"How did privacy policies become licenses to spy? And do we have any hope of effective data regulation? In vivid and accessible prose, *Industry Unbound* offers deep insight into contemporary corporate power to monitor workers, manipulate consumers, and influence governments. With a skilled attorney's understanding of contracts and statutes and a rigorous sociologist's command of empirical methods, Waldman tells a story of 'privacy professionals' who gradually accommodate themselves to surveillance capitalism. This brilliant book is a must-read for understanding the failures of contemporary privacy laws, and how they might evolve toward more robust protections."

Frank Pasquale, Professor of Law, Brooklyn Law School, and author of *The Black Box Society* and *The New Laws of Robotics*

"Ari Waldman peels back the curtain on internal privacy practices at the most powerful tech companies to reveal an alarming trend: Despite robust privacy programs, teams of employees devoted to protecting privacy, and significant laws and regulations requiring many internal measures to safeguard privacy, the reality on the ground is that these things are often failing. Waldman provocatively contends that corporate power turns compliance with even robust privacy laws into an often hollow exercise. As legislatures rush to pass privacy laws, *Industry Unbound* is a wakeup call that these efforts will not end the nightmare. This eye-opening and unsettling book is also constructive, as it offers productive recommendations for a new direction in privacy law. Lively, alarming, and insightful, *Industry Unbound* deftly unites theory, practice, and law. It is essential reading for anyone who cares about the future of privacy."

Daniel J. Solove, John Marshall Harlan Research Professor of Law, George Washington University, and author of *Understanding Privacy*

"Ari Waldman's powerful new book combines fascinating on-the-ground insights and a sharp critical eye to help us understand why, despite touted improvements in data protection, our privacy remains in jeopardy. *Industry Unbound* is clear, compelling, and essential reading for the personal data field and anyone who is concerned about privacy."

Woodrow Hartzog, Professor of Law and Computer Science, Northeastern University, and author of *Privacy's Blueprint*

Industry Unbound

In *Industry Unbound*, Ari Ezra Waldman exposes precisely how the tech industry conducts its ongoing crusade to undermine our privacy. With research based on interviews with scores of tech employees and internal documents outlining corporate strategies, Waldman reveals that companies don't just lobby against privacy law; they also manipulate how we think about privacy, how their employees approach their work, and how we use their data-extractive products. In contrast to those who claim that privacy law is getting stronger, Waldman shows why recent shifts in privacy law are precisely the kinds of changes that corporations want and how even those who think of themselves as privacy advocates often unwittingly facilitate corporate malfeasance. This powerful account should be read by anyone who wants to understand why privacy laws are not working and how corporations trap us into giving up our personal information.

Ari Ezra Waldman is Professor of Law and Computer Science at Northeastern University School of Law and Khoury College of Computer Sciences. A graduate of Harvard Law School and Harvard College, he also earned his PhD in sociology at Columbia University. He is a widely published and award-winning scholar and teacher focusing on the ways law and technology entrench traditional hierarchies of power.

Industry Unbound

The Inside Story of Privacy, Data, and Corporate Power

Ari Ezra Waldman
Northeastern University

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE
UNIVERSITY PRESS

University Printing House, Cambridge CB2 8BS, 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

79 Anson Road, #06–04/06, Singapore 079906

Cambridge University Press is part of the University of Cambridge.

It furthers the University's mission by disseminating knowledge in the pursuit of education, learning, and research at the highest international levels of excellence.

www.cambridge.org
Information on this title: www.cambridge.org/9781108492423
DOI: 10.1017/9781108591386

First published 2021

Printed in the United Kingdom by TJ Books Limited, Padstow Cornwall

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

ISBN 978-1-108-49242-3 Hardback

For GWL

CONTENTS

ONE BOOK IN ONE PAGE

This is a story about people, privacy, and power. It is based on nearly four years of interviews, surveys, field observations, and reviews of both public and confidential internal documents. Its central argument is simple: antiprivacy work is routinized throughout the information industry. The implications of this are profound: even those frontline workers who consider themselves privacy advocates are so steeped in antiprivacy discourses and so constrained by antiprivacy organizational structures that their work ends up serving corporate surveillant interests in the end.

To routinize surveillance, executives in the information industry use the weapons of coercive bureaucracies to control privacy discourse, law, and design. This works in two ways: it inculcates antiprivacy norms and practices from above and amplifies antiprivacy norms and practices from within. Tech companies inculcate corporate-friendly definitions of privacy. They undermine privacy law by recasting the laws' requirements to suit their interests. And they constrain what designers can do, making it difficult for privacy to make inroads in design. As this happens, corporate-friendly discourses and practices become normalized as ordinary and commonsense among information industry employees. This creates a system of power that is perpetuated by armies of workers who may earnestly think they're doing some good but remain blind to the ways their work serves surveillant ends.

This strategy facilitates data extraction while undermining individual, social, institutional, and legal resistance to corporate power. It can persist without buy-in from engineers and privacy professionals; it can persist even as they think they're doing their best. The results are bleak. The edifice of privacy law becomes little more than a house of cards. Resistance is necessary.

PREFACE

I get emails. Some of them are from corporations in the information industry. In the span of three months in 2018 (March through May), fifty-seven companies sent me fifty-nine different emails, almost all of which started with at least one of these statements:

We care about your privacy.
Your privacy is important to us.
We take your data privacy seriously.

Sometimes, they took my privacy "very" seriously. A few even said that my privacy was "very important" to them. One said, *Your privacy. We care.*

The flood of emails was anticipating the May 25 effective date of the European Union's new data protection law, and almost every company that had, at some point, collected data about me was making some changes to its privacy policy. But with each email, I rolled my eyes. The information industry – the ecosystem of for-profit companies that collect and derive some value from our data – has been playing fast and loose with our privacy for decades. So we can be excused a little incredulity when technology companies say they care about our privacy. Snapchat lied about the privacy features of its not-so-ephemeral ephemeral messaging service. Pokemon Go forced its users to disclose information it didn't need. Zoom's default settings gave third parties access to user information. Femtech apps extract data from their users without their knowledge. Uber designed its app so it could follow smartphone users even after they deleted the Uber app. In-home assistants like Amazon's Alexa listen when they're not supposed to. Google G-Suite is so invasive that the company had to be sued to stop it from stealing data from university

students. I could go on. No wonder studies show that few people would associate the words *very*, *important*, *seriously*, and *care* with tech companies' approach to our privacy.[1]

Why say you "care about" my privacy when you've been selling my data to third parties? Why say my privacy is "important" to you when your privacy policy allows you to do pretty much anything with almost any data you've collected about me? Why say you take my privacy "very seriously" when your data-for-profit business model shows that you don't?

And yet, these companies have been using those words for decades: in the press, in their privacy policies, in their statements before Congress, in legal arguments in front of judges, and in emails to their customers. The language persists even though many people think it's more halfhearted PR than anything else.

I read on. Thirty-three of the emails I received continued with some version of this:

At [insert company name here], *you are in control.*

Another nineteen told me how:

We want to give you the information you need so you can make the choices that are right for you.

Four sentences into a spammy email and I had the beginnings of an idea for this book. These companies and I are thinking about the words *care* and *privacy* in very different ways (and, for that matter, probably the words *very* and *important*). By *care*, they mean giving me control; by *privacy*, they mean giving me choices.

"We care deeply about privacy here," said a privacy leader at an invitation-only presentation about his company's recent technical work in artificial intelligence. When I asked him how a particular artificial intelligence (AI) product reflected the company's commitment to privacy, he said, "We are transparent about the information we collect and use to build these tools to make your life easier and help researchers do their job." A colleague of his in the audience added, "When we say we care about your privacy, we really mean that up and down the line. We're constantly thinking about ways of putting you in control of what information you want to share and what you don't, what tools you want and which you don't."[2]

I then asked an acquaintance who worked for Facebook at the time. Here's an excerpt of the exchange:

"Does Mark Zuckerberg really care about my privacy?" I asked.
He responded: "It's my job, and the jobs of a lot of hardworking people here, to make sure he cares about your privacy and to make sure we, as a company, do right by you and your privacy."
"Can you tell me what you mean by 'do right by you and your privacy' and what you do in your job to achieve that goal?"
"If you take a look at the privacy settings on Facebook, you see how much we've done to put you in control of what happens, both in what you see on Facebook and what happens to your information. We've closed those loopholes where your information is used without you knowing. Just last week, we," by which he meant privacy lawyers, "sat as a team to figure out what we could do better in a few specific areas, like with third-party apps and how we can stop the next Cambridge Analytica with better privacy protections."

He was referring to the scandal in which Facebook allowed a data analytics company working with a Republican presidential campaign to collect and analyze the personal information of more than 87 million users without them knowing, resulting in advertisements that suppressed votes, amplified scare tactics, and spread misinformation.[3]

"That's great. How are you approaching this work? What are some of the ideas you threw around?"
"It was easy for us to agree that the millions of people whose data was used without them knowing was a problem for us."
"But didn't Facebook's lawyers make the argument to the FTC that the 87 million people did consent to the use of their information when they signed up and agreed to the terms of service and privacy policy?" I asked.
After a period of silence, he responded: "Of course, we don't always live up to our standards, but who does? Do you?"

There's a lot in that short exchange, much of which we'll tease out in this book. In between a little defensiveness and a lot of well-timed deflection, there was insight. *It's my job*, he said, to get his company and his bosses to care about our privacy. Along with tens of thousands of other privacy lawyers, privacy professionals, and privacy engineers, it is his job to make privacy a priority. He

does that by thinking about ways to inform us about how Facebook is using our data, which reflects a particular value-laden approach to privacy with important implications for the rest of us. What he thinks and what he does matters when we're trying to understand the past, present, and future of privacy in an information age.

I rolled my eyes at corporations saying they cared about my privacy because I was focusing on the antiprivacy political economy in which all of these companies operate: informational capitalism. Informational capitalism refers to a system in which market actors commodify and extract profit from the personal data they gather about us, often without our knowledge. As they do so, Julie Cohen argues, they leverage legal tools to support their data-extractive business models and insulate themselves from liability, making the law complicit in the exploitation of our data for profit. Informational capitalism is a good description of the political economy of our time. It is therefore only rational to be skeptical when informational capitalists, especially those with checkered histories in the privacy space, profess to care about our privacy.[4]

A narrative of political economy frames – but does not fully explain – privacy's fate in informational capitalism. Systems of power need foot soldiers, whether they be true believers, mercenaries, or the merely complicit. What they think and how they do their work matters. And how they come to conceptualize their responsibilities requires us to study the link between law, organizational behavior, identity, performance, and science and technology. That's because the emails I received weren't written by an economic system or by the legal levers that perpetuate it. Nor were they written by faceless organizations we call Google or Facebook. They were written by people doing the jobs they were hired to do. These real people made the choice to use language that they ought to know makes us roll our eyes. Why would they do that? What's really going on here? More to the point, how does a regime of informational capitalism somehow result in fifty-nine emails that all use roughly the same hard-to-believe line?

Of course, we're not just talking about emails. We're talking about what I'll call the social practice of privacy law: the behaviors that implement privacy law on the ground. We're talking about how compliance professionals construct organizational systems and how engineers translate legal requirements into code, about the

arguments lawyers make in court and the counsel they provide in house, about the defaults on the smartphones we buy and the data collection going on in the background while we browse the internet, about the design of "smart" devices in our homes and the tools we have to protect ourselves. We're talking about how it all fits together into a system of corporate power that is taking away our privacy.[5]

This is a story about how companies *do* privacy. And it turns out that saying "We care about your privacy" or "Your privacy is important to us" is not an isolated email from a bad PR team. It is, I argue, a product of the routinization of antiprivacy norms and practices throughout the discourse, law, and design work of the information industry.

The risks to our privacy are so deeply embedded in the organizational, day-to-day practice of the information industry that even those people who say they truly care about our privacy are doing work that serves surveillant ends. Rather than pushing their companies to do better, something I have no doubt some of them hope to do, they often become unwitting accessories to a data-extractive business model they cannot escape. If you're wondering how an anodyne email that most of us deleted immediately is part of that story, read on.

Industry Unbound unearths what privacy scholarship has been missing: a portrait of the social practice of privacy in the political economy of informational capitalism. That portrait is one of corporate decisions constraining and influencing the rank and file and routinizing antiprivacy work, the performance of which normalizes it as the best and most commonsense approach to privacy. When this happens, the social practice of privacy law seems real to those performing it, but it really is just an act. Corporate surveillance is routinized and normalized. Privacy doesn't have a shot.