002/58 concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation

(EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws [2009] OJ L 337/11.

122 Pedro Giovanni Leon and others, "Why Johnny Can't Opt out: A Usability Evaluation of Tools to Limit Online Behavioral Advertising," *Proceedings of the Association for Computing Machinery Special Interest Group on Computer-Human Interaction Conference* (Association for Computing Machinery Press 2012) 4.

123 Ann Cavoukian, "Privacy by Design" (2009) 3 <https://perma.cc/BM3T-KD4Z>; see also Peter Hustinx, "Privacy by Design: Delivering the Promises" (2010) 3 *Identity in the Information Society* 253, 253. See also Chapter 5C.

124 EU Cookie Law Help, "What's the Difference between a Session Cookie and a Persistent Cookie?" <https://perma.cc/M7AM-6LDK>.

125 Peng and Cisna, "HTTP Cookies" (n 11) 151–152.

126 Cofone, "The Way the Cookie Crumbles" (n 36) 54.

127 Ibid 55.

128 Assel Aliyeva and Manuel Egele, "Oversharing Is Not Caring: How CNAME Cloaking Can Expose Your Session Cookies" (2021) Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security 123, 123.

129 Yunge Li, "The California Consumer Privacy Act of 2018: Toughest U.S. Data Privacy Law with Teeth? Student Articles" (2019) 32 *Loyola Consumer Law Review* 177, 190–191.

130 Richie Koch, "Cookies, the GDPR, and the EPrivacy Directive" (*GDPR.eu*, 9 May 2019) <https://perma.cc/3VCQ-SQWY>. See also GDPR Arts 12, 14, Recital 58.

131 Charles E MacLean, "It Depends: Recasting Internet Clickwrap, Browsewrap, I Agree, and Click-through Privacy Clauses as Waivers of Adhesion" (2016) 65 *Cleveland State Law Review* 45, 46; Charlotte A Tschider, "The Consent Myth: Improving Choice for Patients of the Future" (2019) 96 *Washington University Law Review* 1505, 1519.

132 Ian Ayres and Robert Gertner, "Filling Gaps in Incomplete Contracts: An Economic Theory of Default Rules" (1989) 99 *Yale Law Journal* 87, 91; Adam B Badawi, "Rationality's Reach" (2014) 112 *Michigan Law Review* 993, 1006.

133 Eric Posner, "Contract Law in the Welfare State: A Defense of the Unconscionability Doctrine, Usury Laws, and Related Limitations on the Freedom to Contract" (1995) 24 *The Journal of Legal Studies* 283; Korobkin, "Bounded Rationality, Standard Form Contracts, and Unconscionability" (n 99) 1258.

134 Nancy S Kim, *Wrap Contracts: Foundations and Ramifications* (Oxford University Press 2013) 176–192.

135 Ari Ezra Waldman, "Privacy's Law of Design" (2019) 9 *UC Irvine Law Review* 1239, 1279; Katherine Strandburg, "Monitoring, Datafication, and Consent: Legal Approaches to Privacy in the Big Data Context" in Julia Lane and others (eds), *Privacy, Big Data and the Public Good: Frameworks for Engagement* (Cambridge University Press 2014) 22–23. See also Chapter 1A.

136 Strandburg, "Free Fall" (n 82) 165.

137 Ibid 106.

138 Martin, "Manipulation, Privacy, and Choice" (n 40) 465.

139 See Chapters 5–7.

5 Traditionalist Data Protection Rules

1 "The Ford Pinto" (*The American Museum of Tort Law*, 13 June 2016) <https://perma.cc/R7SC-R5DM>.

2 *Grimshaw v Ford Motor Co* (119 Cal App 3d 757); *Gray et al, v Ford Motor Co* (Superior Court of Orange County) With compensatory damages, it added up to $127.8 million.

3 See Chapters 6 and 7.
4 Clare Duffy and others, "Facebook Whistleblower Testifies in Congress" (*CNN Business*, 5 October 2021) <https://perma.cc/5QHS-GD8W>.
5 Thomas Streinz, "The Evolution of European Data Law" in Gráinne de Búrca and Paul Craig (eds), *The Evolution of EU Law* (3rd ed., Oxford University Press 2021) 910–914. See also European Convention on Human Rights, Article 8; Article 8 of the EU Charter of Fundamental Rights; Article 16 Treaty on the Functioning of the EU; *Erich Stauder v City of Ulm – Sozialamt* [1969] ECJ Case 29-69, Case 29-69; Anupam Chandler, Margot Kaminski, and William McGeveran, "Catalyzing Privacy Law" (2021) 105 *Minnesota Law Review* 1733, 1747. Article 39 Treaty on European Union.
6 Eg, Andorra's Personal Data Protection Act, Argentina's Personal Data Protection Act, Canada's Personal Information Protection and Electronic Documents Act, Israel's Protection of Privacy Law, Japan's Act on the Protection of Personal Information, New Zealand's Privacy Act 2020.
7 W Gregory Voss and Kimberly A Houser, "Personal Data and the GDPR: Providing a Competitive Advantage for U.S. Companies" (2019) 56 *American Business Law Journal* 287, 299. See also Guy Aridor, Yeon-Koo Che, and Tobias Salz, "The Effect of Privacy Regulation on the Data Industry: Empirical Evidence from GDPR" (National Bureau of Economic Research, March 2020) <https://perma.cc/5XGM-DW5V>.
8 Przemyslaw Palka, "Data Management Law for the 2020s: The Lost Origins and the New Needs" (2020) 68 *Buffalo Law Review* 559, 614–616.
9 Chris Jay Hoofnagle, Bart van der Sloot, and Frederik Zuiderveen Borgesius, "The European Union General Data Protection Regulation: What It Is and What It Means" (2019) 28 *Information & Communications Technology Law* 65, 70.
10 Margot E Kaminski, "The Case for Data Privacy Rights (Or 'Please, a Little Optimism')" (2022) 97 *Notre Dame Law Review* 385, 386; Paul M Schwartz and Karl-Nikolaus Peifer, "Transatlantic Data Privacy Law" (2017) 106 *Georgetown Law Journal* 115, 128. See also Chapter 1A.
11 "Law 29/2021, of October 28, Qualified as Protection of Personal Data" (*Andorra (Catalan)*, 28 October 2021) art 7 <https://perma.cc/BYW8-9H83>; "Personal Data Protection Act" (*Argentina*, 30 October 2000) ss 5, 11 <https://perma.cc/L8MA-399Y>; "Brazilian Data Protection Law (LGPD) (As Amended by Law No. 13,853/2019)" (*Brazil's National Congress*, 2019) arts 8, 18 <https://perma.cc/A3MV-SFYC>; "Act on the Protection of Personal Data (Data Protection Act)" (*Faroe Islands Prime Minister's Office*, 7 June 2020) art 9 <https://perma.cc/2XFK-E9SL>; "The Data Protection Law"(*Bailiwick of Guernsey*, 2017) art 10 <https://perma.cc/9HVT-2PWS>; "Personal Data Protection Act 2012" (*Singapore Statutes Online*, 2020) <https://perma.cc/FQ3N-N37F> Part 4 Division I; "Personal Information Protection Act (General Law)" (*Personal Data Protection Laws in Korea*, 5 August 2020) art 15 <https://perma.cc/H2JP-LXCK> (official translation); "Act on the Protection of Personal Information (Act No. 57)" (*Government of Japan*, 2003) art 16 <https://perma.cc/Y6A2-PVPS> (unofficial translation); "Law No. 18.331 on the Protection of Personal Data and Habeas Data Action" (*Uruguay*, 2008) art 9 <https://perma.cc/N43G-2QPH>; "Protection of Privacy Law, 5741" (*Israel*, 1981) art 1 <https://perma.cc/L65U-3DZ2>; "Ley Federal de Protección de Datos Personales En Posesión de Los Particulares" (*Mexico*, 5 July 2010) art 8 <https://perma.cc/6U94-BF3B>.
12 With counted exceptions such as New Zealand, where the main driver is legitimate business purposes. John Edwards, "Click to Consent? Not Good Enough Anymore" (*New Zealand Office of the Privacy Commissioner*, 2 September 2019) <https://perma.cc/3RMR-E94P>; "New Zealand: Status of Consent for Processing Personal Data" (*ABLI-FPF Convergence Series*, June 2022) <https://perma.cc/68UF-DASS>.

13 Even modern versions such as the CCPA focus on opt out rights. 1798.140(h), 1798.185. 59. See also s 59.1-573(A)(5).
14 Dennis D Hirsch, "The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation" (2011) 34 *Seattle University Law Review* 439, 440; Kevin E Davis and Florencia Marotta-Wurgler, "Contracting for Personal Data" (2019) 94 *New York University Law Review* 662; Salome Viljoen, "A Relational Theory of Data Governance" (2021) 131 *Yale Law Journal* 573, 592.
15 See California Consumer Privacy Act of 2018 (CCPA), Cal. Civ. Code ss 1798.110-1798.120; California Privacy Rights Act of 2020 (CPRA) ss 2.G., 2.H; Virginia Consumer Data Protection Act, Va. Code Ann. s 59.1; Colorado Privacy Act, Colo. Rev Stat. s 6-1; Biometric Information Privacy Act (BIPA), 740 ILCS/14, Pub. Act 095-994 (2008) (respectively). See also Ari Ezra Waldman, "Privacy, Practice, and Performance" (2022) 110 *California Law Review* 1221, 1224.
16 GDPR art 6.
17 ICO, "Guidance on AI and Data Protection" (*UK Information Commissioner's Office*, 30 July 2020) <https://perma.cc/C76T-38YV>. See also "OGH 6Ob56/21k" (*Lexis* 360, 2021) <https://perma.cc/C7N9-Z8EQ>.
18 GDPR Recital 45.
19 "What Are the Substantial Public Interest Conditions?" (*ICO*, 25 April 2022) <https://perma.cc/63SZ-8CWK>.
20 "When Can We Rely on Legitimate Interests?" (*ICO*, 17 October 2022) <https://perma.cc/748A-YAB4>. See also Orla Lynskey, "General Report Topic 2: The New EU Data Protection Regime" in Jorrit J. Rijpma (ed), *The New Data Protection Regime: Setting Global Standards for the Right to Personal Data Protection*, vol 2 (Eleven International Publishing 2020) 38–39 <https://perma.cc/YS6K-WCQ9>. Robert Niedermeier and Mario Egbe Mpame, "Processing Personal Data under Article 6(f) of the GDPR: The Concept of Legitimate Interest" (2019) 3 *International Journal for the Data Protection Officer, Privacy Officer and Privacy Counsel* 18, 24.
21 Orla Lynskey (n 20) 40 ("Consent is viewed as the primary norm, or default legal basis, for personal data processing in a number of Member States"); Chris Jay Hoofnagle, "Designing for Consent" (2018) 7 *Journal of European Consumer and Market Law* 162, 162; Maximilian Hils, Daniel W Woods, and Rainer Böhme, "Measuring the Emergence of Consent Management on the Web," *Proceedings of the ACM Internet Measurement Conference* (Association for Computing Machinery 2020).
22 Streinz "The Evolution of European Data Law" (n 5) 907.
23 Article 29 Working Party, "Opinion 15/2011 On the Definition of Consent (WP187)" (*European Commission*, 13 July 2011) 3 <https://perma.cc/2CW9-L67C>; Roger Brownsword, "Consent in Data Protection Law: Privacy, Fair Processing and Confidentiality" in Serge Gutwirth and others (eds), *Reinventing Data Protection?* (Dordrecht 2009) 83–110; Lee A Bygrave and Dag Wiese Schartum, "Consent, Proportionality and Collective Power" in Serge Gutwirth and others (eds), *Reinventing Data Protection?* (Springer 2009) 157–173; Lee Bygrave, *Data Protection Law: Approaching Its Rationale, Logic, and Limits* (Kluwer Law International 2002) 63; Iris van Ooijen and Helena U Vrabec, "Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective" (2019) 42 *Journal of Consumer Policy* 91, 92.
24 Charter of Fundamental Rights of the European Union, Art 8(2).
25 Daniel J Solove, "The Myth of the Privacy Paradox" (2021) 89 *George Washington Law Review* 1, 29.
26 Ibid 29.

27 Palka, "Data Management Law for the 2020s: The Lost Origins and the New Needs" (n 8) 584–589; Marc Rotenberg, "Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)" (2001) *Stanford Technology Law Review* 1, 13–17; Woodrow Hartzog, "The Inadequate, Invaluable Fair Information Practices" (2016) 76 *Maryland Law Review* 952, 953–954, 957–961. See FIPPs listed in the GDPR; "Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (E.T.S. 108)" (*Council of Europe*, 28 January 1981) <https://perma.cc/9HJ3-NRGC>.

28 European Data Protection Board, "Guidelines 05/2020 on Consent under Regulation 2016/679" (2020) <https://perma.cc/8Q8Y-XUTU>; GDPR Recital 7, 68, 75, 85. See also Elettra Bietti, "The Discourse of Control and Consent Over Data in EU Data Protection Law and Beyond" (2020) Stanford University Aegis Paper Series; "Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation) (COM/2012/011 Final)," 2 <https://perma.cc/8BL4-5KJ6>; recital 6; "Rights of the Individual" (*European Data Protection Supervisor*) <https://perma.cc/5ZJ7-MBQG>.

29 Bygrave (n 23) 63; Orla Lynskey, "Deconstructing Data Protection: The 'added-Value' of a Right to Data Protection in the EU Legal Order" (2014) 63 *International & Comparative Law Quarterly* 27.

30 Van Ooijen and Vrabec "Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective" (n 23) 92; Orla Lynskey, *The Foundations of EU Data Protection Law* (Oxford University Press 2015) 180, 254–255, 258; Kenneth A Bamberger and Deirdre K Mulligan, *Privacy on the Ground: Driving Corporate Behavior in the United States and Europe* (MIT Press 2015) 21–22; William McGeveran, "Friending the Privacy Regulators" (2016) 58 *Arizona Law Review* 959, 966; Paul M Schwartz and Daniel J Solove, "Reconciling Personal Information in the United States and European Union" (2014) 102 *California Law Review* 877, 883. See also James Whitman, "The Two Western Cultures of Privacy: Dignity Versus Liberty" (2004) 113 *Yale Law Journal* 1151, 1159–1160.

31 Julie Cohen, "What Privacy Is For" (2013) 126 *Harvard Law Review* 1904, 1930.

32 Neil Richards and Woodrow Hartzog, "Taking Trust Seriously in Privacy Law" (2016) 19 *Stanford Technology Law Review* 431, 444.

33 "Customer Loyalty Schemes Review" (*Office of the Australian Information Commissioner*, October 2019) 10 <https://perma.cc/8WAD-MCN5>.

34 Virginia Consumer Data Protection Act 2021 [H.B. 2307]; Colorado Privacy Act 2021 [S.B. 21-190]; Virginia Consumer Data Protection Act 2021 [S.B. 1392]; Utah Consumer Privacy Act (UCPA) 2022 [S.B. 227]; S.B. 260 2021; An Act Concerning Personal Data Privacy and Online Monitoring 2022 [SB 6]. See also Anupam Chandler, Margot Kaminski, and William McGeveran (n 5) 1749–1755.

35 Ari Ezra Waldman, "The New Privacy Law" (2021) 55 *U.C. Davis Law Review Online* 19, 38.

36 Julie E Cohen, "How (Not) to Write a Privacy Law" (*Knight First Amendment Institute at Columbia University*, 23 March 2021) <https://perma.cc/2TTH-8BK5>; Jennifer Cobbe and Jatinder Singh, "Data Protection Doesn't Work: Oversight Failure in Data Processing Figurations," *Privacy Law Scholars Conference* (2022) 38, 47.

37 Neil Richards, *Why Privacy Matters* (Oxford University Press 2021) 174, 176; Cohen "How (Not) to Write a Privacy Law" (n 36); Woodrow Hartzog, "The Case against Idealising Control" (2018) 4 *European Data Protection Law Review* 423, 425. See also Chapter 3.

38 Daniel J Solove, "The Limitations of Privacy Rights" (2023) *Notre Dame Law Review* 5.
39 "European Union Data Protection Directive, Council Directive 95/46, 1995 O.J. (L 281) 31 (EC)"; GDPR arts 12–22.
40 Eg, CCPA 1798.110 and 1798.115 (right to know); GDPR arts 13–14.
41 GDPR art 15; LGPD art. 6(IV); Personal Information Protection and Electronic Documents Act, SC 2000, c 5, s 4.8–4.9 (CAN) [PIPEDA].
42 Solove (n 38) 5.
43 See Chapter 4B.
44 Julie E Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (Oxford University Press 2019) 262–263.
45 GDPR arts 13–15.
46 See Fair Credit Reporting Act, 15 U.S.C. s 1681(g)(a)(1); HIPAA 45 C.F.R. s 164.524(a)(1) 2019; "Law No. 18.331 on the Protection of Personal Data and Habeas Data Action" (n 10); "Uruguay – Data Protection Overview" (*Data Guidance*, March 2021) <https://perma.cc/LG6N-SBP8>; CCPA, 1798.100(a). See also Andrés Guadamuz, "Habeas Data vs. The European Data Protection Directive" (2001) 3 *Journal of Information, Law & Technology* <https://perma.cc/24NZ-GQ82>.
47 Kashmir Hill, "I Got Access to My Secret Consumer Score. Now You Can Get Yours, Too" *The New York Times* (New York, 4 November 2019) <https://perma.cc/NMH4-8EJR>.
48 Sandra Wachter and Brent Mittelstadt, "A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI" (2019) 2019 *Columbia Business Law Review* 494, 6; Rob Bonta, "Opinion No. 20-303" 10 <https://perma.cc/2PYU-JS7M>.
49 See also GDPR art 16; Privacy Act 1988 (as amended 1 April 2022), s 14, principle 13.
50 GDPR art 16.
51 Eg, *Case C-362/14 Maximillian Schrems v Data Protection* (ECR) [90] [EU]. See also accuracy FIPP provisions: GDPR art 5(1)(d); OECD, "Data Quality"; Convention 108 art 5(3)(d); PIPEDA s 4.6; APPI art 19; LGPD art 6(V), 18(III).
52 Solove "The Limitations of Privacy Rights" (n 38) 31.
53 GDPR art 21(2) The LGPD establishes the right to oppose the processing of personal data (arts 15 and 18).
54 Guidelines on consent under Regulation 2016/679 30 (WP259). See also GDPR art 18, GDPR art 21.
55 See Chapter 4B. The US exceptionally uses opt-in, such as in HIPAA and COPPA.
56 Solove "The Limitations of Privacy Rights" (n 38) 44–45.
57 GDPR art 17.
58 Codified under the California Consumer Privacy Act, 1.8 CIV [2018], s 1798.105. [CCPA], the Law 13.709 of 14 August 2018, art 18(iv) (Brazil) [LGPD], and the Quebec Privacy Act, RSQ 2021, c P-39.1, s 28 [Quebec Privacy Act]; Cf LGPD art 16: US, SB 1121; California Consumer Privacy Act, Cal, [2018], para 1798.105 138; 138 VCDPA, s 59.1-573(A)(3); 139 CCPA, 1798.105.
59 Jef Ausloos, *The Right to Erasure in EU Data Protection Law* (Oxford University Press 2020) 197–198. See GDPR Article 17.
60 See GDPR art 17(3). See also ibid.
61 GDPR arts 6(1)(a), 9(2)(a). See also Performance of a Contract art 6(1)(b) (involves consent for that contract). See also Whitney Nixdorf, "Planting in a Walled Garden: Data Portability Policies to Inform Consumers How Much (If Any) of the Harvest Is Their Share" (2019) 29 *Transnational Law and Contemporary Problems* 135, 150–151.
62 GDPR art 20. See CCPA – Cal. Civ. Code s 1798.100(d) (West 2020); Virginia Consumer Privacy Rights Act, ch 36, 2021 Va. Legis. Serv. 1, 4 (West) (to be codified at Va. Code

Ann. 59.1-573[A][4]); Brazil Lei Geral Da Proteção De Dados Pessoais (LGPD), Lei No. 13.709, de 14 de Agosto de 2018, Diário Oficial Da Uniao [D.O.U.] de 15.08.2018 (Braz.); Thailand Personal Data Protection Act, B.E. 2562 (2019) (Thai.); The Data Protection Act, No. 181 Kenya Gazette Supplement No. 24 ss 38(1) 2019; *LGPR* art. 18(v); *CCPA* (ss 1798.100(d), 1798.130(a)(2)); *Quebec Privacy Act*.

63 Barbara Van der Auwermeulen, "How to Attribute the Right to Data Portability in Europe: A Comparative Analysis of Legislations" (2017) 33 *Computer Law & Security Review* 57, 59.

64 Article 29 Data Protection Working Party, "Guidelines on the Right to Data Portability" (5 April 2017) 10–11 <https://perma.cc/K6PB-G5H4>.

65 See Chapter 3C.

66 Kaminski "The Case for Data Privacy Rights (Or 'Please, a Little Optimism')" (10) 398.

67 Sylvie Delacroix and Neil D Lawrence, "Bottom-up Data Trusts: Disturbing the 'One Size Fits All' Approach to Data Governance" (2019) 9 *International Data Privacy Law* 236, 240.

68 See Chapter 3C.

69 Julie E. Cohen "How (Not) to Write a Privacy Law" (n 36).

70 Katherine Strandburg, "Free Fall: The Online Market's Consumer Preference Disconnect" (2013) 430 *University of Chicago Legal Forum* 95.

71 Jennifer Raso, "Implementing Digitalization in an Administrative Justice Context" in Marc Hertogh and others (eds), *The Oxford Handbook of Administrative Justice* (Oxford University Press 2021) 536–537.

72 Ella Corren, "The Consent Burden in Consumer and Digital Markets" (2023) 36 *Harvard Journal of Law & Technology* 1, 10.

73 Guido Calabresi and A Douglas Melamed, "Property Rules, Liability Rules, and Inalienability: One View of the Cathedral" (1972) 85 *Harvard Law Review* 1089, 1119.

74 Corren "The Consent Burden in Consumer and Digital Markets" (n 72) 8.

75 Ibid 32–43.

76 Ibid.

77 See Chapter 4A.

78 See Chapter 4C.

79 Ari Ezra Waldman, "Privacy's Rights Trap" (2022) 117 *Northwestern University Law Review* 88, 95–96.

80 Solove "The Limitations of Privacy Rights" (n 38) 44–45.

81 Waldman, "Privacy, Practice, and Performance" (n 15) 1227.

82 See Elizabeth Denham, "Speech: Privacy and the Worldwide Web: How the OPC Investigation of Facebook Made Worldwide Waves" (*Office of the Privacy Commissioner of Canada*, 7 October 2009) <https://perma.cc/C4RE-HJBV>.

83 Joseph Farrell, "Can Privacy Be Just Another Good" (2012) 10 *Journal on Telecommunications and High Technology Law* 251, 251–252. See eg, Nick Ismail, "People Don't Care about Privacy (and That's Ok, Probably)" (2017) *Information Age* <https://perma.cc/R5B8-QBNE>; Cory Doctorow, "Why Is It so Hard to Convince People to Care about Privacy?" *The Guardian* (London, 2 October 2015) <https://perma.cc/54QK-5R4U>.

84 Waldman, "Privacy, Practice, and Performance" (n 15) 1227. See also Richards and Hartzog (n 32) 434; Mark MacCarthy, "New Directions in Privacy: Disclosure, Unfairness and Externalities" (2010) 6 *I/S: A Journal of Law and Policy for the Information Society* 425, 444–445.

85 Julie E Cohen, *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice* (Yale University Press 2012) 109.

86 See Chapter 3A.
87 Jennifer Cobbe and Jatinder Singh (n 36).
88 Corren "The Consent Burden in Consumer and Digital Markets" (n 72) 8.
89 Michael Lipsky, "Bureaucratic Disentitlement in Social Welfare Programs" (1984) 58 *Social Service Review* 3, 8.
90 See Chapter 3B.
91 Ari Ezra Waldman, *Privacy as Trust: Information Privacy for an Information Age* (Cambridge University Press 2018) 70.
92 See "NOYB Enforces Your Right to Privacy Everyday" (*noyb*) <https://perma.cc/L9WY-L5CC>.
93 Waldman "Privacy's Rights Trap" (n 79) 102–103.
94 Alex Boniface Makulilo, "Privacy and Data Protection in Africa: A State of the Art" (2012) 2 *International Data Privacy Law* 163, 168; Subhajit Basu, "Privacy Protection: A Tale of Two Cultures" (2012) 6 *Masaryk University Journal of Law and Technology* 1, 5.
95 "Corporate Human Rights Policy" (*Meta*, 2021) <https://perma.cc/N5KJ-ESZ6>.
96 Ibid 05 (Governance, Oversight, and Accountability).
97 Andrew Bosworth, "Building the Metaverse Responsibly" (*Meta*, 27 September 2021) <https://perma.cc/PG4M-N77G>.
98 Ari Ezra Waldman, *Industry Unbound: The Inside Story of Privacy, Data, and Corporate Power* (Cambridge University Press 2021) 93–97.
99 GDPR art 25; GDPR arts 37–39. See also "Does My Company/Organisation Need to Have a Data Protection Officer (DPO)?" (*European Commission*) <https://perma.cc/J2CY-S4WH>; GDPR art 37(1).
100 See Chapter 4A.
101 Hartzog, "The Inadequate, Invaluable Fair Information Practices" (n 27) 964.
102 Fred H Cate, "The Failure of Fair Information Practice Principles" *Consumer Protection in the Age of the Information Economy* (2006) 342.
103 Woodrow Hartzog and Neil Richards, "Privacy's Constitutional Moment and the Limits of Data Protection" (2020) 61 *Boston College Law Review* 1687, 1753.
104 Hartzog, "The Inadequate, Invaluable Fair Information Practices" (n 27) 964; Cate (n 102) 342.
105 John Braithwaite, "Rules and Principles: A Theory of Legal Certainty" 27 *Australasian Journal of Legal Philosophy* 47, 53–55.
106 Lyria Bennett Moses, "Recurring Dilemmas: The Law's Race to Keep up with Technological Change" (2007) *University of Illinois Journal of Law, Technology & Policy* 239, 258–264.
107 Bert-Jaap Koops, "The Trouble with European Data Protection Law" (2014) 4 *International Data Privacy Law* 250, 256–259. See also GDPR art 1.
108 BJ Ard, "The Limits of Industry-Specific Privacy Law" (2015) 51 *Idaho Law Review* 607, 608–613.
109 Rebecca Crootof and BJ Ard, "Structuring Techlaw" (2021) 34 *Harvard Journal of Law & Technology* 347, 368.
110 Aaron Sankin and Surya Mattu, "The High Privacy Cost of a 'Free' Website" (*The Markup*, 22 September 2020) <https://perma.cc/6S33-FWTQ>.
111 *Frank v Gaos* (2019) 139 Ct 1041 (Supreme Court).
112 Moses "Recurring Dilemmas: The Law's Race to Keep up with Technological Change" (n 106) 264–268.
113 See Chapter 1C.
114 Waldman, *Industry Unbound* (n 98) 99–160; Ari Ezra Waldman, "Habit and Performative Privacy" (2021) 10 *Social Epistemology Review and Reply Collective* 43, 47.

115 Waldman, *Industry Unbound* (n 98) 132–135, 212–215.
116 Gloria González Fuster and others, "The Right to Lodge a Data Protection Complaint: Ok But Then What? An Empirical Study of Current Practices Under The GDPR" (2022) Data Protection Law Scholars Network <https://perma.cc/9LH6-JHNB>. See also Woodrow Hartzog and Daniel J Solove, "The FTC and the New Common Law of Privacy" (2014) 114 *Columbia Law Review* 583, 595–597.
117 Estelle Massé, "Four Years Under the EU GDPR: How to Fix Its Enforcement" (*Access Now*, July 2022) 4 <https://perma.cc/NJ9W-6DB2>; Matt Burgess, "How GDPR Is Failing" (*Wired*, 23 May 2022) <https://perma.cc/E7CG-K9FP>.
118 *Lindqvist v Åklagarkammaren i Jönköpin* [2003] CJEU Case C-101/01, Case C-101/01.
119 Ibid.
120 The criminal charges were for processing personal information without notifying the authority, processing sensitive personal information absent agreement, and transferring it to another country. The fines added to SEK 4,300, which was just over USD 500 in 2003, "by multiplying the sum of SEK 100, representing Mrs. Lindqvist's financial position, by a factor of 40, reflecting the severity of the offence. Mrs. Lindqvist was also sentenced to pay SEK 300 to a Swedish fund to assist victims of crimes." Ibid paras 15–17.
121 See eg, Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González C-131/12 ECLIEUC2014317 ILEC 060 [26] [EU].
122 See Nadezhda Purtova, "The Law of Everything: Broad Concept of Personal Data and Future of EU Data Protection Law" (2018) 10 *Law, Innovation and Technology* 40, 61–62; Francesca Bignami, "The Case for Tolerant Constitutional Patriotism: The Right to Privacy before the European Courts" (2008) 41 *Cornell International Law Journal* 211, 233.
123 Purtova "The Law of Everything" (n 122).
124 W Gregory Voss and Hugues Bouthinon-Dumas, "EU General Data Protection Regulation Sanctions in Theory and in Practice" (2020) 37 *Santa Clara High Technology Law Journal* 1, 74–76, 91.
125 Michal S Gal and Oshrit Aviv, "The Competitive Effects of the GDPR" (2020) 16 *Journal of Competition Law and Economics* 349, 383–385; Mira Burri and Rahel Schär, "The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy" (2016) 6 *Journal of Information Policy* 479, 500.
126 Damien Geradin, Theano Karanikioti, and Dimitrios Katsifis, "GDPR Myopia: How a Well-Intended Regulation Ended up Favouring Large Online Platforms – the Case of Ad Tech" (2021) 17 *European Competition Journal* 47, 49; Garrett Johnson, Scott Shriver, and Samuel Goldberg, "Privacy & Market Concentration: Intended & Unintended Consequences of the GDPR" (2022) *Social Science Research Network*.
127 See Daphne Keller, "The Right Tools: Europe's Intermediary Liability Laws and the EU 2016 General Data Protection Regulation" (2018) 33 *Berkeley Technology Law Journal* 297, 316; Aylin Akturk and Jeremy Malcolm, "Unintended Consequences, European-Style: How the New EU Data Protection Regulation Will Be Misused to Censor Speech" (*Electronic Frontier Foundation*, 20 November 2015) <https://perma.cc/W4MJ-BM8K>; Nani Jansen Reventlow, "Can the GDPR and Freedom of Expression Coexist?" (2020) 114 *American Journal of International Law Unbound* 31, 33. See also "The EU General Data Protection Regulation: Questions and Answers" (*Human Rights Watch*, 6 June 2018) <https://perma.cc/2X73-YJ3L>.
128 See Amy Kristin Sanders, "The GDPR One Year Later: Protecting Privacy or Preventing Access to Information" (2019) 93 *Tulane Law Review* 1229, 1230. See also David Erdos, "Special, Personal and Broad Expression: Exploring Freedom of Expression Norms

under the General Data Protection Regulation" (2021) 40 *Yearbook of European Law* 398, 400.

129 See Roslyn Layton, "Statement before the Senate Judiciary Committee On the GDPR and CCPA: Opt-Ins, Consumer Control, and the Impact on Competition and Innovation" (*American Enterprise Institute*, 12 March 2019) 4–5 https://perma.cc/RC4W-U3YA; Stéphane Ciriani, "The Economic Impact of the European Reform of Data Protection" (2015) 97 *Digiworld Economic Journal* 41, 46, 51, 54–55; Jian Jia and Liad Wagman, "The One-Year Impact of the General Data Protection Regulation (GDPR) on European Ventures" (*Data Catalyst*, January 2020) <https://perma.cc/3644-EG2M>.

130 Gal and Aviv, "The Competitive Effects of the GDPR" (n 125) 368–369.

131 See Crootof and Ard, "Structuring Techlaw" (n 109) 370.

132 Jack M Balkin, "The Fiduciary Model of Privacy" (2020) 134 *Harvard Law Review Forum* 11, 27.

133 W Nicholson Price and others, "Shadow Health Records Meet New Data Privacy Laws" (2019) 363 *Science* 448.

134 "Data Overprotection" (2015) 522 Nature 391; Jan-Eric Litton, "We Must Urgently Clarify Data-Sharing Rules" (2017) 541 *Nature* 437; Robert Eiss, "Confusion over Europe's Data-Protection Law Is Stalling Scientific Progress" (2020) 584 *Nature* 498.

135 Cameron F Kerry, John B Morris, Jr., and Nicol E Turner Lee, "Bridging the Gaps: A Path Forward to Federal Privacy Legislation" (2020) The Brookings Institution 1, 20.

136 Waldman, *Industry Unbound* (n 98) 157–159.

137 GDPR art 22.

138 Ari Ezra Waldman, "Privacy Law's False Promise" (2020) 97 *Washington University Law Review* 773, 776–777.

139 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* C-131/12 (n. 119); ECR I-317, EUR-Lex CELEX No 62012CJ0131 2014 para 93.

140 W Gregory Voss and Celine Castets-Renard, "Proposal for an International Taxonomy on the Various Forms of the Right to Be Forgotten: A Study on the Convergence of Norms" (2016) 14 *Colorado Technology Law Journal* 281, 325–337; Andrea Slane, "Search Engines and the Right to Be Forgotten: Squaring the Remedy with Canadian Values on Personal Information Flow" (2018) 55 *Osgoode Hall Law Journal* 349, 358.

141 Orla Lynskey, "Control over Personal Data in a Digital Age: Google Spain v AEPD and Mario Costeja Gonzalez" (2015) 78 *The Modern Law Review* 522, 529; Robert C Post, "Data Privacy and Dignitary Privacy: Google Spain, the Right to Be Forgotten, and the Construction of the Public Sphere" (2017) 67 *Duke Law Journal* 981, 998.

142 Dawn Carla Nunziato, "The Fourth Year of Forgetting: The Troubling Expansion of the Right to Be Forgotten" (2017) 39 *University of Pennsylvania Journal of International Law* 1011, 1059–1063; Ignacio Cofone, "Online Harms and the Right to Be Forgotten" in Ignacio Cofone (ed), *The Right to be Forgotten* (Routledge 2020) 1, 11.

143 Pierre-Luc Déziel, "Let's Not Dwell on The Past: The Right to Be Forgotten as More Than a Romantic Revolution" in Ignacio Cofone (ed), *The Right to be Forgotten* (Routledge 2020) 59–61; Catalina Turriago Betancourt and Ignacio Cofone, "The Right to Be Forgotten in Peace Processes" in Ignacio N Cofone (ed), *The Right to be Forgotten* (Routledge 2020) 91–92.

144 Muge Fazlioglu, "Forget Me Not: The Clash of the Right to Be Forgotten and Freedom of Expression on the Internet" (2013) 3 *International Data Privacy Law* 149, 149; Edward Lee, "The Right to Be Forgotten v. Free Speech" (2015) 12 *I/S: A Journal of Law and Policy for the Information Society* 85, 92; Chelsea E Carbone, "To Be or Not to Be

Forgotten: Balancing the Right to Know with the Right to Privacy in the Digital Age" (2015) 22 *Virginia Journal of Social Policy & the Law* 553, 528; Teresa Scassa, "A Little Knowledge Is a Dangerous Thing?" in Ignacio Cofone (ed), *The Right to be Forgotten* (Routledge 2020) 26–39.

145 Fiona Brimblecombe and Gavin Phillipson, "Regaining Digital Privacy: The New Right to Be Forgotten and Online Expression" (2018) 4 *Canadian Journal of Comparative and Contemporary Law* 1, 6–7, 32.

146 Jasmine E McNealy, "The Emerging Conflict between Newsworthiness and the Right to Be Forgotten" (2012) 39 *Northern Kentucky Law Review* 119, 120–128. See also Jeffrey Rosen, "The Right to Be Forgotten" (2012) 64 *Stanford Law Review Online* 88.

147 Eloise Gratton and Jules Polonetsky, "Droit À L'Oubli: Canadian Perspective on the Global 'Right to Be Forgotten' Debate" (2017) 15 *Colorado Technology Law Journal* 337, 343–345.

148 Andrea Slane, "Reconciling Privacy and Expression Rights by Regulating Profile Compilation Services," in Ignacio Cofone (ed), *The Right to be Forgotten* (Routledge 2020); see also Slane "Search Engines and the Right to Be Forgotten: Squaring the Remedy with Canadian Values on Personal Information Flow" (n 140); Post, "Data Privacy and Dignitary Privacy: (n 141).

149 Solove, "The Limitations of Privacy Rights" (n 38) 39.

150 Alicia Solow-Niederman, "Information Privacy and the Inference Economy" (2022) 117 *Northwestern University Law Review* 357, 361.

151 GDPR art 17(3).

152 OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data 1980 s "Collection Limitation Principle."

153 Lina M. Khan, "Remarks of Chair Lina M. Khan as Prepared for Delivery IAPP Global Privacy Summit" (Washington, D.C., Federal Trade Commission, 22 April 2022) <https://perma.cc/B4VL-BNYA>.

154 Nick Saint, "Google CEO: 'We Know Where You Are. We Know Where You've Been. We Can More or Less Know What You're Thinking About.'" (*Insider*, 4 October 2010) <https://perma.cc/P982-5DWW>; Derek Thompson, "Google's CEO: 'The Laws Are Written by Lobbyists'" (*The Atlantic*, 1 October 2010) <https://perma.cc/Y97S-LYUS>.

155 Waldman, "Privacy, Practice, and Performance" (n 15) 1227. See also Waldman "Privacy's Rights Trap" (n 79) 93–94.

156 "Frances Haugen Written Testimony before United States Senate Committee on Commerce, Science and Transportation" (*Whistleblower Aid*, 4 October 2021) <https://perma.cc/MW2K-MS8Y>; Daniel E Slotnik, "Whistle-Blower Unites Democrats and Republicans in Calling for Regulation of Facebook (Updated 26 October 2021)" *The New York Times* (New York, 5 October 2021) <https://perma.cc/94DP-JTMC>.

157 Hartzog and Richards, "Privacy's Constitutional Moment and the Limits of Data Protection" (n 103) 1693–1694.

158 See Chapter 4C.

159 Paul Ohm, "Sensitive Information" (2014) 88 Southern California Law Review 1125, 1167.

160 See also "Hamburg Commissioner Fines H&M 35.3 Million Euro for Data Protection Violations in Service Centre" (*European Data Protection Board*, 2 October 2020) <https://perma.cc/4BLC-ABF3>.

161 European Commission, Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts 2021 [COM

206]. See also "The Digital Services Act" (*European Commission*) arts 34–35 <https://perma.cc/SYC2-NW6U>.

162 European Commission, Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts (n 161) Title II, art 5.

163 Ibid 5(1)(b).

164 François-Philippe Champagne, Bill C-27, An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts 2022.

165 Kate Conger, Richard Fausset, and Serge F Kovaleski, "San Francisco Bans Facial Recognition Technology" *The New York Times* (New York, 14 May 2019) <https://perma.cc/RN3T-5WZE>; "Somerville Becomes First East Coast City to Ban Government Use of Face Recognition Technology" (*American Civil Liberties Union*, 28 June 2019) <https://perma.cc/CD9B-W3YK>; Sarah Ravani, "Oakland Bans Use of Facial Recognition Technology, Citing Bias Concerns" *San Francisco Chronicle* (San Francisco, 16 July 2019) <https://perma.cc/Q9JC-D8QH>; "VICTORY: Bellingham Voters Ban Facial Recognition, Predictive Policing Software" (*American Civil Liberties Union of Washington*, 10 November 2021) <https://perma.cc/ET5R-S3QA>. See also "Ban Facial Recognition Map" (*Fight for the Future*, 2022) <https://perma.cc/2LVJ-JF3S>.

166 Margot E Kaminski, "Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability" (2018) 92 *Southern California Law Review* 1529.

167 GDPR art 5; "Accountability" (*European Data Protection Supervisor*) <https://perma.cc/NS9Q-MA5N>; GDPR art 5(2). See also Margot E Kaminski and Gianclaudio Malgieri, "Multi-Layered Explanations from Algorithmic Impact Assessments in the GDPR," *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency* (Association for Computing Machinery 2020) 69–70. See "PIPEDA Fair Information Principles" (*Office of the Privacy Commissioner of Canada*, 16 September 2011) <https://perma.cc/QNE9-W47T>.

168 Orla Lynskey (n 20) 33–34. The GDPR calls it a "principle" because it's meant to be implemented systemically.

169 GDPR art 5(1)(a); OECD, "Collection Limitation"; *Case C-524/06 Heinz Huber v Bundesrepublik Deutschland* (ECR I-09705) [54–62]; LGPD art. 6(III); APPI art 16.

170 H.B. 2307, 2021 Gen. Assemb., Spec. Sess. (Va. 2021) (to be codified at Va. Code Ann. ss 59.1-574(A)(1)–(2), 59.1-580(A)); Colo. Rev. Stat. s 6-1-1308(3) 2021; Cal. Civ. Code s 1798.100(a)(3) (Deering 2019).

171 Ann Cavoukian, "Privacy by Design" (*Information and Privacy Commissioner of Ontario*, 2013) 1 <https://perma.cc/B888-VQFC>.

172 Woodrow Hartzog, *Privacy's Blueprint: The Battle to Control the Design of New Technologies* (Harvard University Press 2018) 127.

173 Deirdre K Mulligan and Jennifer King, "Bridging the Gap between Privacy and Design" (2011) 14 *University of Pennsylvania Journal of Constitutional Law* 989, 999.

174 Crootof and Ard, "Structuring Techlaw" (n 109) 359–365.

175 Pierre Schlag, "Rules and Standards" (1985) 33 *UCLA Law Review* 379.

176 Braithwaite, "Rules and Principles: A Theory of Legal Certainty" (n 105) 53–55.

177 Daniel J Solove and Woodrow Hartzog, *Breached!* (Oxford University Press 2022) chs 6–7.

178 Schlag, "Rules and Standards" (n 175).

179 Cate, "The Failure of Fair Information Practice Principles" (n 102) 344.

180 Omer Tene and Jules Polonetsky, "Big Data for All: Privacy and User Control in the Age of Analytics" (2012) 11 *Northwestern Journal of Technology and Intellectual Property* 239, 260–262.
181 Ari Waldman, "Data Protection by Design? A Critique of Article 25 of the GDPR" (2020) 53 *Cornell International Law Journal* 147, 154, 165–166.
182 See Ari Ezra Waldman, "Privacy, Notice, and Design" (2018) 21 *Stanford Technology Law Review* 129; Hana Habib and others, "An Empirical Analysis of Data Deletion and Opt-Out Choices on 150 Websites," *USENIX Symposium on Usable Privacy and Security (SOUPS)* (USENIX Association 2019) <https://perma.cc/U7QH-BFFQ>; Idris Adjerid, Alessandro Acquisti, and George Loewenstein, "Choice Architecture, Framing, and Cascaded Privacy Choices" (2019) 65 *Management Science* 2267.
183 See Mark Sullivan, "These Are the Deceptive Design Tricks and Dark Patterns That Steer Your Clicks Each Day" (*Fast Company*, 25 June 2019) <https://perma.cc/ND6M-LTNJ>; Henry Wong, "Inside the Deceptive Design World of Dark Patterns" (*Design Week*, 9 March 2020) <https://perma.cc/XK9M-9T9Q>.
184 Restatement (Third) of Torts: Liability for Economic Harm (2020) s 9.
185 Balkin, "The Fiduciary Model of Privacy" (n 132) 13–15.
186 Richards, Why Privacy Matters (n 37) 203; Ariel Dobkin, "Information Fiduciaries in Practice: Data Privacy and User Expectations" (2018) 33 *Berkeley Technology Law Journal* 1.
187 Woodrow Hartzog and Neil Richards, "Legislating Data Loyalty" (2022) 97 *Notre Dame Law Review Reflection* 356, 364.
188 Woodrow Hartzog and Neil Richards, "The Surprising Virtues of Data Loyalty" (2021) 71 *Emory Law Journal* 985, 988–989.
189 Ibid.
190 Balkin (n 132) 11; Neil Richards and Woodrow Hartzog, "A Duty of Loyalty for Privacy Law" (2021) 99 *Washington University Law Review* 961, 966–967; Claudia E Haupt, "Platforms as Trustees: Information Fiduciaries and the Value of Analogy" (2020) 134 *Harvard Law Review Forum* 34, 36.
191 Balkin, "The Fiduciary Model of Privacy" (n 132) 24.
192 Waldman, *Privacy as Trust* (n 91) 79.
193 Richards and Hartzog "A Duty of Loyalty for Privacy Law" (n 190), 964; Haupt "Platforms as Trustees: Information Fiduciaries and the Value of Analogy" (n 190) 38.
194 Jack Balkin, "Information Fiduciaries and the First Amendment" (2016) 49 *U.C. Davis Law Review* 1183, 1205–1208; Lauren Henry Scholz, "Fiduciary Boilerplate: Locating Fiduciary Relationships in Information Age Consumer Transactions" (2020) 46 *Journal of Corporation Law* 143, 196.
195 Lina M Khan and David E Pozen, "A Skeptical View of Information Fiduciaries" (2019) 133 *Harvard Law Review* 497, 515.
196 Theodore Rostow, "What Happens When an Acquaintance Buys Your Data: A New Privacy Harm in the Age of Data Brokers" (2017) 34 *Yale Journal on Regulation Note* 667, 699–700.
197 Khan and Pozen, "A Skeptical View of Information Fiduciaries" (n 195) 520.
198 Ibid 503–504.
199 Daniel M Filler, David M Haendler, and Jordan L Fischer, "Negligence at the Breach: Information Fiduciaries and the Duty to Care for Data" (2022) 54 *Connecticut Law Review* 105, 134. See also Khan and Pozen "A Skeptical View of Information Fiduciaries" (n 195) 511–517.
200 Balkin, "Information Fiduciaries and the First Amendment" (n 194) 1208–1209.

6 PERVASIVE DATA HARMS

1 *Setoguchi* v *Uber BV* [2021] ABQB 18 1701 16003 [51] (citing *Jones* v. *Tsige*, 2012 ONCA 32, 346 DLR).
2 Daniel J Solove and Woodrow Hartzog, *Breached!* (Oxford University Press 2022) 140–142.
3 *Transunion LLC* v *Ramirez* [2021] Supreme Court of United States No. 20-297, No. 20-297 141 SCt 2190–2201 [US].
4 Ibid 2205.
5 Ibid 2205–2209.
6 Danielle Keats Citron, "Addressing Cyber Harassment: An Overview of Hate Crimes in Cyberspace" (2015) 6 *Case Western Reserve Journal of Law, Technology and the Internet* 1, 5–6; Thomas Kadri, "Networks of Empathy" (2020) 4 *Utah Law Review* 1075, 1081–1083; Danielle Keats Citron and Daniel J Solove, "Privacy Harms" (2022) 102 *Boston University Law Review* 793, 837–841.
7 Ari Waldman, "Cybermobs Multiply Online Threats and Their Danger" *New York Times* (New York, 3 August 2016) <https://perma.cc/C8AU-TXC6>.
8 Danielle Keats Citron, "A New Compact for Sexual Privacy" (2020) 62 *William & Mary Law Review* 1763, 1783.
9 Danielle Keats Citron, *The Fight for Privacy: Protecting Dignity, Identity, and Love in the Digital Age* (WW Norton 2022) 33–41; Danielle Keats Citron, *Hate Crimes in Cyberspace* (Harvard University Press 2014) 24–46.
10 Danielle Citron and Mary Anne Franks, "Criminalizing Revenge Porn" (2014) 49 *Wake Forest Law Review* 345, 350–356.
11 *Herrick v Grindr, LLC* (2018) 306 F Supp 3d 579 (Dist Court) 586, 588; Ari Ezra Waldman, "Law, Privacy, and Online Dating: 'Revenge Porn' in Gay Online Communities" (2019) 44 *Law & Social Inquiry* 987, 988; Ari Waldman, "Queer Dating Apps Are Unsafe by Design: Privacy Is Particularly Important for L.G.B.T.Q. People" *The New York Times* (New York, 20 June 2019) <https://perma.cc/N7S8-GKGS>.
12 Citron and Solove, "Privacy Harms" (n 6) 834–837.
13 Danielle Keats Citron, "Mainstreaming Privacy Torts" (2010) 98 *California Law Review* 1805, 1815, 1834; Marshall Allen, "Health Insurers Are Vacuuming Up Details About You – And It Could Raise Your Rates" (*ProPublica*, 17 July 2018) <https://perma.cc/XG32-AXBM>.
14 Joost Poort and Frederik Borgesius, "Does Everyone Have a Price? Understanding People's Attitude towards Online and Offline Price Discrimination" (2019) 8 *Internet Policy Review* 1, 2–5; Frederik Zuiderveen Borgesius and Joost Poort, "Online Price Discrimination and EU Data Privacy Law" (2017) 40 *Journal of Consumer Policy* 347, 348–353. See also Vincent Conitzer, Curtis R Taylor, and Liad Wagman, "Hide and Seek: Costly Consumer Privacy in a Market with Repeat Purchases" (2012) 31 *Marketing Science* 277, 277–280.
15 Daniel J Solove and Danielle Keats Citron, "Risk and Anxiety: A Theory of Data-Breach Harms" (2018) 96 *Texas Law Review* 737, 745, 766.
16 Ryan Calo, "Digital Market Manipulation" (2014) 82 *George Washington Law Review* 995, 999, 1003–1008; Tal Z. Zarsky, "Privacy and Manipulation in the Digital Age" (2019) 20 *Theoretical Inquiries in Law* 157, 172–174. See also Przemyslaw Palka, "The World of Fifty (Interoperable) Facebooks" (2020) 51 *Seton Hall Law Review* 1193, 1220. See generally Shoshana Zuboff, *The Age of Surveillance Capitalism* (1st ed., PublicAffairs 2019).
17 Mary Anne Franks, "Sexual Harassment 2.0" (2012) 71 *Maryland Law Review* 655, 657–658; Citron and Solove, "Privacy Harms" (n 6) 831–834.

18 Franks, "Sexual Harassment" (n 17) 657–659; Ari Ezra Waldman, "Amplifying Abuse: The Fusion of Cyberharassment and Discrimination" (2015) 95 *Boston University Law Review Annex* 83, 85–86. See also Citron, *The Fight for Privacy* (n 9) 89–90.
19 See Ian Parker, "The Story of a Suicide" *The New Yorker* (6 February 2012) <https://perma.cc/8BW7-ZSXA>; Michelle Dean, "The Story of Amanda Todd" *The New Yorker* (18 October 2012) <https://perma.cc/5ZEB-4MFZ>. See also Chapter 1B.
20 Svana Calabro, "From the Message Board to the Front Door: Addressing the Offline Consequences of Race- and Gender-Based Doxxing and Swatting" (2018) 51 *Suffolk University Law Review* 55, 57–60. See *R v BLA* (2015) BCPC 203 BCPC 203 [3] [Canada].
21 Danielle Keats Citron, "Sexual Privacy" (2019) 128 *Yale Law Journal* 1870, 1904–1928. See also Citron, *The Fight for Privacy* (n 9) 107–118.
22 Anita L Allen, "Dismantling the 'Black Opticon': Privacy, Race Equity, and Online Data" (2021) 131 *Yale Law Journal Forum* 907, 913–928; Citron and Solove, "Privacy Harms" (n 6) 855–859.
23 See *Fair Housing Council Of San Fernando Valley v Roommates.com, LLC* (2008) 521 F 3d 1157 (Court of Appeals, 9th Circuit) 1162, 1169 [US].
24 Ariana Tobin, "Facebook Promises to Bar Advertisers from Targeting Ads by Race or Ethnicity. Again" (*ProPublica*, 25 July 2018) <https://perma.cc/MC3F-A2GK>; Ariana Tobin and Jeremy B Merrill, "Besieged Facebook Says New Ad Limits Aren't Response to Lawsuits" (*ProPublica*, 23 August 2018) <https://perma.cc/VU2Z-Z3K7>.
25 Solon Barocas and Andrew Selbst, "Big Data's Disparate Impact" (2016) 104 *California Law Review* 671, 677–694; Ignacio Cofone, "Algorithmic Discrimination Is an Information Problem" (2019) 70 *Hastings Law Journal* 1389, 1428.
26 Frederik Zuiderveen Borgesius and others, "Online Political Microtargeting: Promises and Threats for Democracy" (2018) 14 *Utrecht Law Review* 82, 82–84.
27 Siva Vaidhyanathan, *Antisocial Media: How Facebook Disconnects Us and Undermines Democracy* (Oxford University Press 2018) 148–174.
28 "Meta Settles Cambridge Analytica Scandal Case for $725m" *BBC News* (London, 23 December 2022) <https://perma.cc/Z6TQ-GTSZ>.
29 Daniel Susser, Beate Roessler, and Helen Nissenbaum, "Online Manipulation: Hidden Influences in a Digital World" (2019) 4 *Georgetown Law Technology Review* 1, 34–41.
30 *Plaintiffs' Notice of Motion and Motion to Certify a Settlement Class and Grant Preliminary Settlement Approval* [2022] MDL No 2843, online: <https://perma.cc/Z8ZN-BELG>. Nate Raymond, "Facebook Parent Meta to Settle Cambridge Analytica Scandal Case for $725 Million" *Reuters* (London, 23 December 2022) <https://perma.cc/G4BS-YVQ9>.
31 Neil Richards, *Why Privacy Matters* (Oxford University Press 2021) 74–76.
32 Maria Angel and Ryan Calo, "Holes in the Umbrella: A Critique of Privacy as Taxonomy" (forthcoming 2023) 123 *Columbia Law Review*.
33 Ignacio Cofone, "Privacy Standing" (2022) *University of Illinois Law Review* 1367, 1401–1405.
34 Ryan Calo, "The Boundaries of Privacy Harm" (2011) 86 *Indiana Law Journal* 1131, 1143.
35 Ibid. See also Jeffrey Bellin, "Pure Privacy" (2021) 116 *Northwestern University Law Review* 463, 492–497; Jeffrey M Skopek, "Untangling Privacy: Losses versus Violations" (2020) 105 *Iowa Law Review* 2169, 2186.
36 *ArbG Düsseldorf, Urteil vom 05032020* [2020] ArbG Düsseldorf 9 Ca 6557/18, 9 Ca 655718 [111]; AG *Frankfurt/Main* [2020] 385 C 15519 70; see also pre-GDPR cases V *European Parliament* [2011] Case F-4609 [174–175]; *Nikolaou v Commission* [2007] CJEU T-259/03, T-25903 [301–304]; *Annibale Culin v Commission of the European Communities* [1990] Case C-34387 EUC199049 [27]; *Council of the European Union v Lieve de Nil*

and Christiane Impens [1998] ECJ Case C-259/96 P, EU:C:1998:224, Case C-25996 P EUC1998224 [23]; *Commission of the European Communities v Marie-Claude Girardot* [2008] ECJ C-348/06 P, EU:C:2008:107, C-34806 P EUC2008107 [54]; see also GDPR art. 82 in French (dommage matériel ou moral).

37 Cofone, "Privacy Standing" (n 33) 1396–1397.

38 Thomas Kadri, "Brokered Abuse" (2023) *Journal of Free Speech* 1, 8–11.

39 Ibid.

40 See Daniel Solove, "Conceptualizing Privacy" (2002) 90 *California Law Review* 1087, 1116. See also Section B.

41 Editorial Board, "The Unfinished Business of the Equifax Hack" (*Bloomberg*, 29 January 2019) <https://perma.cc/R4FW-6AAJ>.

42 Scott Skinner-Thompson, "Outing Privacy" (2015) 110 *Northwestern University Law Review* 159, 164–176.

43 Patrick Lorio, "Access Denied: Data Breach Litigation, Article III Standing, and a Proposed Statutory Solution" (2017) 51 *Columbia Journal of Law and Social Problems* 79, 91–105.

44 Felix T Wu, "Defining Privacy and Utility in Data Sets" (2013) 84 *University of Colorado Law Review* 1117, 1161–1162.

45 See *Kamal v J Crew Group, Inc* (2019) 918 F 3d 102 (Court of Appeals, 3rd Circuit) 113 [US]; *Katz v Donna Karan Company, LLC* (2017) 872 F 3d 114 (Court of Appeals, 2nd Circuit) 131 [US]; *Bassett v ABM Parking Services, Inc* (2018) 883 F 3d 776 (Court of Appeals, 9th Circuit) 777 [US]; *Crupar-Weinmann v Paris Baguette America, Inc* (2018) 861 F 3d 76 (Court of Appeals, 2nd Circuit) 77 [US]; *Meyers v Nicolet Restaurant of De Pere, LLC* (2016) 843 F 3d 724 (Court of Appeals, 7th Circuit) 729 [US].

46 See *Forbes v Wells Fargo Bank* [2006] Dist Court Minn No. Civ. 052409(DSD/RLE), 420 F Supp 2d 1018, 1020–21 [US]; *Guin v Brazos Higher Educ Serv Corp* [2006] US Dist LEXIS 4846 No. Civ. 05-668 RHK/JSM, Minn *15-17 [US]; *Stollenwerk v Tri-West Healthcare Alliance* [2005] US Dist LEXIS 41054 No. Civ. 03-0185-PHX-SRB, Ariz *7-*16 [US]; *Reilly v Ceridian Corp* (2011) 664 F 3d 38 (Court of Appeals, 3rd Circuit) 42, 45 [US]; *Wilson v Sessoms* [1998] US Dist LEXIS 8154 No. Civ. 4:96CV01031, Md *16-17 [US].

47 *Beck v. McDonald*, No. 15-1395 (4th Circuit 2017) [US].

48 *Spokeo, Inc v Robins* (2016) 136 Ct 1540 (Supreme Court) [US]; *Transunion LLC v. Ramirez* (n 3) paras 1553–1554.

49 Jeff Kosseff, "Defining Cybersecurity Law" (2017) 103 *Iowa Law Review* 985, 1016; Solove and Hartzog, Breached! (n 2) 55–59.

50 Margot E Kaminski, "Standing after Snowden: Lessons on Privacy Harm from National Security Surveillance Litigation" (2016) 66 *DePaul Law Review* 413, 422–430.

51 *In Re Horizon Healthcare Services Inc Data Breach Litig* (2017) 846 F 3d 625 (Court of Appeals, 3rd Circuit) 639 [US].

52 *Attias v Carefirst, Inc* (2017) 865 F 3d 620 (Court of Appeals, Dist of Columbia Circuit) 629–630 [US].

53 Travis LeBlanc and Jon R Knight, "A Wake-Up Call: Data Breach Standing Is Getting Easier" (2018) 4 *Cybersecurity Law Report* 1, 1–2.

54 Labor Court Dresden; Labor Court Lübeck [Germany].

55 *Urteil vom 26052020* [2020] LG Darmstadt 13 O 244/19, 13 O 24419 [Germany].

56 AG Hamburg-Barmbek *Urteil vom 18082020* [2020] AG Hamburg-Barmbek 816 C 33/20, 816 C 3320 [Germany].

57 Magistrate Court Hannover [Germany].

58 Orla Lynskey, "General Report Topic 2: The New EU Data Protection Regime" in Jorrit J Rijpma (ed), *The New Data Protection Regime: Setting Global Standards for the Right to Personal Data Protection*, vol 2 (Eleven International Publishing 2020) 68–69 <https://perma.cc/YS6K-WCQ9>.
59 UI v Österreichische Post AG [2022] C-300/21 [Austria].
60 Oliver Peschel, "Gerichtshof der Europäischen Union" (*noyb*, 29 September 2020) <https://perma.cc/Z6RB-HP87>.
61 "OGH Court Decision"(*Das Rechtsinformationssystem des Bundes (RIS)*, 15 April 2021) <https://perma.cc/TRR3-WPSD>.
62 Max Schrems, "No Non-Material Damages for GDPR Violations? Analysis of the Advocate General Opinion in C-300/21" (*noyb*, October 2022) 5, 14 <https://perma.cc/B432-NUHX>.
63 Campos Sánchez-Bordona, "Case C 300/21 UI v Österreichische Post AG (Opinion)" (*InfoCuria – Court of Justice of the European Union*, 6 October 2022) paras 27–34 <https://perma.cc/MDV7-WPQT>.
64 Ibid 113–116.
65 Laura Kabelka, "Privacy Activists Warn against Removing Compensation for Data Protection Breaches" (*Euractiv*, 13 October 2022) <https://perma.cc/Z33R-845L>.
66 See *Setoguchi v Uber B.V.* (n 1) para 53.
67 *Lamoureux v OCRCVM* [2021] QCCS 1093 [3–4].
68 Douez v Facebook, Inc (33 SCC) [59–61].
69 Felix T Wu, "How Privacy Distorted Standing Law" (2016) 66 *DePaul Law Review* 439, 447–448; Kaminski, "Standing after Snowden" (n 50) 416.
70 Alleruzzo v SuperValu, Inc (In re SuperValu, Inc, Customer Data Sec Breach Litig) [2017] 870 F3d 763 (8th Cir) [768, 773].
71 *Kirchein v Pet Supermarket, Inc* (2018) 297 F Supp 3d 1354 (Dist Court) 1354; *Katz v Pershing, Llc* (2012) 672 F 3d 64 (Court of Appeals, 1st Circuit) 80; *Reilly v. Ceridian Corp.* (n 46) 40, 44; *Meyers v. Nicolet Restaurant of De Pere, LLC* (n 45) 727.
72 Wu, "How Privacy Distorted Standing Law" (n 69) 459.
73 Neil Richards, "The Dangers of Surveillance" (2012) 126 *Harvard Law Review* 1934, 1934; Richards, *Why Privacy Matters* (n 31) 135.
74 Ryan Calo, "Privacy Harm Exceptionalism" (2014) 12 *Colorado Technology Law Journal* 361.
75 See Chapter 1B.
76 Daniel Townsend, "Who Should Define Injuries for Article III Standing" (2015) 68 *Stanford Law Review Online* 76, 79; Peter C Ormerod, "Privacy Injuries and Article III Concreteness" (2020) 48 *Florida State University Law Review* 133, 142–149, 173–191.
77 Ryan Calo, "A Long-Standing Debate: Reflections on Risk and Anxiety: A Theory of Data Breach Harms by Daniel Solove and Danielle Keats Citron Response" (2017) 96 *Texas Law Review Online* 59, 61–62. See *In Re Horizon Healthcare Services Inc. Data Breach Litig.* (n 51) 639; *Church v Accretive Health Inc* [2016] 11th Cir No. 15-15708, 654 Fed Appx 990, 994–95 [US].
78 Cofone, "Privacy Standing" (n 33) 1370; Citron and Solove, "Privacy Harms" (n 6).
79 See Chapter 5B.
80 Neil Richards and Woodrow Hartzog, "Trusting Big Data Research" (2017) 66 *DePaul Law Review* 579, 584.
81 See *Katz v. Donna Karan Company, LLC* (n 45) 119.
82 Julie E Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (Oxford University Press 2019) 145.

83 See *Transunion LLC v. Ramirez* (n 3) paras 2203–2214.
84 Ibid 2200.
85 Ibid.
86 Ibid.
87 Citron and Solove, "Privacy Harms" (n 6) 828–829.
88 Daniel J Solove and Danielle Keats Citron, "Standing and Privacy Harms: A Critique of Transunion v. Ramirez" (2021) 101 *Boston University Law Review Online* 62, 69.
89 Cofone, "Privacy Standing" (n 33) 1415.
90 *Transunion LLC v. Ramirez* (n 3) paras 2218–2219 (Thomas, J., dissenting); Kaminski (n 50) 416.
91 Kashmir Hill, "The Secretive Company That Might End Privacy as We Know It" *The New York Times* (New York, 18 January 2020) <https://perma.cc/B2JF-547D>.
92 Kashmir Hill, "Facial Recognition Start-Up Mounts a First Amendment Defense" *The New York Times* (New York, 11 August 2020) <https://perma.cc/5XDL-K5QK>.
93 Hill, "The Secretive Company That Might End Privacy as We Know It" (n 91).
94 Hill, "Facial Recognition Start-Up Mounts a First Amendment Defense" (n 92).
95 Evan Selinger and Woodrow Hartzog, "The Inconsentability of Facial Surveillance" (2019) 66 *Loyola Law Review* 101.
96 Charlie Warzel, "We Need a Law to Save Us From Dystopia" *The New York Times* (New York, 21 January 2020) <https://perma.cc/E5ZM-BAU9>.
97 Richards, *Why Privacy Matters* (n 31) 32–33.
98 Woodrow Hartzog and Evan Selinger, "Surveillance as Loss of Obscurity" (2015) 72 *Washington and Lee Law Review* 1343.
99 Ignacio Cofone and Adriana Robertson, "Privacy Harms" (2018) 69 *Hastings L.J.* 1039, 1049–1056.
100 *Brown v Google LLC and Alphabet Inc* (ND Cal) [3–4].
101 Ben Popken, "Google Sells the Future, Powered by Your Personal Data" *NBC News* (New York, 10 May 2018) <https://perma.cc/KW67-AK62>.
102 "Topics: The New Privacy Sandbox Proposal for Interest-Based Advertising" (*Google Ads Help*, 22 February 2022) <https://perma.cc/VEU9-TMAD>.
103 Cofone and Robertson, "Privacy Harms" (n 99) 1050–1051.
104 Hartzog and Selinger, "Surveillance as Loss of Obscurity" (n 98) 1363; Evan Selinger and Woodrow Hartzog, "Obscurity and Privacy," Spaces for the Future (Routledge 2017) 4, 8.
105 Cofone and Robertson, "Privacy Harms" (n 99) 1051.
106 Richards, *Why Privacy Matters* (n 31) 21–34. See also Chapter 1B.
107 *Frank v Gaos* (2019) 139 Ct 1041 (Supreme Court) 1044. See also Chapter 4C.
108 Ibid 1045–1046. See also *In re Google Referrer Header Privacy Litigation* [2020] US Dist Court LEXIS 99291 No. 10-cv-04809-EJD, 465 F Supp 3d 999, 1007–1010.
109 Cofone and Robertson, "Privacy Harms" (n 99) 1059–1060.
110 Lior Strahilevitz, "A Social Networks Theory of Privacy" (2005) 72 *The University of Chicago Law Review* 919, 939. See *Sanders v ABC* [1999] Supreme Court No. S059692., 978 P 2d 67 [911] [US].
111 Strahilevitz, "A Social Networks Theory of Privacy" (n 110) 920–925.
112 Ibid 953–954.
113 Ibid 988.
114 "Norwegian DPA: Intention to Issue €10 Million Fine to Grindr LLC" (*European Data Protection Board*, 26 January 2021) <https://perma.cc/DNQ4-3KKP>; "Out of Control: Complaints and Follow Up" (*Forbrukerrådet*, 14 January 2020) <https://perma.cc/

ZGX5-6L5Z>; "Administrative Fine – Grindr LLC" (*Datatilsynet*, 13 December 2021) <https://perma.cc/F9AG-T59K>. See also Chapter 3C.

115 William Prosser, "Privacy" (1960) 48 *California Law Review* 383, 392–98.
116 Cofone and Robertson, "Privacy Harms" (n 99) 1058–1061.
117 Strahilevitz, "A Social Networks Theory of Privacy" (n 110) 988.
118 *Transunion LLC v. Ramirez* (n 3) para 2209.
119 Scott Skinner-Thompson, *Privacy at the Margins* (Cambridge University Press 2020) 8–10.
120 Wu, "Defining Privacy and Utility in Data Sets" (n 44) 1157.
121 *Lloyd v Google* (UKSC 50) [9–14].
122 Ibid 92.
123 Richards, "The Dangers of Surveillance" (n 73) 1951.
124 *Lloyd v. Google* (n 121) para 159.
125 Calo, "The Boundaries of Privacy Harm"(n 34) 1142.
126 Maria Lillà Montagnani and Mark Verstraete, "What Makes Data Personal?" (2023) 56 *U.C. Davis Law Review* 25–27*.
127 See Chapter 5B.
128 Bellin, "Pure Privacy" (n 35) 495–496.
129 Ryan Calo, "Privacy Law's Indeterminacy" (2019) 20 *Theoretical Inquiries in Law* 33, 40.
130 See Helen Nissenbaum, *Privacy in Context: Technology, Policy and the Integrity of Social Life* (Stanford University Press 2010) 67–88.
131 *Spokeo, Inc.* v *Robins* (n 48) 1546, 1550.
132 Solove, "Conceptualizing Privacy" (n 40) 1092.
133 Nissenbaum, *Privacy in Context: Technology, Policy and the Integrity of Social Life* (n 130) 186.
134 Daniel J Solove, "A Taxonomy of Privacy" (2005) 154 *University of Pennsylvania Law Review* 477, 484.
135 Maria Angel and Ryan Calo (n 32) 3–5*.
136 Neil Richards, *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age* (Oxford University Press 2015) 95–108.
137 Daniel Susser, Beate Roessler, and Helen Nissenbaum, "Technology, Autonomy, and Manipulation" (2019) 8 *Internet Policy Review* 1, 6.
138 Nitasha Tiku, "Welcome to the Next Phase of the Facebook Backlash" (*Wired*, 21 May 2017) <https://perma.cc/TPJ6-BG2B>; Darren Davidson, "Facebook Targets 'Insecure' Young People" *The Australian* (Surrey Hills, 1 May 2017) <https://perma.cc/S9CU-HW33>; "Comments on Research and Ad Targeting" (*Meta*, 30 April 2017) <https://perma.cc/KKS5-36HT>. See also Chapter 2C.
139 See Chapter 3C.
140 Calo, "Digital Market Manipulation" (n 16) 1029.
141 Luciano Floridi, "The Informational Nature of Personal Identity" (2011) 21 *Minds and Machines* 549, 562; Samuel Warren and Louis Brandeis, "The Right to Privacy" (1890) 4 *Harvard law Review* 193, 195–196. See also Citron and Solove, "Privacy Harms" (n 6) 859–861.
142 Danielle Keats Citron, "The Roots of Sexual Privacy: Warren and Brandeis & the Privacy of Intimate Life" (2019) 42 *Columbia Journal of Law & the Arts* 383, 385–386.
143 Neil Richards and Daniel Solove, "Privacy's Other Path: Recovering the Law of Confidentiality" (2007) 96 *Georgetown Law Journal* 123, 128–133. See also Warren and Brandeis, "The Right to Privacy" (n 141); Citron, "The Roots of Sexual Privacy" (n 142).

144 Brent Mittelstadt, "From Individual to Group Privacy in Big Data Analytics" (2017) 30 *Philosophy & Technology* 475, 481–483.
145 Tobin, "Facebook Promises to Bar Advertisers From Targeting Ads by Race or Ethnicity. Again" (n 24); Tobin and Merrill, "Besieged Facebook Says New Ad Limits Aren't Response to Lawsuits" (n 24).
146 Christopher McCrudden, "Human Dignity and Judicial Interpretation of Human Rights" (2008) 19 *European Journal of International Law* 655, 679–680.
147 See generally Immanuel Kant, *Grounding for the Metaphysics of Morals* (first published 1785, Cambridge 2012) (discussing the idea of people as ends in themselves as tied to their dignity).
148 Edward J Bloustein, "Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser" (1964) 39 *New York University Law Review* 962, 1000–1007. See also Stanley Benn, "Privacy, Freedom and Respect for Persons" in Ronald Pennock and John Chapman (eds), *Nomos XIII: Privacy*, vol 8 (Atherton Press 1971) 8–9; Jeffrey Reiman, "Privacy, Intimacy and Personhood" (1976) 6 *Philosophy & Public Affairs* 26, 39.
149 Clare McGlynn and Erika Rackley, "Image-Based Sexual Abuse" (2017) 37 *Oxford Journal of Legal Studies* 534, 546–547; Citron, *The Fight for Privacy* (n 9) 105–130. See also Citron and Franks, "Criminalizing Revenge Porn" (n 10) 350–356.
150 See GDPR art 88. See also "Opinion 4/2015 Towards a New Digital Ethics: Data, Dignity and Technology" (*European Data Protection Supervisor*, 11 September 2015) 12 <https://perma.cc/TF9H-ABHV> ("Privacy is an integral part of human dignity, and the right to data protection was originally conceived in the 1970s and 1980s as a way of compensating the potential for the erosion of privacy and dignity through large scale personal data processing"); James Whitman, "The Two Western Cultures of Privacy: Dignity Versus Liberty" (2004) 113 *Yale Law Journal* 1151, 1154–1160. See *Campbell v MGN* [2004] 2 AC 457 [51].
151 Citron and Solove, "Privacy Harms" (n 6) 841–845; Solove and Citron, "Risk and Anxiety: A Theory of Data-Breach Harms" (n 15) 769–771. See also William Prosser and Wade, "Restatement of the Law (Second) of Torts s 652" (*The American Law Institute*, 1977) 652H <https://perma.cc/923C-77BG>.
152 Solove and Citron, "Risk and Anxiety: A Theory of Data-Breach Harms" (n 15) 778–781; Kadri, "Brokered Abuse" (n 38) 10–11.
153 See*Hosking v Runting*, [2005] 1 N.Z.L.R. 1 para 58 [NZ]; *Campbell v. MGN* (n 150) para 51.
154 Woodrow Hartzog and Daniel J Solove, "The Scope and Potential of FTC Data Protection" (2014) 83 *George Washington Law Review* 2230, 2284.
155 Cristina Bicchieri, Ryan Muldoon, and Alessandro Sontuoso, "Social Norms" in Edward N Zalta (ed), *The Stanford Encyclopedia of Philosophy* (Winter 2018, Metaphysics Research Lab, Stanford University 2018) <https://perma.cc/D65U-977Y>.
156 Helen Nissenbaum, "Contextual Integrity Up and Down the Data Food Chain" (2019) 20 *Theoretical Inquiries in Law* 221, 224–228. See also Nissenbaum, *Privacy in Context: Technology, Policy and the Integrity of Social Life* (n 130) 132–147.
157 Bicchieri, Muldoon, and Sontuoso, "Social Norms" (n 155).
158 Paul Ohm, "Sensitive Information" (2014) 88 *Southern California Law Review* 1125, 1166.
159 Nissenbaum, *Privacy in Context: Technology, Policy and the Integrity of Social Life* (n 130) 186.
160 Peter Ormerod, "Making Privacy Injuries Concrete" (2022) 79 *Washington and Lee Law Review* 101, 146–154. See also Helen Nissenbaum, "Privacy as Contextual Integrity" (2004) 79 *Washington Law Review* 119, 136–157.

161 Helen Nissenbaum, "Respect for Context as a Benchmark for Privacy Online: What It Is and Isn't" in Carine Dartiguepeyrou (ed), *The Futures of Privacy* (2019) 23–25; Helen Nissenbaum, "Respecting Context to Protect Privacy: Why Meaning Matters" (2018) 24 *Science and Engineering Ethics* 831, 839.
162 Nissenbaum, *Privacy in Context: Technology, Policy and the Integrity of Social Life* (n 130) 129–157.
163 Woodrow Hartzog, "Social Data" (2013) 74 *Ohio State Law Journal* 995, 1019; Frederic Stutzman and Woodrow Hartzog, "Boundary Regulation in Social Media" (2012) Proceedings of the ACM 2012 conference on Computer Supported Cooperative Work 769, 776.
164 Cofone and Robertson, "Privacy Harms" (n 99) 1055.
165 Nissenbaum, "Contextual Integrity Up and Down the Data Food Chain" (n 156) 234.
166 Andrea Slane and Ganaele Langlois, "Debunking the Myth of 'Not My Bad': Sexual Images, Consent, and Online Host Responsibilities in Canada" (2018) 30 *Canadian Journal of Women and the Law* 42, 63–79.
167 See Chapter 5B.
168 Ari Ezra Waldman, *Privacy as Trust: Information Privacy for an Information Age* (Cambridge University Press 2018) 34–45.
169 Nissenbaum, *Privacy in Context: Technology, Policy and the Integrity of Social Life* (n 130) 129–158.
170 Ormerod, "Making Privacy Injuries Concrete" (n 160) 146–154.
171 Steve Krenzel [@stevekrenzel], "Tweet about Twitter's Change in Ownership" (*Twitter*, 7 November 2022) <https://perma.cc/SN92-CQ2T>.
172 Steve Krenzel [@stevekrenzel], "Telco Data Tweet" (*Twitter*, 7 November 2022) <https://perma.cc/2JD8-GTE6>.
173 Steve Krenzel [@stevekrenzel], "Telco Director Tweet" (*Twitter*, 7 November 2022) <https://perma.cc/AXJ9-EFJJ>.
174 Steve Krenzel [@stevekrenzel], "User Terms of Service Tweet" (*Twitter*, 7 November 2022) <https://perma.cc/6DL4-7CAD>.
175 Steve Krenzel [@stevekrenzel], "New Owner of Twitter Mindset Tweet" (*Twitter*, 7 November 2022) <https://perma.cc/M7RY-DKPA>.
176 See Jules L Coleman, *Risks and Wrongs* (Oxford University Press 2002) 223.
177 Ira S Rubinstein and Woodrow Hartzog, "Anonymization and Risk" (2016) 91 *Washington Law Review* 703, 706.
178 See Chapter 5C.
179 Solove and Hartzog, Breached! (n 2) 144–146.
180 See Chapters 3B, 4B. See also Omer Tene and Jules Polonetsky, "Big Data for All: Privacy and User Control in the Age of Analytics" (2012) 11 *Northwestern Journal of Technology and Intellectual Property* 239, 261. Jessica Litman, "Information Privacy/Information Property" (2000) 52 *Stanford Law Review* 1283, 1309–1311. See generally Guido Calabresi and A. Douglas Melamed, "Property Rules, Liability Rules, and Inalienability: One View of the Cathedral" (1972) 85 *Harvard Law Review* 1089, 1119–1121.
181 See Chapter 3A.
182 Rubinstein and Hartzog, "Anonymization and Risk" (n 177) 730.
183 See Chapter 5A.
184 Ari Ezra Waldman, "Privacy, Practice, and Performance" (2022) 110 *California Law Review* 1221, 1227.
185 Jack M Balkin, "The Fiduciary Model of Privacy" (2020) 134 *Harvard Law Review Forum* 11, 11–14; Neil Richards and Woodrow Hartzog, "A Duty of Loyalty for Privacy Law" (2021) 99 *Washington University Law Review* 961, 966–967.

186 Robert H Sitkoff, "The Economic Structure of Fiduciary Law" (2011) 91 *Boston University Law Review* 1039, 1042–1045; Frank H. Easterbrook and Daniel R. Fischel, "Corporate Control Transactions" (1982) 91 *Yale Law Journal* 698, 702–703.
187 Lina M. Khan and David E. Pozen, "A Skeptical View of Information Fiduciaries" (2019) 133 *Harvard Law Review* 497, 520.
188 Daniel M. Filler, David M. Haendler, and Jordan L. Fischer, "Negligence at the Breach: Information Fiduciaries and the Duty to Care for Data" (2022) 54 *Connecticut Law Review* 105, 134. See also Khan and Pozen (n 187) 511–517.
189 Khan and Pozen, "A Skeptical View of Information Fiduciaries" (n 187) 515.
190 Theodore Rostow, "What Happens When an Acquaintance Buys Your Data: A New Privacy Harm in the Age of Data Brokers" (2017) 34 *Yale Journal on Regulation Note* 667, 699–700.
191 Khan and Pozen, "A Skeptical View of Information Fiduciaries" (n 187) 503–504.
192 Alan McQuinn and Daniel Castro, "A Grand Bargain on Data Privacy Legislation for America," *Information Technology and Innovation Foundation* (2019) 61.
193 Karin M. McGinnis, "Beck v. McDonald – 4th Circuit Weighs In on Standing in Data Breach Case" (*Data Points*, 8 February 2017) <https://perma.cc/N6MA-YRRA>.
194 See Wayne Unger, "Reclaiming Our Right to Privacy by Holding Tech. Companies Accountable" (2020) 27 *Richmond Journal of Law & Technology* 1, 8, 22–27.
195 Maria Angel and Ryan Calo (n 32); Neil M Richards, "The GDPR as Privacy Pretext and the Problem of Co-Opting Privacy" (2022) 73 *Hastings Law Journal* 1511, 1523–1537; Ignacio Cofone and Katherine J Strandburg, "Strategic Games and Algorithmic Secrecy"(2019) 64 *McGill Law Journal* 623, 632–633.
196 Cofone, "Privacy Standing" (n 33) 1372–1373.
197 Cameron F Kerry and others, "Bridging the Gaps: A Path Forward to Federal Privacy Legislation" (Brookings Place 2020) 19–21.
198 CCPA s 128.5.
199 Omri Ben-Shahar, "Data Pollution" (2019) 11 *Journal of Legal Analysis* 104, 127.
200 Ibid 125–126. See also Jack M Balkin, "Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation" (2018) 51 *U.C. Davis Law Review* 1149, 1167–1168.
201 Margot E Kaminski, "Regulating the Risks of AI" (2023) 103 *Boston University Law Review* 18, 69.
202 Leon Trakman, Robert Walters, and Bruno Zeller, "Tort and Data Protection Law: Are There Any Lessons to Be Learnt?" (2019) 5 *European Data Protection Law Review* 500, 517–518. Solove and Citron, "Risk and Anxiety: A Theory of Data-Breach Harms" (n 15) 785.
203 Ben-Shahar, "Data-Pollution" (n 199) 125–127.
204 *Spokeo, Inc. v. Robins* (n 48) 1548.
205 Cofone, "Privacy Standing" (n 33) 1371–1375, 1397–1399.
206 See *Aubry v Éditions Vice-Versa Inc*, [1998] 1 S.C.R. 591 [Canada].
207 Donald G Gifford, "The Challenge to the Individual Causation Requirement in Mass Products Torts" (2005) 62 *Washington and Lee Law Review* 873, 908.
208 Market share liability would be less effective because it assumes harm is proportional to market share. See Ignacio Cofone, "The Limits of Probabilistic Causality in Law" (2015) 15 *Global Jurist* 29, 47–48. This is not the case for companies with different data practices that have different risks.
209 Omri Ben-Shahar and Kyle D Logue, "How Insurance Substitutes for Regulation Insurance" (2013) 36 *Regulation* 36, 37–38; Jay P Kesan and Carol M Hayes, "Strengthening Cybersecurity with Cyberinsurance Markets and Better Risk Assessment"

(2017) 102 *Minnesota Law Review* 191, 231–232. But see Kenneth S. Abraham and Daniel Schwarcz, "The Limits of Regulation by Insurance" (2022) 98 *Indiana Law Journal* 5.

210 Asaf Lubin, "Public Policy and the Insurability of Cyber Risk" (2021) 5 *Journal of Law and Technology at Texas (JOLTT)* 45, 101–107.

211 Asaf Lubin, "Insuring Evolving Technology" (2021) 28 *Connecticut Insurance Law Journal* 130.

212 See "Brief of the Chamber of Commerce of the United States of America and the International Association of Defense Counsel as Amici Curiae in Support of Petitioner" 6–8, 15–16; *Spokeo, Inc. v. Robins* (n 48) para 1549.

213 Citron, "Mainstreaming Privacy Torts" (n 13) 1847.

214 See Citron and Solove, "Privacy Harms" (n 6) 799–813.

215 See Chapter 7A,C.

7 PRIVACY AS CORPORATE ACCOUNTABILITY

1 Daniel J Solove and Woodrow Hartzog, *Breached!* (Oxford University Press 2022) 128–137.

2 Jim Bronskill, "Data Breach at Desjardins Caused by Series of Gaps, Privacy Watchdog Says" *Global News* (Vancouver, 14 December 2020) <https://perma.cc/L8L4-AR4T>.

3 "Desjardins Identity Protection | Desjardins Security" (*Desjardins*, 2020) <https://perma.cc/4X7V-4TC8>.

4 The Canadian Press, "Desjardins Settles 2019 Data Breach Class-Action Lawsuit for up to Nearly $201M" *CBC* (Ottawa, 16 December 2021) <https://perma.cc/DVS3-5WFM>; "Quebec Court Approves $200.9M Settlement against Desjardins over Data Breach | CBC News" *CBC* (Ottawa, 17 June 2022) <https://perma.cc/A27G-D9ST>. The breach also forced the bank to create a more robust practice to hold data, an example of "after-the-fact" accountability. Desjardins created a 900-people security office with a starting budget of $150 million. This is an example of how corporations begin to internalize externalities even with minimal accountability: Liability forces corporations to change their behavior. See also "Frequently Asked Questions" (*Desjardins Settlement*) <https://perma.cc/WX4Q-RR6L>. Victims who didn't prove material harm received $90 for loss of time.

5 "Equifax Data Breach Settlement" (*Federal Trade Commission*, December 2022) <https://perma.cc/BR69-3V5T>.

6 "Stipulated Order for Permanent Injunction and Monetary Judgment, Federal Trade Commission v. Equifax Inc." (*Case 1:19-mi-99999-UNA*, 22 July 2019) 27–31 <https://perma.cc/47ER-XQBN>. See also Sean Hollister, "Why You Probably Won't Actually Get $125 from the Equifax Settlement" (*The Verge*, 26 July 2019) <https://perma.cc/86MX-UDZ3>.

7 Federal examples are the Fair Credit Reporting Act (15 U.S.C. s 1681 et seq.), the Telephone Consumer Protection Act (47 U.S.C. s 227), the Fair Debt Collection Practices Act (15 USC s 1692 et seq.), the Children's Online Privacy Protection Act, the Cable Communications Policy Act (15 USC s 6501), the Driver's Privacy Protection Act (18 USC s 2721 et seq.), the Fair and Accurate Credit Transactions Act (15 USC 1681 et seq.), the Stored Communications Act (18 USC ss 2701 to 2710), and the Video Privacy Protection Act (18 USC s 2710). A state-level example is Illinois' Biometric Information Privacy Act (SB2400, Public Act 095-0994).

8 *Mutnick v Clearview AI, Inc, No 1:20-cv-00512, 2020 US Dist LEXIS 144583 (ND Ill)*.

9 Isobel Asher Hamilton, "Zoom Is Being Sued for Allegedly Handing over Data to Facebook" (*Business Insider*, 31 March 2020) <https://perma.cc/Y3F3-DUC5>.

10 *Heeger et al v Facebook, Inc ND Cal*, No 18-cv-06399-JD (Order Re: Motion to Dismiss).
11 Health Insurance Portability and Accountability Act, Pub.L. 104–191; Gramm-Leach-Bliley Act, Pub.L. 106–102; Family Educational Rights and Privacy Act, 20 U.S.C. s 1232g.
12 Fair Credit Reporting Act, Pub.L. 91-508; Financial Privacy Act, Pub.L. 95–630.
13 *Transunion LLC v Ramirez* [2021] Supreme Court of United States No. 20-297, No. 20-297 141 SCt 2190 [1–3] [US].
14 Virginia Consumer Data Protection Act 2021 [H.B. 2307]; Colorado Privacy Act 2021 [S.B. 21-190].
15 Anupam Chandler, Margot Kaminski, and William McGeveran, "Catalyzing Privacy Law" (2021) 105 *Minnesota Law Review* 1733, 1759; California Consumer Privacy Act of 2018, 1.81.5 Calif. Civ. Code s 1798.150, s 1798.155(a)-(b) 2018.
16 *C-362/14 Schrems v Data Protection Commissioner* [64–65, 95]; Article 47 of the EU Charter of Fundamental Rights arts 22–23.
17 GDPR arts 79-82.
18 Emmanuela N Truli, "The General Data Protection Regulation and Civil Liability" in Mor Bakhoum and others (eds), *Personal Data in Competition, Consumer Protection and Intellectual Property: Towards a Holistic Approach?* (Springer 2018) 313–334.
19 See Chapter 6A.
20 See GDPR arts 79–82(1).
21 See Chapter 5A, B.
22 "Enforcement of PIPEDA" (*Office of the Privacy Commissioner of Canada*, 20 April 2017) <https://perma.cc/2YZC-JRBB>.
23 Arturo J Carrillo and Matías Jackson, "Follow the Leader? A Comparative Law Study of the EU's General Data Protection Regulation's Impact in Latin America" (2022) 16 *ICL Journal* 177, 193–194; "Article 42 – Geral Da Proteção De Dados Pessoais (LGPD)" (*Brazil*) <https://perma.cc/NG9E-XTPA>; "Arts 33-34 – Ley de Proteccion de Datos Personales" (*Argentina*) <https://perma.cc/XFN3-2MUD>; "Personal Data Protection Act 2012" (*Singapore Statutes Online*, 2020) s 32(1) <https://perma.cc/FQ3N-N37F>. See also An Act to modernize legislative provisions as regards the protection of personal information 2021 [c 25] s 93.1; Privacy Act 1996 [c 373] s 1(1).
24 *Rechtbank Overijssel* (Overijssel District Court) (2019) AWB 18/2047; Jan Spittka, "Germany: First Court Decision on Claims for Immaterial Damages under GDPR: Privacy Matters" (*DLA Piper*, 12 December 2018) <https://perma.cc/9GXE-GDDZ>.
25 Jon L Mills and Kelsey Harclerode, "Privacy, Mass Intrusion, and the Modern Data Breach" (2017) 69 *Florida Law Review* 771, 785–788.
26 Daniel J Solove and Danielle Keats Citron, "Risk and Anxiety: A Theory of Data-Breach Harms" (2018) 96 *Texas Law Review* 737, 749–754.
27 Chandler, Kaminski, and McGeveran, "Catalyzing Privacy Law" (n 15) 1759; California Consumer Privacy Act of 2018, 1.81.5 Calif. Civ. Code § 1798.150, s 1798.155(a)-(b).
28 Nicolas Vermeys, "Why Class Action Suits for Security Breaches Need to Look Beyond Privacy Concerns" in Ignacio Cofone (ed), *Class Actions in Privacy Law* (Routledge 2020) 82.
29 Stephen D. Burns and others, "Breach Notification Rules Under GDPR, PIPEDA and PIPA" (*Bennett Jones*, 1 October 2018) <https://perma.cc/96RZ-GKG8>. Paul M Schwartz and Edward J Janger, "Notification of Data Security Breaches" (2006) 105 *Michigan Law Review* 913, 915–916; Mark Verstraete and Tal Zarsky, "Optimizing Breach Notification" (2021) *University of Illinois Law Review* 803, 805–806. See also GDPR, Article 34.
30 *Davis v Facebook* [2020] 956 F3d 589, 598–600.

31 William Prosser and Wade, "Restatement of the Law (Second) of Torts s 652" (*The American Law Institute*, 1977) <https://perma.cc/923C-77BG>; William Prosser, "Privacy" (1960) 48 *California Law Review* 383, 389. See also Neil Richards and Daniel Solove, "Privacy's Other Path: Recovering the Law of Confidentiality" (2007) 96 *Georgetown Law Journal* 123, 126.
32 Daniel J Solove and Paul M Schwartz, "Privacy Law Fundamentals" (International Association of Privacy Professionals 2019) 5th ed 2, 17–18.
33 Ignacio Cofone and Adriana Robertson, "Privacy Harms" (2018) 69 *Hastings Law Journal* 1039, 1061. See also Chapter 6B.
34 Danielle Keats Citron, "Mainstreaming Privacy Torts" (2010) 98 *California Law Review* 1805, 1831–1852; Richards and Solove, "Privacy's Other Path: Recovering the Law of Confidentiality" (n 31) 145–156.
35 Neil M Richards, "The Limits of Tort Privacy" (2011) 9 *Journal on Telecommunications & High Technology Law* 357, 382–384.
36 Leon Trakman, Robert Walters, and Bruno Zeller, "Tort and Data Protection Law: Are There Any Lessons to Be Learnt?" (2019) 5 *European Data Protection Law Review* 500, 505–513.
37 Matthew S. DeLuca, "The Hunt for Privacy Harms after Spokeo" (2018) 86 *Fordham Law Review* 2439, 2458–2464.
38 See In re Vizio, Inc. Consumer Privacy Litig., 238 F. Supp. 3d 1204, 1215-17 (C.D. Cal. 2017) [US].
39 See *Rechtbank Overijssel* (n 24) (Netherlands); *Rechtbank Amsterdam* (Amsterdam District Court) (2019) 7560515 CV EXPL 19-4611 <https://perma.cc/8LTZ-7X7J>; *Rechtbank Noord-Nederland* (North Holland District Court) (2020) C/18/189406/HA ZA 19-6 <https://perma.cc/65VJ-B4KY>. Spindler and Horváth, "DS-GVO Art. 82 – Haftung Und Recht Auf Schadenersatz," *RECHT DER ELEKTRONISCHEN MEDIEN (4th ed Splinder/Schuster)* (2019) 757. See also art 6:106 of the Dutch Civil Code.
40 *Vidal-Hall, Hann and Bradshaw v Google Inc* (EWHC 13 (QB)) [96–98].
41 *Vidal-Hall, Hann and Bradshaw v Google Inc* (EWCA Civ 311) [95–98].
42 Ibid 77.
43 Jojo YC Mo, "Misuse of Private Information as a Tort: The Implications of Google v Judith Vidal-Hall" (2017) 33 *Computer Law & Security Review* 87, 96.
44 *Douez v Facebook, Inc* (33 SCC) [61].
45 William McGeveran, "The Duty of Data Security" (2018) 103 *Minnesota Law Review* 1135, 1188–1199; Ido Kilovaty, "Psychological Data Breach Harms" (2021) 23 *North Carolina Journal of Law & Technology* 1, 66.
46 McGeveran, "The Duty of Data Security" (n 45) 1176–1179.
47 Solove and Citron, "Risk and Anxiety" (n 26) 739–741.
48 McGeveran, "The Duty of Data Security" (n 45) 1139–1140. See also Carol M Hayes, "Comparative Analysis of Data Breach Laws: Comprehension, Interpretation, and External Sources of Legislative Text" (2020) 23 *Lewis & Clark Law Review* 1221, 1262–1267.
49 See Eoin O'Dell, "Compensation for Non-Material Damage Pursuant to Article 82 GDPR" (cearta.ie, 6 March 2020) <https://perma.cc/8DK7-GRAB>.
50 See generally Rebecca Crootof, "The Internet of Torts: Expanding Civil Liability Standards to Address Corporate Remote Interference" (2019) 69 *Duke Law Journal* 583, 649–652 (discussing broadening relational duties for Internet of Things companies).
51 Ari Ezra Waldman, "Privacy Law's False Promise" (2020) 97 *Washington University Law Review* 773, 812.
52 Ibid 831.

53 Ryan Calo, "A Long-Standing Debate: Reflections on Risk and Anxiety: A Theory of Data Breach Harms by Daniel Solove and Danielle Keats Citron Response" (2017) 96 *Texas Law Review Online* 59, 61–62. See *In Re Horizon Healthcare Services Inc Data Breach Litig* (2017) 846 F 3d 625 (Court of Appeals, 3rd Circuit) 639; *Church v Accretive Health Inc* [2016] 11th Cir No. 15-15708, 654 Fed Appx 990, 994–995.
54 Carrillo and Jackson (n 23) 193–194; "Article 42 – Geral Da Proteção De Dados Pessoais (LGPD)" (n 23); "Arts. 33-34 – Ley de Proteccion de Datos Personales" (n 23); "Personal Data Protection Act 2012" (n 23) s 32(1). See also An Act to modernize legislative provisions as regards the protection of personal information (n 23) s 93.1; Privacy Act (n 23) s 1(1).
55 Zachary D. Clopton, "Redundant Public-Private Enforcement" (2016) 69 *Vanderbilt Law Review* 285, 318–320.
56 See *Jones v Tsige* [2012] ONCA 32.
57 Hayley Tsukayama, "Federal Preemption of State Privacy Law Hurts Everyone" (*Electronic Frontier Foundation*, 28 July 2022) <https://perma.cc/H89H-XT4A>; Jordan M Blanke, "The CCPA, 'Inferences Drawn,' and Federal Preemption" (2023) 29 *Richmond Journal of Law & Technology* 53.
58 Clopton, "Redundant Public-Private Enforcement" (n 55) 318–320.
59 *Google Inc v (1) Judith Vidal-Hall (2) Robert Hann (3) Marc Bradshaw* [2015] EWCA Civ 311 [51] [UK].
60 "Halfords E-Receipt Service a Delivery System for Marketing" (*Mind My Data*, 6 May 2018) <https://perma.cc/39P5-4PDF>.
61 Jane Yakowitz Bambauer, "The New Intrusion" (2012) 88 *Notre Dame Law Review* 205, 209–210, 238.
62 Citron, "Mainstreaming Privacy Torts" (n 34) 1809–1810.
63 *Campbell v. MGN*, [2004] 2 A.C. 457 paras 93–100 [UK]. See also *Murray v Express Newspapers* [2008] E.C.D.R. 12 paras 35–36 [UK]; *Australian Broadcasting Corp v Lenah Game Meats Pty* (2001) 185 ALR 1 paras 41–42 [Australia]; *Jones v Tsige*, 2012 ONCA 32 paras 70–73 [Canada].
64 See Chapter 6C.
65 See Jane Yakowitz Bambauer, Saura Masconale, and Simone Sepe, "Reckless Associations" (2022) *Harvard Journal of Law & Technology* 1, 4; Emily Laidlaw, "The Future of the Tort of Privacy" (2021) *The Canadian Bar Association National Magazine* <https://perma.cc/8SE8-65CZ>.
66 See *Jones v Tsige*, 2012 ONCA 32 [Canada] paras 65–73; *C v Holland*, [2012] 3 NZLR 672 (NZ) paras 94–97. See generally Kristen Thomasen, "Private Law & Public Space : The Canadian Privacy Torts in an Era of Personal Remote-Surveillance Technology" (2022) uOttawa Research Thesis 63–66 <https://perma.cc/2NRG-S9VV>.
67 See Chapter 6B.
68 Ari Ezra Waldman, "A Breach of Trust: Fighting Nonconsensual Pornography" (2017) 102 *Iowa Law Review* 709, 730–731; Alicia Solow-Niederman, "Beyond the Privacy Torts: Reinvigorating a Common Law Approach for Data Breaches" (2018) 127 *Yale Law Journal Forum* 614, 618–631; Richards and Solove, "Privacy's Other Path: Recovering the Law of Confidentiality" (n 31) 175–178.
69 Ari Ezra Waldman, *Privacy as Trust: Information Privacy for an Information Age* (Cambridge University Press 2018) 61–75. See also Richards and Solove, "Privacy's Other Path: Recovering the Law of Confidentiality" (n 31) 157–158.
70 Waldman, *Privacy as Trust* (n 69) 65–67.
71 *Lysko v. Braley* (2006), 79 O.R. (3d) 721 (C.A.), para 17.

72 *Lysko v. Braley* (2006), 79 O.R. (3d) 721 (C.A.), para 18.
73 Richards and Solove, "Privacy's Other Path: Recovering the Law of Confidentiality" (n 31) 133–145.
74 The Netherlands: See Art 6:106 of the Dutch Civ. Code. See *Rechtbank Overijssel* (n 24); *Rechtbank Amsterdam* (n. 39); *Rechtbank Noord-Nederland* (n 39).
Germany: See Spittka, "Germany: First Court Decision on Claims for Immaterial Damages under GDPR: Privacy Matters" (n 24).
Austria: "Innsbruck Higher Regional Crt. (Oberlandesgericht)" (*1 R 182/19b (AT)*, 2020) <https://perma.cc/5Y6T-7R5K> The Higher Regional Court of Innsbruck reversed based on the standard that should be applied. Portugal: Judgment of the Supreme Court of Justice of 3 November 2016, Proc. No. 323/12.6TVLSB,L2.S1 AND Supreme Court of Justice of 4 May 2010, Proc. No. 256/03.7TBPNH.C1.S1 <https://perma.cc/22YP-GW9N>.
75 *Lloyd v Google LLC*, *EWCA Civ 1599* [1]. See also Priv. & Elec. Commc'n Regs. 2003 SI 2003 No. 2426, art 22; Brendan Van Alsenoy, "Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation" (2016) 7 *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 271, 3; *Lloyd v Google* (UKSC 50) [1–2].
76 See Chapter 3A. See also *Meyers v Nicolet Restaurant of De Pere, LLC* (2016) 843 F 3d 724 (Court of Appeals, 7th Circuit) [725]. *Kirchein v Pet Supermarket, Inc* (2018) 297 F Supp 3d 1354 (Dist Court) [1356]. See Solove and Citron, "Risk and Anxiety" (n 26) 756–757.
77 Finn Myrstad and Øyvind H. Kaldestad, "Historic Victory for Privacy as Dating App Receives Gigantic Fine" (*Forbrukerrådet*, 26 January 2021) <https://perma.cc/77RN-XJGA>; "Norwegian DPA: Intention to Issue € 10 Million Fine to Grindr LLC" (*European Data Protection Board*, 26 January 2021) <https://perma.cc/DNQ4-3KKP>. See also Chapter 3.
78 Alex Hern, "Grindr Fined £8.6m in Norway over Sharing Personal Information" *The Guardian* (London, 26 January 2021) <https://perma.cc/9M8E-HCRU>.
79 See generally Sarah Moss, *Probabilistic Knowledge* (Oxford University Press 2018).
80 Byron Tau and Georgia Wells, "Grindr User Data Was Sold Through Ad Networks" (*Wall Street Journal*, 2 May 2022) <https://perma.cc/JF5K-5TZZ>.
81 Skadeserstatningsloven, para S3-6a.
82 Waldman, *Privacy as Trust* (n. 69) 67. See also Julia Belluz, "Grindr Is Revealing Its Users' HIV Status to Third-Party Companies" (*Vox*, 3 April 2018) <https://perma.cc/C54S-UTHH>.
83 See Chapter 2A.
84 Danielle Keats Citron, "A New Compact for Sexual Privacy" (2020) 62 *William & Mary Law Review* 1763, 1795; Danielle Keats Citron and Daniel J Solove, "Privacy Harms" (2022) 102 *Boston University Law Review* 793, 855. See also Jonathon W Penney, "Understanding Chilling Effects" (2021) 106 *Minnesota Law Review* 1451, 1510–1513.
85 Guido Calabresi, "Optimal Deterrence and Accidents" (1975) 84 *The Yale Law Journal* 656.
86 Steven Shavell, *Economic Analysis of Accident Law* (Harvard University Press 1987) 73–104.
87 Steven Shavell, "Strict Liability Versus Negligence" (1980) 9 *The Journal of Legal Studies* 1.
88 Steven Shavell, *Economic Analysis of Accident Law* (n 86) 73–104.
89 Richard A Epstein, "A Theory of Strict Liability" (1973) 2 *The Journal of Legal Studies* 151, 152.
90 Ibid.

91 Shavell, "Strict Liability Versus Negligence" (n 87) 19.
92 Solow-Niederman, "Beyond the Privacy Torts" (n 68) 630–631. See also Siva Vaidhyanathan, "Don't Delete Facebook. Do Something About It" *The New York Times* (New York, 8 June 2018) <https://perma.cc/K7BD-JKWJ>.
93 Chris Jay Hoofnagle, "Internalizing Identity Theft" (2009) 13 *UCLA Journal of Law and Technology* 1, 34–36.
94 Ibid 33.
95 Ibid.
96 Ibid 19–20.
97 Danielle Citron, "Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age" (2007) 80 *Southern California Law Review* 241, 248–249. See also Thomas Kadri, "Brokered Abuse" (2023) *Journal of Free Speech* 1, 2–4.
98 Hoofnagle, "Internalizing Identity Theft" (n 93) 33.
99 Kilovaty, "Psychological Data Breach Harms" (n 45) 44–45.
100 Dennis D Hirsch, "Protecting the Inner Environment: What Privacy Regulation Can Learn from Environmental Law" (2006) 41 *Georgia Law Review* 1, 37–40.
101 Solow-Niederman, "Beyond the Privacy Torts" (n 68).
102 Peter C. Ormerod, "A Private Enforcement Remedy for Information Misuse" (2019) 60 *Boston College Law Review* 1893, 1937; Mark A Geistfeld, "Protecting Confidential Information Entrusted to Others in Business Transactions: Data Breaches, Identity Theft, and Tort Liability" (2016) 66 *DePaul Law Review* 385, 404.
103 Solow-Niederman, "Beyond the Privacy Torts" (n 68) 630–631.
104 Calabresi, "Optimal Deterrence and Accidents" (n 85).
105 Ibid.
106 See civil law concept of "obligations of result."
107 Paul Ohm, "The Underwhelming Benefits of Big Data" (2012) 161 *University of Pennsylvania Law Review PENNumbra* 339.
108 Yafit Lev-Aretz, "Data Philanthropy" (2019) 70 *Hastings Law Journal* 1491, 1493.
109 Justin Hurwitz, "Cyberensuring Security" (2016) 49 *Connecticut Law Review* 1495, 1525.
110 Citron, "Reservoirs of Danger" (n 97) 264–265. See also Citron, "Mainstreaming Privacy Torts" (n 34) 1847.
111 Ormerod, "A Private Enforcement Remedy for Information Misuse" (n 102) 1937–1938.
112 *Rylands v Fletcher* (1868), LR 3 HL 330.
113 Citron, "Mainstreaming Privacy Torts" (n 34) 1844–46. But see *Del Giudice v Thompson*, 2021 ONSC 5379.
114 Solow-Niederman, "Beyond the Privacy Torts" (n 68) 629–630; Ormerod, "A Private Enforcement Remedy for Information Misuse" (n 102) 1937–1938.
115 Citron, "Reservoirs of Danger" (n 97) 266.
116 Tom Baker, "On the Genealogy of Moral Hazard" (1996) 75 *Texas Law Review* 237, 280.
117 *Imperial Oil v Quebec* (Minister of the Environment), 2003 SCC 58 paras 23–24.
118 Rebecca Crootof, "International Cybertorts: Expanding State Accountability in Cyberspace" (2018) 103 *Cornell Law Review* 565, 615.
119 Verstraete and Zarsky (n 29) 835–837; Solow-Niederman, "Beyond the Privacy Torts" (n 68) 630–631. See also Citron, "Reservoirs of Danger" (n 97) 261–268.
120 Hirsch, "Protecting the Inner Environment" (n 100) 23–30; A Michael Froomkin, "Regulating Mass Surveillance as Privacy Pollution: Learning from Environmental Impact Statements" (2015) 2015 *University of Illinois Law Review* 1713, 1717–1737, 1742–1745; Omri Ben-Shahar, "Data Pollution" (2019) 11 *Journal of Legal Analysis* 104, 110–118.
121 See Chapter 5B.

122 Ormerod, "A Private Enforcement Remedy for Information Misuse" (n 102) 1896.
123 John Hartshorne, "The Standard of Liability in Claims for Misuse of Private Information" (2021) 13 *Journal of Media Law* 211, 231.
124 Ibid 233.
125 See William L Prosser, *Handbook of the Law of Torts* (St. Pail: West Publishing Co, 1941) 810–817.
126 See *Womack v. Eldridge*, 210 S.E.2d 145, 147; *State Rubbish Collectors Ass'n v. Siliznoff*, 240 P.2d 282, 284 (Cal. 1952); *Russo v. White*, 400 S.E.2d 160, 163 (Va. 1991).
127 McGeveran, "The Duty of Data Security" (n 45) 1200–1204.
128 Jules L Coleman, *Risks and Wrongs* (Cambridge University Press 1992) 217–218.
129 Ibid.
130 See Chapter 2B.
131 Gregory C Keating, "Distributive and Corrective Justice in the Tort Law of Accidents" (2000) 74 *Southern California Law Review* 193, 202–203.
132 Citron, "Reservoirs of Danger" (n 97) 290.
133 Sandra Waddock, "Building a new institutional infrastructure for corporate responsibility" (2008) 22(3) Academy of Management Perspectives 87, 88.
134 Jutta Gurkmann, "Data Protection Violations by Meta and Co: ECJ Confirms Extensive Right of Consumer Organisations to Take Legal Action to Enforce GDPR" (*Verbraucherzentrale Bundesverband*, 28 April 2022) <https://perma.cc/54TG-GE4E>.
135 Marc Rotenberg and David Jacobs, "Enforcing Privacy Rights: Class Action Litigation and the Challenge of Cy Pres" in David Wright and Paul De Hert (eds), *Enforcing Privacy: Regulatory, Legal and Technological Approaches* (Springer International Publishing 2017) 307; Janet Walker, "Douez v Facebook and Privacy Class Actions" in Ignacio Cofone (ed), *Class Actions in Privacy Law* (Routledge 2020) 67–72 <https://perma.cc/W48V-GVNL>.
136 Johanna Chamberlain and Jane Reichel, "The Relationship between Damages and Administrative Fines in the EU General Data Protection Regulation Articles – Privacy Forum" (2020) 89 *Mississippi Law Journal* 667, 694–696.
137 Lauren Henry Scholz, "Private Rights of Action in Privacy Law" (2022) 63 *William & Mary Law Review* 1639, 1646–1648, 1655–1663; "A Private Right of Action Is Key to Ensuring That Consumers Have Their Own Avenue for Redress" (*New America*, 20 November 2019) <https://perma.cc/UTP6-453M>.
138 See Solove and Citron, "Risk and Anxiety" (n 26) 781–782.
139 Sanna Toropainen, "The Expanding Right to Damages in the Case Law of CJEU" (2019) Maastricht Faculty of Law Working Paper No. 2019-03 1 <https://perma.cc/X3SD-NQXL>; Janet Walker (n 134) 68–69. See also James Dempsey and others, "Breaking the Privacy Gridlock: A Broader Look at Remedies" 28–32 <https://perma.cc/KB72-H4BF>.
140 See Solove and Citron, "Risk and Anxiety" (n 26) 781–782.
141 See Chapter 5C.
142 See Ben-Shahar, "Data Pollution" (n 120) 105.
143 Chris Jay Hoofnagle and Jan Whittington, "Free: Accounting for the Costs of the Internet's Most Popular Price" (2014) 61 *UCLA Law Review* 606, 651–657; Joseph Turow and others, "The Federal Trade Commission and Consumer Privacy in the Coming Decade 2007 Privacy Year in Review" (2007) 3 *I/S: A Journal of Law and Policy for the Information Society* 723, 746–747.
144 Ben-Shahar, "Data Pollution" (n 120) 104–108.
145 Kai Hüschelrath and Sebastian Peyer, "Public and Private Enforcement of Competition Law: A Differentiated Approach" (2013) 36 *World Competition* 585, 586–588, 591–592.

146 See Chapter 1B.
147 Dempsey and others, "Breaking the Privacy Gridlock" (n 138) 30.
148 See Motor Vehicles and Traffic Act, GA. Code Ann. s 40-8-20 (West 1982); 17 N.Y. Veh & Traf Law s 375(2)(a) (McKinney 2021); 46 Wash. Rev. Code Ann. s 46.37.040 (West 1977).
149 Michael S Greve, "Private Enforcement of Environmental Law" (1990) 65 *Tulane Law Review* 339, 340.
150 Dempsey and others, "Breaking the Privacy Gridlock" (n 139) 23–25.
151 See Chapter 6C.
152 *Davis v. Facebook* (n 30).
153 See *Wilkinson v Downton* (1897) 2 QB 57 [UK]; *Bourhill v Young* (1943) AC 92 [UK]; *Andrews v. Grand & Toy Alberta Ltd.*, [1978] 2 S.C.R. 229 (SCC) [Canada]; *Thornton v. School District No. 57 (Prince George) et al.*, [1978] 2 S.C.R. 267 (SCC) [Canada]; *Arnold v. Teno*, [1978] 2 S.C.R. 287 (SCC) [Canada].
154 Rachael Mulheron, "Rewriting the Requirement for a 'Recognized Psychiatric Injury' in Negligence Claims" (2012) 32 *Oxford Journal of Legal Studies* 77, 96–100; See *Saadati v Moorhead* (2017) 28 SCC [2] [Canada]; *Mustapha v Culligan of Canada Ltd* (2008) 27 SCC [8–10] [Canada]; *McLoughlin v O'Brian* (1983) 1 AC 410, 441–442.
155 Eli A Meltz, "No Harm, No Foul: Attempted Invasion of Privacy and the Tort of Intrusion upon Seclusion" (2015) 83 *Fordham Law Review* 3431, 3465–3466. See also Daniel Townsend, "Who Should Define Injuries for Article III Standing" (2015) 68 *Stanford Law Review Online* 76, 80–81.
156 See Chapter 6B.
157 McGeveran, "The Duty of Data Security" (n 45) 1179.
158 See *Augustus v Gosset* [1996] 3 SCR 268 [Canada] (providing an overview).
159 *Saadati v Moorhead* (n 154) 6.
160 Ryan Calo, "Privacy Harm Exceptionalism" (2014) 12 *Colorado Technology Law Journal* 361, 363.
161 Sasha Romanosky, David Hoffman, and Alessandro Acquisti, "Empirical Analysis of Data Breach Litigation" (2014) 11 *Journal of Empirical Legal Studies* 74, 9. See also McGeveran, "The Duty of Data Security" (n 45) 1143–1158. Felix T Wu, "Defining Privacy and Utility in Data Sets" (2013) 84 *University of Colorado Law Review* 1117, 1161; George Ashenmacher, "Indignity: Redefining the Harm Caused by Data Breaches" (2016) 51 *Wake Forest Law Review* 1, 6.
162 Bart van der Sloot, "Where Is the Harm in a Privacy Violation" (2017) 8 *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 322, 329, 337.
163 Ibid 338–339.
164 Ormerod, "A Private Enforcement Remedy for Information Misuse" (n 102) 1939–1940.
165 *Jones v. Tsige* (n 56) para 7.
166 See *Federal Election Comm'n v Akins* [1998] No 96-1590.
167 Felix T Wu, "How Privacy Distorted Standing Law" (2016) 66 *DePaul Law Review* 439, 444–447.
168 Ignacio Cofone, "Privacy Standing" (2022) *University of Illinois Law Review* 1367, 1407–1411.
169 Susan Bandes, "The Idea of a Case" (1990) 42 *Stanford Law Review* 227, 285.
170 Israel Gilead, "Tort Law and Internalization: The Gap between Private Loss and Social Cost" (1997) 17 *International Review of Law and Economics* 589, 597–600.
171 Jonathan Siegel, "Chilling Injuries as a Basis for Standing" (1989) 98 *Yale Law Journal* 905, 915.

172 Rachel Bayefsky, "Psychological Harm and Constitutional Standing" (2015) 81 *Brooklyn Law Review* 1555, 1570–1571; Jonathan H Adler, "Stand or Deliver: Citizen Suits, Standing, and Environmental Protection" (2001) 12 *Duke Environmental Law & Policy Forum* 39, 55–57.
173 *In Sierra Club v Morton* [1972] 405 US 727, 734.
174 *Friends of Earth, Inc v Laidlaw Environmental Services* (TOC), Inc [2000] Supreme Court 528 US, 528 US 167 181–184.
175 *Volkswagen Group Canada Inc v Association québécoise de lutte contre la pollution atmosphérique* (SCC 53); Camille Cameron and Riley Weyman, "Class Actions and Climate Change Loss and Damage Litigation" [2021] *Research Handbook on Climate Change Law and Loss & Damage* 410, 431.
176 Jack M Balkin, "Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation" (2018) 51 *U.C. Davis Law Review* 1149, 1167–1168; Jack Balkin, "2016 Sidley Austin Distinguished Lecture on Big Data Law and Policy: The Three Laws of Robotics in the Age of Big Data" (2017) 78 *Ohio State Law Journal* 1217, 1234–1235.
177 Ben-Shahar, "Data Pollution" (n 120) 105; Ignacio Cofone, "Beyond Data Ownership" (2021) 43 *Cardozo Law Review* 501, 515–516.
178 See Susan Bandes, "The Idea of a Case" (n 169) 273; Katherine Strandburg, "Monitoring, Datafication, and Consent: Legal Approaches to Privacy in the Big Data Context" in Julia Lane and others (eds), *Privacy, Big Data and the Public Good: Frameworks for Engagement* (Cambridge University Press 2014) 24; Dennis D Hirsch, "Is Privacy Regulation the Environmental Law of the Information Age?" in Katherine J. Strandburg and Daniela Stan Raicu (eds), *Privacy and Technologies of Identity: A Cross-Disciplinary Conversation* (Springer US 2006) 243–246.
179 Solove and Citron, "Risk and Anxiety" (n 26) 785.
180 Pierre Schlag, "Rules and Standards" (1985) 33 *UCLA Law Review* 379.
181 McGeveran, "The Duty of Data Security" (n 45) 1179.
182 Richard B Stewart and Cass R. Sunstein, "Public Programs and Private Rights" (1982) 95 *Harvard Law Review* 1193, 1214.
183 Calli Schroeder, "Intangible Privacy Harms Post-Spokeo" (*International Association of Privacy Professionals*, 15 December 2016) <https://perma.cc/8PD7-LH68>; Peter C Ormerod, "Privacy Injuries and Article III Concreteness" (2020) 48 *Florida State University Law Review* 133. See also 15 U.S.C. s 1681n(a)(1)(A).
184 See ECLI:NL:RBROT:2021:6822, Rechtbank Rotterdam, ROT 20/3286 [2021] Rb Rotterdam ECLI:NL:RBROT:2021:6822.
185 Wayne Unger, "Reclaiming Our Right to Privacy by Holding Tech. Companies Accountable" (2020) 27 *Richmond Journal of Law & Technology* 1, 16–21.
186 Michael A Eizenga and Emrys Davis, "A History of Class Actions: Modern Lessons from Deep Roots" (2011) 7 *Canadian Class Action Review* 3, 22.
187 Brian Fitzpatrick, "An Empirical Study of Class Action Settlements and Their Fee Awards" (2010) 7 *Journal of Empirical Legal Studies* 811, 837; Tyler Hill, "Financing the Class: Strengthening the Class Action through Third-Party Investment" (2015) 125 *Yale Law Journal* 484, 487.
188 *Schrems v Facebook Ireland, 6Ob91/19d* [49]. See also Eoin O'Dell (n 49).
189 *Davis v. Facebook* (n 30) 598–600.
190 Solove and Hartzog, Breached! (n 1) 59.
191 Ibid 55–56.
192 *Karasik v Yahoo! Inc*, ONSC 1063 [137].

193 *Transunion LLC v. Ramirez* (n 13) 2206–2214.
194 Daniel J Solove and Danielle Keats Citron, "Standing and Privacy Harms: A Critique of Transunion v. Ramirez" (2021) 101 *Boston University Law Review Online* 62, 69.
195 *Transunion LLC v. Ramirez* (n 13) 2206–2214.
196 "Equifax Data Breach Settlement" (n 5).
197 *Lloyd v. Google* (n 75) para 92.
198 *Transunion LLC v. Ramirez* (n 13) paras 2218–2219 (Thomas, J., dissenting).
199 Tau and Wells, "Grindr User Data Was Sold Through Ad Networks" (n 80).
200 Elizabeth J Cabraser and Samuel Issacharoff, "The Participatory Class Action Conference" (2017) 92 *New York University Law Review* 846, 846.
201 See Chapters 3A and 4B.
202 Samuel Issacharoff and Florencia Marotta-Wurgler, "The Hollowed Out Common Law" (2020) 67 *UCLA Law Review* 600, 634–635.
203 D Theodore Rave, "When Peace Is Not the Goal of a Class Action Settlement" (2016) 50 *Georgia Law Review* 475, 503–504. See *Loewenthal v Sirius XM Holdings, Inc et al* [2021] ONSC 8220 [Canada].
204 Christopher R Leslie, "De Facto Detrebling: The Rush to Settlement in Antitrust Class Action Litigation" (2008) 50 *Arizona Law Review* 1009, 1017–1018; Bruce L Hay, "Asymmetric Rewards: Why Class Actions (May) Settle for Too Little Essay" (1996) 48 *Hastings Law Journal* 479, 506.
205 Rave, "When Peace Is Not the Goal of a Class Action Settlement" (n 203) 504.
206 *GDPR*, *Art 80*. See also Brazilian LGPD arts 22 and 42.
207 Truli, "The General Data Protection Regulation and Civil Liability" (n 18).
208 "Reference for a Preliminary Ruling – Regulation (EU) 2016/679 – C319/20" (*Curia*, 28 April 2022) <https://perma.cc/2HP2-XSNW>.
209 Orla Lynskey, "General Report Topic 2: The New EU Data Protection Regime" in Jorrit J. Rijpma (ed), *The New Data Protection Regime: Setting Global Standards for The Right to Personal Data Protection*, vol 2 (Eleven International Publishing 2020) 70–71 <https://perma.cc/YS6K-WCQ9>. See also "Our Detailed Concept" (*noyb*) <https://perma.cc/Z4XD-4JA4>; Code de la consummation, Articles L. 623-1, 623-2. 623-3, L. 811–1.
210 Council Directive 2020/1828/EC of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC 2020 [2020] OJ L409/1, online: <https://perma.cc/MKL5-WDFU>.
211 Janet Walker, "Who's Afraid of U.S.-Style Class Actions" (2011) 18 *Southwestern Journal of International Law* 509, 518; Eizenga and Davis, "A History of Class Actions: Modern Lessons from Deep Roots" (n 186) 22.
212 See Gene R Nichol, "The Roberts Court and Access to Justice" (2009) 59 *Case Western Reserve Law Review* 821, 827–834; Gene R Nichol, "Judicial Abdication and Equal Access to the Civil Justice System" (2010) 60 *Case Western Reserve Law Review* 325, 325–326.

CONCLUSION

1 Julie E Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (Oxford University Press 2019) 25–47; Carissa Véliz, *Privacy Is Power: Why and How You Should Take Back Control of Your Data* (Bantam Press 2021) 50–82; Daniel Solove, "Privacy and Power: Computer Databases and Metaphors for Information Privacy" (2001) 53 *Stanford Law Review* 1393, 1413–1430; Lisa M. Austin, "Enough About

Me: Why Privacy Is about Power, Not Consent (or Harm)" in Austin Sarat (ed), *A World Without Privacy?: What Can/Should Law Do* (2014) 134 <https://perma.cc/EPK4-HCRJ>; Orla Lynskey, "Grappling with 'Data Power': Normative Nudges from Data Protection and Privacy" (2019) 20 *Theoretical Inquiries in Law* 189, 192.

2 Anita L. Allen, *Why Privacy Isn't Everything: Feminist Reflections on Personal Accountability* (Rowman & Littlefield Publishers 2003) 26.

3 Omri Ben-Shahar and Lior Jacob Strahilevitz, "Contracting over Privacy: Introduction" (2016) 45 *The Journal of Legal Studies* S1, 8.

4 Daniel J. Solove and Woodrow Hartzog, *Breached!* (Oxford University Press 2022) 98–99; Thomas Kadri, "Brokered Abuse" (2023) *Journal of Free Speech* 1.

5 Shoshana Zuboff, *The Age of Surveillance Capitalism* (1st ed., PublicAffairs 2019) 338–345.

6 Woodrow Hartzog, "The Case against Idealising Control" (2018) 4 *European Data Protection Law Review* 423; Iris van Ooijen and Helena U. Vrabec, "Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective" (2019) 42 *Journal of Consumer Policy* 91.

7 Mark Zuckerberg, "Moving Fast and Breaking Things" (*Business Insider*, 14 October 2010) <https://perma.cc/522W-RE9C>; Steven Levy, "Mark Zuckerberg on Facebook's Future, From Virtual Reality to Anonymity" (*Wired*, 30 April 2014) <https://perma.cc/2EXG-ALQP>. See also Jonathan Taplin, *Move Fast and Break Things: How Facebook, Google, and Amazon Cornered Culture and Undermined Democracy* (Little, Brown and Company 2017).

8 "Form S-1 Registration Statement under The Securities Act of 1933: Facebook, Inc." (*US Securities and Exchange Commission*, 2012) 67 <https://perma.cc/VV9D-J35S>.

9 Allen Wood, "Exploitation" in Ted Honderich (ed), *The Oxford Companion to Philosophy* (2nd ed., Oxford University Press) 283–284; Matt Zwolinski, "Exploitation and Consent" in Peter Schaber and Andreas Müller (eds), *The Routledge Handbook of the Ethics of Consent* (1st ed., Routledge 2018) 154. See also Allen W. Wood, "Exploitation*" (1995) 12 *Social Philosophy and Policy* 136, 147 ("To exploit someone or something is to make use of him, her, or it for your own ends by playing on some weakness or vulnerability in the object of your exploitation").

10 Wood, "Exploitation" (n 9).

11 Shoshana Zuboff, *Age of Surveillance Capitalism* (n 5) 74–82. See also Cohen, *Between Truth and Power* (n 1) 42.

12 Nicholas Vrousalis, "How Exploiters Dominate" (2021) 79 *Review of Social Economy* 103, 110; Nicholas Vrousalis, "Exploitation: A Primer" (2018) 13 *Philosophy Compass* e12486, 10.

13 Nikita Aggarwal, "The Norms of Algorithmic Credit Scoring" (2021) 80 *The Cambridge Law Journal* 42, 45–47; Muhammad Ali and others, "Discrimination through Optimization: How Facebook's Ad Delivery Can Lead to Biased Outcomes" (2019) 3 *Proceedings of the ACM on Human-Computer Interaction* 199:1; Pauline Kim and Sharion Scott, "Discrimination in Online Employment Recruiting" (2019) 63 *St. Louis University Law Journal* 93, 115–118.

14 Gary Anthes, "Data Brokers Are Watching You" (2015) 58 *Communications of the ACM* 28; Theodore Rostow, "What Happens When an Acquaintance Buys Your Data: A New Privacy Harm in the Age of Data Brokers" (2017) 34 *Yale Journal on Regulation Note* 667.

15 Cohen, *Between Truth and Power* (n 1) 154–167.

16 Ari Ezra Waldman, "Outsourcing Privacy" (2020) 96 *Notre Dame Law Review Reflection* 194, 195; Ari Ezra Waldman, "Privacy, Practice, and Performance" (2022) 110 *California Law Review* 1221.

17 Ari Ezra Waldman, *Industry Unbound: The Inside Story of Privacy, Data, and Corporate Power* (Cambridge University Press 2021) 99–160; W. Gregory Voss and Hugues Bouthinon-Dumas, "EU General Data Protection Regulation Sanctions in Theory and in Practice" (2020) 37 *Santa Clara High Technology Law Journal* 1, 74–76.
18 Cohen, *Between Truth and Power* (n 1) 154–164.
19 See Julie E Cohen, "How (Not) to Write a Privacy Law" (*Knight First Amendment Institute at Columbia University*, 23 March 2021) <https://perma.cc/2TTH-8BK5>; Ari Ezra Waldman, "Privacy's Rights Trap" (2022) 117 *Northwestern University Law Review* 88; Daniel J Solove, 'The Limitations of Privacy Rights' (2023) 98 *Notre Dame Law Review* 975.
20 Neil Richards and Woodrow Hartzog, "The Pathologies of Digital Consent" (2018) 96 *Washington University Law Review* 1461; Daniel J Solove, 'Introduction: Privacy Self-Management and the Consent Dilemma' (2012) 126 *Harvard Law Review* 1880.
21 Cohen, *Between Truth and Power* (n 1) 155–156.
22 See François-Philippe Champagne, Bill C-27, An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts 2022 [Canada].
23 Derek Thompson, "Google's CEO: 'The Laws Are Written by Lobbyists'" (*The Atlantic*, 1 October 2010) <https://perma.cc/Y97S-LYUS>. See *also* YouTube, "Eric Schmidt: The Laws Are Written by Lobbyists" (*The Atlantic*, 28 March 2018) <https://perma.cc/XW63-Z4ME>.
24 "Client Profile: Amazon.Com" (*OpenSecrets*, 2022) <https://perma.cc/NZ4M-HYVD>; "The Amazon Lobbyists Who Kill U.S. Consumer Privacy Protections" (*Reuters*, 19 November 2021) <https://perma.cc/R2TK-8FB8>.
25 Karl Evers-Hillstrom, "Amazon, Meta Report Record Lobbying Spending in 2021" (*The Hill*, 21 January 2022) <https://perma.cc/M3JS-K6MK>; Isobel Asher Hamilton, "Amazon and Meta Each Spent Record Amounts Lobbying Washington Lawmakers in 2021, Report Says" (*Business Insider*, 24 January 2022) <https://perma.cc/3JDJ-EGW7>.
26 Max Bank and others, "The Lobby Network: Big Tech's Web of Influence in the EU" (*Corporate Europe Observatory and LobbyControl e.V.*, August 2021) 10 <https://perma.cc/5J4C-63VB>; Natasha Lomas, "US Giants Top Tech Industry's $100M+ a Year Lobbying Blitz in EU" (*TechCrunch*, 31 August 2021) <https://perma.cc/DP67-YLYA>.
27 Gordon Hull, "Successful Failure: What Foucault Can Teach Us about Privacy Self-Management in a World of Facebook and Big Data" (2015) 17 *Ethics and Information Technology* 89, 96.
28 Ibid 97.
29 See "Press Release, Merkel: Regulate Ownership of Data" (*Bundesregierung*, 18 March 2017) <https://perma.cc/A8M7-QBK4>; Andrew Yang, "Regulating Technology Firms in the 21st Century" (*Yang2020 – Andrew Yang for President*, 14 November 2019) <https://perma.cc/T57L-VHSP>; "Digital Privacy Rights Require Data Ownership" *Financial Times* (21 March 2018) <https://perma.cc/8E8C-XJRT>; Will.I.Am, "We Need to Own Our Data as a Human Right—And Be Compensated for It" *The Economist* (21 January 2019) <https://perma.cc/7AGH-CXWD>; Dan Demers, "From Complexity To Control: It's Time To Own Your Data" *Forbes* (27 February 2020) <https://perma.cc/PB36-P8Q2>; Matt Stevens, "Andrew Yang's Next Move: A New Nonprofit Organization" *New York Times* (New York, 5 March 2020) <https://perma.cc/H7W3-LJDS>; Jill Cowan, "How Much Is Your Data Worth?" *New York Times* (New York, 25 March 2019) <https://perma.cc/YX8E-T788>.

30 See "Europe Agrees New Law to Curb Big Tech Dominance" *BBC News* (London, 25 March 2022) <https://perma.cc/PT7N-QFBP>; "Remarks of President Joe Biden – State of the Union Address as Prepared for Delivery" (*The White House*, 7 February 2023) <https://perma.cc/49H6-RVYY>.
31 See *eBay Canada Ltd v Mofo Moko* [2018] QCCA 1735 [18–20].
32 See Gregory Day and Abbey Stemler, "Infracompetitive Privacy" (2019) 105 *Iowa Law Review* 61; Tom Wheeler, "Big Tech Giving European Consumers What They Deny Americans" (*Brookings*, 28 December 2022) <https://perma.cc/P3UF-M7MG>.
33 Vida Panitch, "Exploitation" in C. M. Melenovsky (ed), *The Routledge Handbook of Philosophy, Politics, and Economics* (1st ed., Routledge 2022) 217.
34 See generally Ruth J. Sample, *Exploitation: What It Is and Why It's Wrong* (Rowman & Littlefield Publishers 2003).
35 Chris Meyers, "Wrongful Beneficence: Exploitation and Third World Sweatshops" (2004) 35 *Journal of Social Philosophy* 319, 324.
36 Alan Wertheimer, *Exploitation* (Princeton University Press 1996) 253–259.
37 Ibid 258–264.
38 Ibid 251–253.
39 Jonathan Zittrain, "How to Fix Twitter and Facebook" *The Atlantic* (9 June 2022) <https://perma.cc/FYE3-XPVP>; Franklin Foer, "Facebook's War on Free Will" *The Guardian* (London, 19 September 2017) <https://perma.cc/7AGG-9XA9>.
40 See Nofar Sheffi, "We Accept: The Constitution of Airbnb" (2020) 11 *Transnational Legal Theory* 484; Kristen E. Eichensehr, "Digital Switzerlands" (2019) 167 *University of Pennsylvania Law Review* 665; Kate Klonick, "The New Governors: The People, Rules, and Processes Governing Online Speech" (2018) 131 *Harvard Law Review* 1598, 1663.
41 Vili Lehdonvirta, *Cloud Empires: How Digital Platforms Are Overtaking the State and How We Can Regain Control* (The MIT Press 2022) 3.
42 Lynskey, "Grappling with 'Data Power'" (n 1) 201.
43 Robert M Bond and others, "A 61-Million-Person Experiment in Social Influence and Political Mobilization" (2012) 489 *Nature* 295. See also Cohen, *Between Truth and Power* (n 1) 96; Shoshana Zuboff, *Age of Surveillance Capitalism* (n 5) 299–309.
44 Kate Klonick, "Inside the Making of Facebook's Supreme Court" (*New Yorker*, 12 February 2021) <https://perma.cc/AY3R-U3TG>.
45 Lehdonvirta, *Cloud Empires* (n 41) 210–214.
46 Joey Roulette, "SpaceX Curbed Ukraine's Use of Starlink Internet for Drones - Company President" (*Reuters*, 9 February 2023) <https://perma.cc/2TAQ-Z7FC>; Reuters, "SpaceX Should Choose between Ukraine and Russia – Ukrainian Official" (*Reuters*, 9 February 2023) <https://perma.cc/D3XT-J2YG>.
47 Lehdonvirta, *Cloud Empires* (n 41) 199–203.
48 Shoshana Zuboff, *Age of Surveillance Capitalism* (n 5) 351–375; Lynskey, "Grappling with 'Data Power'" (n 1) 196–197.
49 See *Fair Housing Council Of San Fernando Valley v Roommates.com, LLC* (2008) 521 F 3d 1157 (Court of Appeals, 9th Circuit) 1162, 1169. "Meta Settles Cambridge Analytica Scandal Case for $725m" *BBC News*, (London, 23 December 2022) <https://perma.cc/Z6TQ-GTSZ>.
50 See Jack Balkin, "Information Fiduciaries and the First Amendment" (2016) 49 *U.C. Davis Law Review* 1183; Woodrow Hartzog, *Privacy's Blueprint: The Battle to Control the Design of New Technologies* (Harvard University Press 2018); Ari Ezra Waldman, *Privacy as Trust: Information Privacy for an Information Age* (Cambridge University Press 2018); Neil Richards, *Why Privacy Matters* (Oxford University Press 2021); Danielle Keats

Citron, *The Fight for Privacy: Protecting Dignity, Identity, and Love in the Digital Age* (WW Norton 2022).

51 United States Department of Health Education and Welfare, "Records, Computers and the Rights of Citizens" (MIT Press 1973) <https://perma.cc/67N5-TFJC>; Robert Pitofsky and others, "Privacy Online: A Report to Congress" (1998) *Federal Trade Commission* 64, 41.

52 GDPR Art 5; "Accountability" (*European Data Protection Supervisor*) <https://perma.cc/NS9Q-MA5N>; GDPR art. 5(2).

53 "PIPEDA Fair Information Principles" (*Office of the Privacy Commissioner of Canada*, 16 September 2011) <https://perma.cc/QNE9-W47T>.

54 Rostow, "What Happens When an Acquaintance Buys Your Data" (n 14) 699–700; Sarah Spiekermann, "The Challenges of Privacy by Design" (2012) 55 Communications of the ACM 38.

55 Daniel M Filler, David M Haendler, and Jordan L. Fischer, "Negligence at the Breach: Information Fiduciaries and the Duty to Care for Data" (2022) 54 *Connecticut Law Review* 105, 134. See also Lina M Khan and David E Pozen, "A Skeptical View of Information Fiduciaries" (2019) 133 *Harvard Law Review* 497, 511–517.

56 Ari Waldman, "Data Protection by Design? A Critique of Article 25 of the GDPR" (2020) 53 *Cornell International Law Journal* 147, 154, 165–166; Khan and Pozen, "A Skeptical View of Information Fiduciaries" (n 55) 503–504.

57 Omri Ben-Shahar, "Data Pollution" (2019) 11 *Journal of Legal Analysis* 104, 104–108.

58 Jennifer Cobbe and Jatinder Singh, "Data Protection Doesn't Work: Oversight Failure in Data Processing Figurations," *Privacy Law Scholars Conference* (2022). See "Final One Stop Shop Decisions" (*European Data Protection Board*) <https://perma.cc/7SED-453W>.

59 Jennifer Cobbe and Jatinder Singh, "Data Protection Doesn't Work" (n. 58).

60 See Yafit Lev-Aretz and Katherine J Strandburg, "Privacy Regulation and Innovation Policy" (2020) 22 *Yale Journal of Law and Technology* 256.

61 Jack M Balkin, "The Fiduciary Model of Privacy" (2020) 134 *Harvard Law Review Forum* 11, 23.

Index