Understanding Privacy

Heather Burns

Understanding Privacy

by

Heather Burns

Published 2022 by Smashing Media AG, Freiburg, Germany.

ISBN: 978-3-945749-64-7

Copyediting: Owen Gregory
Cover & interior illustration: Espen Brunborg
Book design and indexing: Ari Stiles
Ebook production: Cosima Mielke
Typefaces: Elena by Nicole Dotin and Mija by Miguel Hernández.

Understanding Privacy was written by Heather Burns

This book is printed with material from FSC® certified forests, recycled material and other controlled sources.

Please send errors to: errata@smashingmagazine.com

To the centre of the city
where all roads meet

Contents

Foreword

by Vitaly Friedman

To many of us, privacy might feel like a complex, abstract concept. We can't hold privacy in our hands, we can't touch it, we can't explore its volume or shape with our eyes. Surely it's a part of each of us, yet it feels so intangible and so invisible — beyond reach and out of view.

And because we can't get hold of privacy, often we soothingly wave away privacy concerns, arguing that it doesn't really matter that much — after all, there is nothing particularly valuable that we deliberately and meticulously hide from anybody.

This is calming and reassuring, but also dangerous and precarious. Often we aren't even aware how our data is used; how insurance companies and mortgage calculators use our data to adjust interest rates and monthly payments; how tech genies gather data to nudge us towards buying, clicking, liking, hearting; how phones gladly listen in to our conversations to supply us with a fresh batch of targeted messages in social media; not to mention our pictures, posts, passwords and personal preferences crossing the shores of the web left and right, landing on all kinds of sites we've never heard of.

Privacy needs to be protected. It needs to be integrated in our work. It also needs to be included by default when we craft first mock-ups or refine our final prototypes. Yet to get there, we need to understand what it really means, and how to design and build experiences that have privacy at their heart.

And that's exactly what this book is about. Heather goes into all the fine details, explaining the principles behind the collection, storage, and use of personal data, and how to use those principles to create safer experiences for your users.

There are plenty of practical insights in this book, but most importantly, it will help you make better sense of privacy and get a better grasp of the privacy implications of seemingly obvious design and development decisions. Ultimately, it will give you the confidence to comfortably and confidently navigate the unpredictable waters of privacy disputes with your team, and design privacy-aware, ethical, safe and inclusive digital experiences.

Acknowledgements

This is a book I wanted to write for years. When the time was right, Smashing Magazine got the hint. The team has been a pleasure to work with, both remotely and in person at Smashing Conference Freiburg in September 2019, which proved to be my last software development conference before the world changed.

The lessons I share in this book were learned through teaching. I want to thank everyone who came to my conference talks from 2014 to 2020 for taking the time to listen and to learn. On a lonely road, your feedback kept me going. And we had some good laughs along the way.

I wrote this book in Scrivener at home in Glasgow, Scotland, and in my happy place at Joy Division's old rehearsal studio in Manchester, England. Obviously, I only function in heavy rain.

Privacy stands at a crossroads of many disciplines: code, design, law, human rights, digital rights, academia, and tech policy. It has been a privilege to work with professionals from all of those fields, including Juliette Reinders Folmer, Remkus de Vries, Stefan Kremer, Leo Postovoit, Thomas Kräftner, Peter Putzer, Robert Windisch,

Kåre Mulvad Steffensen, Konstantinos Xenos, Garrett Hyder, Chris Teitzel, JJ Jay, Lorelei Aurora, Hugo Finley, Jamie Abrahams, Rachel Lawson, Peter Ponya, Alan MacKenna, Dan Foster and the team at 34sp, Gilbert Hill, Wojtek Kutyla, Leah Lockhart, Per Axbom, James Royal-Lawson, Dan Barker, Rian Kinney, Neil Brown, Rachel Cherry, Amanda Caarson, the Accessibility Scotland team, Jasmina Byrne, Linda Raftree, Matthew Rice, Richard Wingfield, Ruth Smeeth, Mark Johnson, Gabrielle Guillemin, Rowenna Fielding, Sarah Clarke, Jen Persson, Pat Walshe, Nik Sunil Williams, Sahdya Darr, Mike Morel, Mariano delli Santi, Lilian Edwards, Richard Eskins, Dom Hallas, Maria Farrell, Konstantinos Komaitis, and Robin Wilton, all of whom contributed to the years of experience that informed this book.

My work and this book, and many other unexpected and wonderful things, would not have been possible without the friendship of Morten Rand-Hendriksen, Rian Rietveld, Caspar Hübinger, Simon Dickson, and Tom Nowell. You've all given me more than you'll ever know.

Last but not least, my daughter has gifted me with some astonishingly astute perspectives about privacy, both online and offline, and how it shapes her worldview as a young woman coming of age in a connected world. Those conversations keep me grounded. Let's keep talking, kid.

INTRODUCTION

What This Book Is About

This is a book born out of one of the biggest mistakes I've ever made. (Professionally, at least. I have already apologized to the victims of my conference karaoke.)

Let's back up a few decades. As a teenaged member of Amnesty International, I handwrote airmail letters on onion-skin paper on behalf of "prisoners of conscience" who had been jailed – and often tortured – for their private beliefs. Being a spirited young human rights activist triggered a deep obligation to understand, respect, and defend the rights to privacy and freedom of expression for people who had been deprived of those rights, and who had paid the ultimate price as a result. I still feel that today. A teenage dream's so hard to beat.

A few years later, after I taught myself how to hand-code HTML in the Lynx text browser on my university's dial-up Unix system, I found myself making websites for friends and for my student jobs. (I paid for my first analytics counter, I kid you not, by writing a check every month and sending it off in the post. Yes, I'm internet old.) Privacy was easy to achieve back in those halcyon days of the World Wide Web; we were all so exhilarated by creating a

new communications medium in real time that we had no thought for malice.

After a few years of work in international politics, local community development, and business, I found myself out of a job with a baby in my arms. So I put my mad HTML skillz to work and set up shop as a professional web designer and developer, a role which spanned the transition from graphic-based web design software to the rise of open-source CMS applications. A few years into my work as a web designer, something called social media entered the picture. Like a failed marriage, it was amazing at the beginning, but it got dark really quickly. Privacy was, and remains, a large part of that problem.

The thing about working in politics is that it's like the Mafia: you never really leave. The game can, and will, creep back into your blood. Through my involvement in open-source CMS communities, I found myself giving conference talks on policy issues such as privacy, accessibility, and intermediary liability – and I loved it. I loved it so much that I pivoted out of web design and went to the politics of tech full-time. My ability to translate the complexities of regulations and standards into actionable language has helped dozens of development communities across Europe and remotely around the world. It now sees me working directly with politicians in Westminster, Edinburgh, and Brussels

on helping to shape proposed laws in ways that will, I hope, keep the web open. But I'm getting ahead of myself here.

Around 2016, as the General Data Protection Regulation (GDPR) entered the picture, I began to give conference talks on what the updated European privacy rules would mean for web professionals, and what developers and designers would need to do to up their privacy game. Some audiences left confident about their new knowledge. Some audiences left enlightened about privacy as a fundamental value. Some audiences left inspired to make privacy-centric development a selling point for their digital agencies.

And some audiences responded as if I'd slapped them in the face. They attacked me, my work, my colleagues, Europe, and the concept of privacy in general in language that was – well, not suitable for the Smashing family of books.

What the—? I thought. *What did I miss?*

This book is about what I missed.

What follows in these pages is an introduction to the beliefs, concepts, and ideas that inform privacy as it exists – or has failed to exist – on the open web that we build. It's about all the fundamental values of privacy *as a concept*, which precede privacy *as a legal compliance issue*. It's about the ways

these concepts impact your work as a designer, a developer, or a project manager. And it's about the ways you can adopt these principles to create a healthy, user-centric approach to privacy in everything you do.

That's what I missed. I had understood users but not my audiences. I had assumed that my development audiences knew the basics and the principles and the concepts, and from there the jump to a legal compliance overview would be easy. I had mistaken my formative experiences, both on- and offline, for theirs. I was wrong. Through no fault of their own, my audiences didn't know the basics, or the principles, or the concepts.

That comprehension gap also explained the hateful push-back. To some audiences, when I spoke about GDPR, they didn't hear me talking about the users of the services they build, or the fundamental right to privacy, or the role their work plays helping to uphold those rights. They heard me yapping about a foreign government telling them what to do and creating a lot of bureaucracy. They saw me and everything I was saying as a personal and professional threat. They *hated* me for it.

That realization was as much of an enlightenment for me as it was for some of my audiences. The number of developers who told me that my conference talks were the first time

they had been taught about privacy – *at all, ever, from anyone* – was genuinely terrifying. What I had done, as a result, was thrown them straight into the advanced levels without explaining the fundamentals.

This book is the response to that hard lesson. I have done my best to explain what I have experienced working on privacy from every angle – human rights, law, policy, and web development – in the simplest way possible, and in the most positive way possible, in ways you can comprehend, use, and adapt in your work on the web right away. It's why I've called it *Understanding Privacy*: it's as much about my learning journey as it is about the one you are now beginning.

What I'm going to discuss in this book is applicable to any programming language, software community, or project workflow. For that reason, you won't find any code samples in this book. A healthy approach to user privacy, after all, doesn't tell you *how* to code. It tells you how to make the right decisions which *inform* the code. It also gives you the foundation you need to question, and even challenge, workplace practices which might not be in your users' best interests.

Likewise, this book is not a legal reference manual. While I will briefly cover the major privacy regulations and propos-

als in context, I want you to understand the common values which inform nearly all user-centric privacy regulations, and to apply them regardless of the presence or absence of a legal framework. For those of you working in countries and systems which do not have comprehensive or sufficient privacy laws – I'm looking at you, America – these concepts and principles are all the more important for you to understand and adopt right away.

> It should go without saying, by the way, that I am not a lawyer, this book is not legal advice, and it should not be used for any legal compliance purpose. Neither I, nor the good folks at Smashing, are legally or morally responsible for any compliance issues you may find yourself facing in your work.

By the end of this book, you will have shifted your understanding from a negative view of privacy as a scary legal compliance obligation to a positive view of privacy as an opportunity to build a better web. You'll understand what privacy is *really* about beyond scary headlines. You'll gain

some insight into what public expectations of you are at a time when people feel that they have no control over their data. And, for what it's worth, you'll gain some insight into the expectations that lawmakers and privacy regulators have about you and your work on the web at a time when many of them are out for blood.

I hope this book will help you put your users first in everything you do. You'll become a better web professional in the process, and – just maybe – a better person.

This book is in five parts. In the book's first section, "**Privacy and You**," we will review the fundamental concepts, definitions, and frameworks behind privacy and data protection.

In the second section, "**Privacy and Your Work**," we will discuss how to integrate a healthy approach to user privacy into everything you do, whether you are a designer, a developer, or a project manager.

In "**Privacy and Your Users**" we will review the issues around user privacy where you can make a difference.

In the fourth section, "**Privacy and Your Future**," we'll discuss how to make the job easier for those who will follow us.

And in the last unexpected section, "**Postscript: Privacy and Health Data**," I address issues which I could never have imagined when I started this book: the hard lessons we learned about user privacy from the global pandemic, and what those experiences teach us about the health data challenges ahead.

So let's begin.

PART ONE

Privacy and You

“Privacy is the ability to make our own choices without fear.”

—Roger McNamee, *Zucked: Waking Up to the Facebook Catastrophe* (2019)

CHAPTER ONE

Privacy and You

The first step we'll take together in our shared journey to build a more privacy-conscious web is to arrive at a shared understanding of concepts, values, and approaches.

What Privacy Is

Let's strip it all the way back to the basics. *What is privacy? How does it work?* It's a lot simpler than you think.

When we talk about the web we build, we often use the terms *privacy* and *data protection* as if they are the same thing. They are not. Privacy and data protection are two very different concepts, and two very different disciplines, existing in very different settings. And while lawyers, academics and philosophers can split hairs over the two terms' precise definitions, as well as the century of international treaties and case law that have informed them, the broad concepts applicable to our work are a lot easier to understand.

So here's the simplest way to understand it.

Privacy is a person's *right* to maintain control over their private life, to make choices about the information which exists about them, and to be free from intrusion in their private life. Privacy in the online context is about the *right* to control the access people have to you and the information they hold about you. It is about having the right to have options to safeguard or diminish that control. Privacy, in the words of the famous legal judgement, means the *right* to be left alone, if that is what you wish.

Data protection, on the other hand, is the legal and procedural structure that exists to provide the *means* for people to exercise their privacy rights, as well as any human rights that safeguard them, over the collections of information that bodies and individuals hold about them. Data protection in the online world is the *means* that gives you the ability to control the access people have to you, and the data they hold about you. It is about having the structures and protections of the rule of law, whether statutory or contractual, in upholding your personal privacy. Data protection is the *means* of not being adversely affected by the collection, processing, and analysis of data about you, if that is what you wish.

Privacy is a concept. Data protection is a procedure built around that concept.

Privacy is a value. Data protection is a process to uphold that value.

Privacy establishes freedoms. Data protection establishes safeguards to uphold those freedoms.

Privacy is what you believe. Data protection is how you put those beliefs into action.

The "beliefs into action" part is where we, as the makers of the web, tend to go wrong. By reading this book, you're taking a small step towards putting things right.

Differing Legal, Cultural, and Historical Approaches

When it comes to teaching online privacy, I presented at dozens of conferences, wrote tens of thousands of words, trained rooms full of developers, spoke myself hoarse on podcasts, and supported numerous privacy teams. What I am going to tell you now is the one thing I did not fully understand until many years into that work:

We don't have a clue about each other.

I certainly didn't.

It's that lack of understanding about one another and where we come from, and the things we believe about privacy and data protection, which have inadvertently brought about so many of the privacy problems we face today. And understanding those differences so that we can overcome them is the key to moving forward, together, to make the web better.

The fact is, when we are discussing privacy, **we have very different historical, cultural, and legal approaches** about what privacy is, where it comes from, and how it works. We grow up believing, knowing, and living by those values. We assume everyone else lives by those values too. They do not. Yet here we all are, working together remotely on the same teams, working on the same projects, and integrating our conflicting beliefs into our work. Our users have paid the price.

The web, as the medium you work on, is essentially transatlantic. It was invented in Switzerland by an English scientist, but it reached its commercial potential in the United States. This means that the majority of the sites, services, and platforms we use and have come to rely on are American. In many ways, the commercial web has become a form of cultural diplomacy: it has exported American values on privacy around the world, to the point where the private actions of tech companies have set the global defaults we live with. It seemingly never occurred to anyone that those

views on privacy might be different in other places. It's why the situation became so explosive when the European view on privacy began to assert itself in the run-up to GDPR. What should have been a professional discussion about technology became a clash of civilizations.

So a little more cultural diplomacy might be in order.

What follows are *admittedly broad* generalizations outlining the values we hold about privacy. I have explained these differences not to cast sides against each other, or to claim one is better than the other, or to push us further apart. Just the opposite. I want you to understand what the people you work with understand and know and believe, the values that inform the ways they build the web, and the places where our differences begin, so that you can recognize them and work together to overcome them.

These differences might just surprise you.

CULTURAL APPROACHES TO PRIVACY

The European approach to privacy holds that it is a fundamental human right, as well as a value upheld in law through data protection regulations which set out how private data can be used. Those laws are built around a framework of the individual rights a user has over their data. That

framework holds the user as the *owner* of their data, even if it is in the possession of someone else. It also takes what we will call an "opt-in" approach: the user must actively give consent for their data to be collected, used, and held by someone else. In other words, the approach is centered around individuals.

In general, Europeans trust governments far more than businesses. For this reason, the European approach sees disputes about user privacy addressed by data protection regulators, which are mostly arms-length government bodies for the purposes of objective independence. These bodies (in theory) work constructively and cooperatively with companies holding data about people to bring them into healthy compliance with data protection law. Fines or court action are only ever a rare last resort in cases of truly egregious privacy breaches, truly sloppy data protection practices, or truly uncooperative companies.

By contrast, the American cultural approach to privacy does not view it as a fundamental right. While privacy is briefly alluded to in the Bill of Rights, free speech – not privacy – is held to be the primary right, and courts have been known to rule that privacy, in certain cases, is an *impediment* to freedom of speech. The American approach holds that the data about a person, no matter how personal or intimate, belongs to the party holding the data. It also takes what we

will call an "opt-out" approach: the user does not have to give active consent for their data to be collected and used and held by someone else, and they must actively request that their data should not be used. In other words, the approach is centered around companies.

In general, Americans trust businesses far more than governments. For this reason, the American approach to privacy is through a culture of adversarial courtroom legislation, and one which sees privacy dealt with as a subcategory of other forms of law. There is no constructive cooperation through an independent privacy regulator first; this is a "sue first, ask questions later" way of doing things.

Those differing cultural approaches to privacy were born out of very different historical experiences.

HISTORICAL APPROACHES TO PRIVACY

The historical European perspective on privacy is one which places the needs of collective society over the needs of any one section of it. (You may know this as "the needs of the many outweigh the needs of the few.") That view, above all else, prioritizes human rights – including privacy – over individual rights. This view does not mean that individuals have no, or fewer rights; it means that individuals are seen to have obligations over other people's right

to privacy. This has been a lesson learned through the most painful experience possible. The post-war recovery period which established privacy as a fundamental right was a direct response to the continent's legacy of genocides, ethnic cleansing, pogroms, and state totalitarianism. The historical European approach, at its heart, is a form of atonement: one that says "never again."

The historical American perspective on privacy, by contrast, is one which places the needs of the individual over the needs of collective society. This approach prioritizes individual liberties and freedoms over human rights as they are known in the European context. This view was born out of two formative legacies. The first was the east coast "Puritan" legacy, a theological view which held that private life should be public life (and if there was something in your life you wanted to keep private, it obviously must have been some form of filthy sin). The other was the west coast "frontier" legacy, the mythology of an endless land, which you had the freedom to make your own, and do what you wanted to do, without permission or consent. The historical American approach to privacy, at its heart, is an extension of the American dream.

Those very different historical experiences have led to two contrasting legal approaches to privacy.

LEGAL APPROACHES TO PRIVACY

In the European approach, privacy is *legislated* through hard law in the form of data protection regulations. This view has one "omnibus"[1] law which applies to all member states, all situations, all sectors, and all sizes, whether the person holding the data is a one-woman business or a multinational corporation. That view does not preclude additional privacy regulations, such as the safeguards used in the financial services sector, or even tougher privacy legislation, as is practiced by some German states.

In the European approach, privacy is *administered* and *enforced* through data protection authorities. An individual's privacy rights are not tied to their citizenship, nationality, or location, and there are no qualifications required before those rights apply; if the data exists about them in Europe, so do their rights. Privacy, of course, is its own distinct body of law, and litigation is a last resort.

In the American approach, privacy is *governed* through soft law in the form of industry codes of practice, self-regulation, or terms and conditions. There is no omnibus law applicable to all states, situations, or sectors; what privacy law exists instead is an array of local and sectoral laws. Without a federal-level privacy law to regulate, there is no national data protection regulator.

1. "Omnibus" is a specific legal term which you may prefer to think of as "umbrella": it covers everything.

In the American approach, an individual's privacy rights, such as they are, are very much tied to their citizenship, nationality, or location. If there are no protections covering them because of where the data happens to be held, or what sort of business happens to have it, that's just something they have to live with. Finally, because privacy is largely shoehorned into other ways of dealing with it, litigation is often the first resort.

So what does all of that transatlantic trivia mean?

It means that for nearly thirty years, we – as the makers of the web – have approached our work with different understandings of what privacy is, how it works, how it applies to the things we build, and what expectations our users have of the things we build for them. We have never paused to consider those cultural, historical, and legal differences, much less understand the impacts they have on the web we build. As a result, we haven't always done everything we could have done to understand the privacy rights that our users are entitled to, or to build them the safeguards they deserve even if they don't have those rights.

Our users should *never* have been caught in the middle of that.

Building a better web needs to mean overcoming our biases, enhancing our foundational knowledge, and committing to

do whatever it takes to put user privacy first. Let's learn how a healthy understanding of data protection concepts can give us the tools we need.

Essential Privacy and Data Protection Values

Data protection laws, believe it or not, are not just plucked out of the air. The values which create a healthy approach to privacy, and which inform the shape of data protection laws, have been determined over several decades by a range of international treaties and standards. It's testament to the work that went into them that their values remain universal and modern, even though some of the frameworks predate the open web. Those documents are not laws themselves; rather, much like web standards, they are recognized agreements on the concepts, definitions, and guidelines for good data protection practice.

By looking at the main data protection conventions and principles,[2] we can map out the essential values which all of them share in common. These values form what I call the essential privacy data protection principles. ***These are the actions which make privacy possible.*** A healthy understanding of these principles is essential to forming a user-centric view of privacy on the web.

2. https://smashed.by/oecd; https://smashed.by/coe; https://smashed.by/isoprivacy; https://smashed.by/apec; https://smashed.by/ftcprinciples

Essential Privacy Principles

1. Data Minimization

- ✓ Restrict the data you collect and process to the minimum amount necessary.
- ✓ Restrict access to that data to the minimum amount of people and systems necessary.
- ✓ Do not duplicate or aggregate data by default.

2. Data Integrity

- ✓ Ensure that the data you collect and process is correct, relevant, and up-to-date.
- ✓ Consider the consequences which could arise if any of the data you hold is inaccurate.
- ✓ Consider the consequences which could arise if poor data negatively impacted someone.

3. Purpose Minimization

- ✓ Only collect and process personal data for the active purpose it was intended for.
- ✓ Only collect and process personal data that the user was clearly informed about in advance.
- ✓ Do not collect and process personal data you do not have an active purpose for but might have a potential purpose for in the future.

4. Life Cycle Limitation

- ✓ Delete unnecessary, excessive, outdated, and redundant data on a regular basis.
- ✓ Delete data, both in active use and in archives, which is no longer needed by both the recipient and any third parties.
- ✓ Do not share data with others at any point in its life cycle without a justified reason as well as user consent.

5. Information, Technical, and Human Security Measures

- ✓ Take adequate information security measures to protect the data you hold from misuse and its subjects from harm.
- ✓ Take adequate technical security measures to safeguard the data, such as your systems, software, and code.
- ✓ Take adequate human security measures over the people who have access to the data, through procedures such as staff training, guidelines, and supervision.

6. Transparency and Notice

- ✓ Inform your users how their data is being collected, processed, and shared, including the data you send to or receive from third parties, and inform your users of any changes in your use and processing.
- ✓ Inform your users what rights and choices they have over the ways you collect, process, and share their data.
- ✓ Make your privacy disclosures transparent, publicly available, and accountable to both your users and to privacy regulators.

7. User Participation and Rights

- ✓ Give your users rights to access their data, download their data, correct errors, and to control your collection and processing of their data.
- ✓ Give your users the ability to ask you to stop using their data, and to stop sharing it with third parties.
- ✓ Give your users the right to delete their accounts and their data.

8. Accountability, Redress, and Enforcement

- ✓ Create robust internal documentation of your collection and processing of user data, your stewardship over that data, and your legal compliance.
- ✓ Fix problems as soon as they are discovered, and provide redress when data is misused, leaked, or breached.
- ✓ Take responsibility when things go wrong, and be morally and legally accountable for the consequences.

9. Choice, Control, and Consent

- ✓ Give your users and visitors choices and options over your collection and processing of their data, including the data you send to or receive from third parties.
- ✓ Require clear, specific, and informed opt-in consent for all users of a user's or visitor's data, and do not require unnecessary consents in order to use a service.
- ✓ Give your users and visitors a means to control their options and rights at any time through settings, user accounts, or control panels.

10. Special Categories of Data

- ✓ Take extra informational, technical, and human security measures to safeguard sensitive data that could result in the people it is about being hurt, exploited, or in some political contexts, placed at physical risk. This may include information about a person's race, religion, health, sexuality, location, genetic/biometric information, etc.
- ✓ Take extra care to ensure that sensitive data is not aggregated with other data, duplicated, sent to third parties, or combined with data received from third parties.
- ✓ Consider how you will respond to law enforcement or government demands for information about

your users for reasons which are not necessarily in your users' interests.

11. Legal Compliance and Accountability

- ✓ Ensure that the work you are putting into the world meets the privacy regulations of the places where it will be used to collect and process people's data.
- ✓ Work cooperatively and productively with data protection regulators, data protection officers, privacy professionals, policymakers, and industry/supervisory bodies.
- ✓ Do not use the absence of a privacy law as an excuse to violate your users' privacy.

If you work in a system where data protection exists within a legal framework, these concepts will look and feel familiar to you already. If you work in a system which does not have a robust approach to privacy, it is all the more important for you to understand and adopt these principles into your work.

After all, the most important principle for all of us to remember is that **a user's privacy protections should never be contingent on the presence, or the absence, of a privacy regulation which has formalized those principles into law.**

Speaking of laws, let's go into a non-legal overview of the major privacy regulations that shape your work on the web – whether you realize it or not!

Privacy through Hard Law

As we've discussed, in countries and systems that uphold privacy as a fundamental human right, privacy is *regulated* through privacy law. In countries and systems that do not uphold privacy as a human right, privacy is *governed* through other forms of law, or through soft regulation.

While that may seem like a difference in semantics, for web professionals like you and me, it creates huge differences in our approaches to user privacy and protection. It also creates very different attitudes towards consequences and enforcement.

What follows is an overview of each approach. Because this book is geared towards readers in the two systems where the key battles of online privacy are fought – Europe and North America – I will give a broad compare-and-contrast overview of each system. While I would also love to give an overview of the divergent concepts of privacy in Asia and in South America, as well as the vibrant approaches emerging from Africa's tech sector, those topics are not mine to discuss. Perhaps you'll be the ones to write about them.

THE EUROPEAN PRIVACY FRAMEWORK

As we've discussed, Europe has a strong legal, cultural, and historical approach to user privacy as a function of human rights. This resulted in the original EU data protection framework, the Data Protection Directive of 1995 (that's 95/45/EC for my fellow wonks).

As with all EU-wide legislation, this law was then transposed – meaning implemented – into each member state's national legislation through their domestic political processes. For example, in the UK, if you ever heard (as you certainly did) someone referring to the Data Protection Act, what they were really referring to was the domestic implementation of an EU law.

The 1995 directive established the eight core principles of the European data protection approach – principles you'll instantly recognize from our earlier overview. According to the principles, data must be:

1. Processed in a manner which is fair and lawful

2. Used only for the manner in which it was intended to be used

3. Processed in a manner which is adequate, relevant, and not excessive

4. Accurate and kept up to date

5. Not kept for longer than its intended purpose

6. Processed in accordance with the rights of the people the data is about

7. Protected by technical and organizational security measures

8. Not transferred to third countries outside the EU which do not guarantee an adequate measure of data protection

That numbering system is canon, and within professional privacy and data protection circles it is the terminology of the profession. For example, you might hear a data protection regulator explaining how a company violated the fifth principle.

The 1995 Directive established the European data protection framework as being both *universal* and *extraterritorial*. This means that the rules apply to all personal data collected, processed, and retained about persons within the European Union regardless of citizenship or nationality, regardless of the holder's size, sector, or turnover, regardless of the situation it is being used for, and regardless of where that

data is being handled. This established that anyone doing business in an EU member state, or collecting data on European customers, is legally required to protect their data in full accordance with the regulations as if they themselves were in Europe.

The 1995 law also set out the framework for regulatory oversight, enforcement, international data transfers, and exemptions for obvious situations such as law enforcement. More importantly, the original Directive also established the core data protection concepts which structure the European approach.

GDPR

All things considered, the 1995 Data Protection Directive did remarkably well to work for twenty-three years, despite having been drafted for a dial-up-and-floppy-disk world. For a mobile world, however, an update was clearly needed. After many years of work and contention, the modernization was GDPR, the General Data Protection Regulation, which took effect on May 25, 2018.

GDPR took everything from the original directive and upgraded it – and hopefully future-proofed it – to better deal with the ways we handle data today. Nothing in the original directive was lost or discarded. It was, however, brought up

to date: for example, with updated definitions of the essential concepts behind the European data protection approach. GDPR also refreshed its requirements to better reflect the ways we engage with our users through things like privacy notices, data breach preparation, and user consent, as well as the data we collect about children.

GDPR also added a ninth data protection principle to the 1995 definitions: the *accountability* principle. In my training work with developers, I referred to this as "Document it or it didn't happen." The accountability principle means that you need to document your processes, your inventories, and your approaches to prove that you are in healthy compliance with the first eight principles. As far as I am concerned – and, for that matter, as far as slightly crotchety European data protection regulators are concerned – if you can't show me a document which proves your accountability, signed off by a senior decision-maker and available to everyone working in a project, you didn't do it at all. But more on that later on.

Companies that were in healthy compliance with the 1995 Data Protection Directive found that the upgrade to GDPR was relatively straightforward and clear. Companies that had been remiss in their compliance with the existing rules had the most work to do. Wherever you fall on that scale, it's important to remember that both laws were the codification

of best practice principles, which were then grouped around the essential concepts we discussed earlier.

What I'm really saying here is that if you approach GDPR as a *legal compliance obligation about punishments and fines*, you are going to panic and freak out. If you approach GDPR as *a series of concepts about safeguarding user privacy*, you are going to approach the task with confidence. So take a minute to shift your thinking.

Are we cool? We're cool. Let's now get to grips with those concepts.

> One phrase you will never hear me use is "GDPR-compliant." Why? Because there's no such thing as being GDPR-compliant. It isn't possible. GDPR is about systems, processes, and procedures. It is a journey, not a destination. That journey, for what it's worth, should be taken from the positive view of user protection, not a negative view of compliance as a regulatory threat. So don't think in terms of becoming GDPR-compliant – think instead of how to work towards a healthy regard for user

privacy, using GDPR as your roadmap, every day. And while you're on that journey, remember to cast a very suspicious eye at any individual or service provider claiming they can make you compliant.

BASIC DEFINITIONS ABOUT DATA

The basic concepts behind the European data protection framework were defined in the 1995 Directive, and all of them were carried through to the GDPR modernization and upgrade. That's because, as you will see, these concepts are simple, universal, and common-sense.

Personal Data

The European data protection framework pertains to *personal data*. This is defined as "any information relating to an identified or identifiable natural person."[3] This can be one piece of information or multiple data points combined to create a record.

GDPR expanded the definition of personal data to include:

- genetic data
- location data

3. https://smashed.by/europeanparliament

- biometric data (such as facial recognition or fingerprint logins)
- pseudonymized data (more on that in a minute)
- online identifiers

The final item is important for developers. It includes things like IP addresses, mobile device IDs, browser fingerprints, RFID tags, MAC addresses, cookies, telemetry, user account IDs, and any other form of system-generated data which identifies a natural person.

Personally Identifiable Information

The European term *personal data* differs from the American term *personally identifiable information (PII)*. The latter pertains to a much more limited set of information than the European model. It also does not see information as contextual, whereas the European framework stresses the risks inherent in data aggregation.

PII includes a person's full name (if it is not common); their home address; their email address; their email address (if it is considered private, as opposed to something like a work or association address); their national ID number (for example, their social security number); their passport number; their license plate number; their driver's license number; their face, fingerprints, or handwriting; their credit card

numbers; a digital identity; their date of birth; their birthplace; genetic information; their telephone number; and their login name, screen name, nickname, or handle.

What *might* be PII? A person's first or last name, if common; their country, state, postcode or city of residence; their age, especially if non-specific; their gender or race; the name of the school they attend or workplace; their grades, salary, or job position; their criminal record; and the cookies on their devices.

All of those things, plus many more, are personal data in the European definition.

The important thing to remember is not to use the terms personal data and PII interchangeably. They are very different concepts in very different contexts, and you'll risk looking like you're bluffing if you mix them up.

Sensitive Personal Data

Beyond personal data there is also *sensitive personal data*, defined in the European model as information about a person's:

1. racial or ethnic origin

2. political opinions

3. religious or philosophical beliefs
4. trade union membership
5. health data
6. sex life or sexual orientation
7. past or spent criminal convictions

It should go without saying that breaches of these kinds of data can have devastating – and sometimes literally fatal – consequences for the people the data is about. For those reasons, sensitive personal data requires stricter protections than regular personal data, and the consequences for its leakage or misuse are greater. We'll take an unexpected deep dive into this topic in the Postscript.

Pseudonymous Data

GDPR introduced a new category of data called *pseudonymous data*. Pseudonymization is "the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information."[4]

In other words, the personally identifying data is stripped out and held separately and securely away from the pro-

4. https://smashed.by/europeanparliament

cessed data. What makes data pseudonymized is that it can be reassembled with the personally identifying data linked to the data record later on. Hence the term pseudonymous: the data is not quite anonymous.

Europe would like developers to pseudonymize their data and, to that end, pseudonymized data carries relaxed requirements on data controllers. You may wish to look into it.

> Under the GDPR's penalty rules, "unauthorized reversal" of pseudonymized data – in other words, reassembling datasets to identify the individual concerned without permission – constitutes a data breach.

Data Controllers and Data Processors

Personal data is used by *data controllers* and *data processors*.

The *data controller* is a person or an entity, such as you or your organization, which decides what data is collected, how it is used, and with whom it is shared. If you collect personal data about people, whether that's your cus-

tomers or the people who have downloaded your app, you are a data controller.

The *data processor* is any entity other than the data controller who processes the data on their behalf. If you work with clients who give you access to their data and systems, or if you provide a third-party application which stores personal data for those who use it, you are a data processor.

In your work on the web, you may be a data controller, you may be a data processor, and you may be both.

USER RIGHTS

As we discussed earlier, the European view of privacy holds that a person is the owner of the data that exists about them. For that reason, the European data protection model gives users certain fundamental rights over your possession and use of the data you hold about them.

The 1995 Directive viewed these user rights through the lens of the technology which existed at the time, meaning the information that a user voluntarily provided to a data controller. The 2018 GDPR revamp refreshed and enhanced these rights to reflect the ways that much of the data that

flows about us, and in turn influences the decisions made about us, is held by companies using our data without our knowledge or consent.

I want you to memorize these fundamental user rights, because wherever you live or work, you should build them into the foundations of everything you create. They are:

1. The right to be **informed** about what you are doing with people's data, specifically through privacy notices and clear information.

2. The right of users to **access** their data, which means the right to see just what information you have on file about them.

3. The right to **rectification**, which quite simply means the right to correct any incorrect data you are holding about them.

4. The right to **erasure**, commonly known as the "right to be forgotten," meaning the right to have certain kinds of data deleted under certain circumstances.

5. The right to **restrict processing**, meaning the right for a user to ask you to stop using their data in certain ways.

6. The right to **data portability**, which means the user's right to download the data you hold about them and upload it to a different service provider.

7. The right to **object**, meaning a user's right to object to your uses of their data.

8. Rights in relation to **automated decision-making and profiling**, which largely pertains to data you may use for the purposes of advertising, marketing, and behavioral analysis, including through artificial intelligence or machine learning.

These individual rights are **granular**, which means that a data subject can invoke any one of those rights at any time. One is not a prerequisite for another. It also means that GDPR does not permit an all-or-nothing, either–or view of data processing, which would be considered an abuse of the user's rights. For example, a customer can object to your sharing their data with third parties for advertising purposes while still keeping their account open with you. You cannot require their data to be shared for advertising purposes as a prerequisite for being a customer.

The fourth right, the "right to be forgotten," is perhaps the most misunderstood aspect of GDPR. It is not universal and it is not unconditional. The "right to be forgotten" is

not the right to fly under the radar and have inconvenient information scrubbed from a database. (An Irish prisoner recently made a rather creative attempt to have his criminal convictions forgotten – while still serving time for them.) The "right to be forgotten" is also not a tool for censorship, covering up criminal wrongdoing, or shutting down conversations we would rather not have. What it does mean is that information which is truly irrelevant, redundant, or harmful can, under the right circumstances and with careful consideration, be removed from places it no longer needs to be.

Subject Access Requests

So how does a user invoke their rights? The best way to start is by invoking their right to be informed, so that they know what data you hold about them; from there, they can decide on their next course of action. One way they can do this is to file a *subject access request*, or SAR. Think of it as a Freedom of Information Act request for your own data.

An SAR is a request made by someone whose data you hold or process, submitted in any format, for you to provide them with:

1. confirmation that you are collecting and/or processing their personal data

2. a copy of the personal data that you hold on them

3. any other information you have in your possession about the subject, such as details of the data you have passed to third parties

Your SAR process should be clearly explained in your privacy notices, which we will discuss later. There are strict time limits, defined by your data protection regulator, for when you must respond to an SAR. An SAR must also be responded to in a machine-readable format. That does not mean sending the individual a CD-ROM in the post, which – I am not making this up – some companies are still doing, in the year 2022, in response to SARs. I also still hear stories of companies responding to SARs by sending the requester a paper printout, which is the tech bro equivalent of a toddler tantrum.

> Before GDPR, it wasn't unknown for site administrators to charge users a fee for invoking their data protection rights, such as deleting old forum posts, ostensibly to cover the costs of staff administration and time. Under GDPR you cannot charge an individual who wishes to invoke one of these rights, nor can you withhold the service if they cannot or will not pay.

That is because you cannot charge an individual to exercise a fundamental human right – and privacy, of course, is one.

CONSENT AND WHERE TO FIND IT

In the European data protection model, user consent is everything. This means that you cannot just collect whatever personal data you want, whenever and how you might want to do it, for any purpose you might like. You must have active user consent, grounded in a legally justifiable reason to use it. The data you collect and process must be for the user's active and current benefit – not your passive and potential benefit. And the ways you capture that consent, whether that is through an active customer relationship or a passive website visit, must be clear, documented, and verifiable.

In most cases, the data collection and processing you perform must be done with the *consent* of the people that data is about. Consent, however, is obviously not absolute. In situations where consent is not the basis for your use of a person's data, your use of data must be grounded in a *legal justification*.

Let's talk about consent first. The ways in which your users grant consent for you to collect, process, and share their personal data must be:

1. **Active**: their consent must be freely given, specific, and unambiguous.

2. **Positive**: active consent must also be positive, meaning you have not presumed their consent from a pre-ticked box, inactivity, or *not* selecting any option. If the consent was not active, and it was not opt-in, it wasn't consent.

3. **Granular**: privacy, like user rights, must be presented as multiple choices, and not as a black-and-white, either–or choice.

4. **Unbundled**: users cannot be forced to grant consent for one thing in order to receive another.

5. **Named**: the user must be made aware of all specific third parties who will be receiving their data and why they will be receiving it – you'll do this through your privacy notice, which we'll discuss later.

6. **Balanced in the relationship**: the user's consent must not create an unfair relationship between the

user and the data processor, such as mandatory location tracking of an employee's whereabouts outside working hours and, in our times, tracking an employee's contacts outside working hours with a Covid tracking app.

7. Most importantly, **verifiable and documented**: you must be able to prove who gave their consent, how consent was given, what information they were given, what they agreed to, when they consented, and whether or not the user has withdrawn their consent.

Recall the user rights we just discussed: all of those user rights apply to these forms of consent. A data subject may withdraw their consent for any reason at any time, and they do not have to provide you with a reason for doing so.

If your user data is not grounded in active consent, you must be able to justify your collection and processing of data in one of five specific **legal bases** for the use of personal data. These include being:

1. Necessary for the performance of a contract, meaning the personal data you have to collect to provide someone with a product or service, such as their order data or account setup.

2. Necessary to comply with a legal obligation, whether that is your own obligations as a professional or the user's obligations to any other law.

3. Necessary to protect the person's vital interests; for example, providing emergency medical help.

4. Necessary for the performance of a task in the public interest or in the exercise of official authority, meaning that you work for the public sector.

5. Necessary for the purposes of the "legitimate interests" pursued by the controller or third party.

Legitimate Interests

Let's talk a little bit about that last one, "legitimate interests." This is the most abused aspect of GDPR. Legitimate interest was intended to provide a means for personal data to be collected and processed, in good faith, for situations that simply did not fit either a consent or legal basis situation, such as third-party relationships. However, in practice, it has become a catch-all excuse for people to do whatever they want and call it "legitimate interest."

Personally, whenever I see (for example) a newspaper site using legitimate interest to default opt-in to over 1,500

third-party adtech providers, what I really see is a marketing manager throwing a tantrum and shouting "I don't care what YOU want. I WANT YOUR DATA, AND I AM GOING TO GET IT!" (That's not actually what I hear her saying, but this book will be read by young adults.)

This game won't last long: privacy professionals are now requiring legitimate interest impact assessments, similar to privacy impact assessments, from anyone claiming legitimate interest with a straight face. Data protection regulators are also taking a very low opinion of companies using legitimate interest as the first choice rather than the last resort.

In my training, I advised people not to invoke legitimate interest at all: if the situation does not fit a consent or legal basis, don't do it. However, if you feel that your use of data meets legitimate interest in good faith, and you are willing to put your name to a separate legitimate interest impact assessment which confirms that, and you are also willing to explain your decision to your data protection regulator's face, go ahead and use it.

DATA PROTECTION REGULATORS

In EU member states, the supervision and enforcement of data protection issues rests with the **data protection**

authority (DPA). Each country has a DPA, and Germany has state-level DPAs as well. Iceland, Liechtenstein, and Norway, as EEA members, also have DPAs which work in alignment with the European model.[5]

Data protection authorities are privacy educators as well as watchdogs. Most DPA websites contain useful compliance advice for small businesses, developers, and growing enterprises. Outside their educational role, they issue rulings and guidance on privacy law, audit organizations for compliance, process public complaints, and in cases of data protection breaches or issues, work to fix the problems and enforce the penalties. DPAs work in close cooperation across Europe through an umbrella organization called the European Data Protection Board, which issues guidance and legal clarifications on a regular basis.

And, believe it or not, they are not out to get you. DPAs will happily work with businesses that come to them in good faith for guidance and support in getting it right for their customers and users. Some will even do site visits to your place of work to listen to your concerns and offer compliance advice. It is far better to make their acquaintance to get it right before you have done something wrong than it would be to meet them after a complaint has been made.

5. For a full directory of DPAs across the EU, visit https://smashed.by/edpbmembers

Most data protection authorities require companies processing personal data to be registered with them. This usually requires a small fee. The registry number they will give you should be displayed in your privacy notice. Your details will be searchable on the national data protection registry, which is public. A failure to be registered can be a data protection offence in and of itself.

If your work in the EU spans more than one member state, you will need to identify what is known as a **lead supervisory authority**. This refers to the data protection authority in the country that is the location of your main establishment. The standard for determining that location is: it is where decisions about data processing are made; in other words, where the authority to process data comes from. If this rule applies to you, your lead supervisory authority must be clearly stated in your privacy notices too.

(A bit of office politics comes into play here. The lead supervisory authority rule was a response to certain data-hungry companies – we won't name them, but you can guess – which engaged in "jurisdiction shopping." That means they sought to base their legal registration in countries they perceived to have the most relaxed data protection laws. It didn't work.)

Penalties and Fines

Most data protection regulators work on a four-tier system of enforcement.

The first three tiers are known as notifications, undertakings, and enforcement notices. Put loosely, notifications are a polite heads-up to advise a company to get its act together; an undertaking is a company's agreement to get its act together; and an enforcement notice is an order for a company to get its act together. These initial three tiers cover the majority of data protection issues.

Fines are only the fourth tier and are used as a last resort or in cases where the data misuse was clearly beyond the realm of a polite agreement. Under GDPR, DPAs are authorized to impose two levels of fines for data breaches or actionable violations of data protection law. Level 1 fines can be imposed for up to €10 million or 2% of a company's global annual turnover, whichever is the greatest. Level 2 fines can be imposed for up to €20 million or 4% of a company's global annual turnover, whichever is the greatest.

The difference between level 1 and level 2 fines, predictably, concerns the size, severity, and depth of the data protection issue. While those fines clearly target the tech giants who

can afford it, they should also be a nudge to tighten up your own data protection practices.

Once remitted, fines for data protection violations go into the member state's national treasury. Data protection regulators are not padding their own nests.

Prosecutions are also used in cases where data misuse is a part of more widespread criminal activity.

Data protection regulators, as they did before GDPR and as they continue to do after it, only issue penalties and fines which are necessary, reasonable, and proportionate to the breach committed as well as the business which breached it. A small business will be fined as a small business, not as a multinational. A small breach will not force you to sell your house. It is also helpful to remember that fines only tend to be imposed as a last resort, or issued in cases where the data breach was so large or reprehensible that a punitive fine was absolutely necessary.

It is equally helpful to remember that 99% of what you have heard about GDPR is scaremongering rubbish about what privacy professionals came to call "finesfinesfinesfinesfines!" In fact, any article about

data protection or privacy that mentions fines at all is a sign of a bad article or, more likely, one trying to drum up business.

In the years I spent getting digital professionals ready for GDPR, the first question asked in any session was "What happens if I don't comply?" That question was often phrased another way: "Can I get away with not complying?" And, for the record, I even heard, "If Europe fines us, we'll just pay the fee." Good data protection practice is not about avoiding fines, it is not about a negative obligation to comply "or else" receive a fine, and it is not about gloating that you are wealthy enough to get away with breaking the law. Data protection practice is about protecting users from the misuses of their data and the abuses of their human rights. Data protection practice is not about sticking it to the man and punishing your users instead.

ENFORCEMENT IN THE EUROPEAN SYSTEM

One thing I often found myself explaining to conference audiences is that privacy enforcement in the European system is not carried out on a "parking warden" model. Contrary to what some scaremongers might tell you, there are not squads of data protection regulators wandering the streets of the web looking for violators to ticket and fine on a quota system. (What can I say? Some people watch too much TV.)

In most cases, a privacy regulator will only respond to a complaint or a concern raised by the public or the media. If you are a large company or a household name, it goes without saying that the regulator will take a more proactive approach, and will be in regular contact with your data protection officer (more on that in Part Two).

All members of the public are welcome and encouraged to contact their data protection regulator to report concerns. The paradox there, of course, is that the public will only do so if they have both a grasp of their fundamental privacy rights as well as a sense that those rights, and the laws which safeguard them, have been violated. That's a big ask for your everyday web user.

So activists, privacy advocates, and academics often take the lead in reporting concerns and filing cases with privacy regulators; indeed, it's not uncommon for them to provide

research and analytical studies which go far beyond anything the regulators would have been able to produce on their own. One of the most vocal activists, Max Schrems – whose persistence in not taking no for an answer has inspired privacy advocates everywhere – has created a site which tracks all GDPR enforcement activity.[6]

It should go without saying that if you have a concern about the way a company is failing to safeguard your privacy, either by the spirit or the letter or the rule of the law, you should contact them first to start a constructive dialogue before you escalate the issue to your regulator. The company may be able to assuage your concerns. It's just as likely they will turn you into a privacy activist overnight.

PRIVACY ENFORCEMENT IS NOT A GRIEVANCE MECHANISM

Privacy regulators, for all their occasional shortcomings, are not dumb. Every day they receive data protection complaints from members of the public who are not really interested in privacy. They know these complainants are using the system to hit back at a service provider for some other gripe, grudge, or grievance.

Under most data protection laws, regulators are under no obligation to respond to a complaint – known as a vexatious request – that has been filed in bad faith, which is really

6. https://gdprhub.eu/

about another issue, or which has clearly been filed out of malice or harassment. They will respond with a polite request and close the ticket (so to speak). Provisions against vexatious requests also extend the other way to cover service providers. A company is under no obligation to honor or respond to privacy complaints that are quite clearly weaponizing data protection law for other purposes.

That doesn't stop people from trying. For example, in 2019 there was a coordinated social media campaign to flood a gaming company with subject access requests in protest against their ejection of a player for his political stance. Yet those submissions, as vexatious requests, went straight into the bin. The campaign was a pointless action, and the protesters would have known that if they had not cherry-picked the parts of GDPR they wanted to hear.

No matter how angry you may be about a company's behavior or an issue which matters to you, abuses of privacy law as a grievance mechanism aren't smart and they aren't clever. They're a childish waste of everyone's time, and you are under no obligation to lend them yours.

ePRIVACY

GDPR, which concerns data at rest, is only half of the European privacy regime. The other strand of the double helix is a law on data in transit called the ePrivacy Directive. You

know it, somewhat incorrectly, as the "cookie law," and it's this law, *not* GDPR, that created those cookie consent pop-ups we've all grown to hate.

The ePrivacy Directive – or, for the techlaw geeks, Directive 2002/58/EC on Privacy and Electronic Communications, aka PECR (and yes, that's pronounced "pecker") – was a law dealing with marketing consent, secure communications, and, yes, cookies. It has been revamped several times, most notably in 2012, to form the shape of the cookie law we know.[7]

In fact, it has been revamped so many times that something new is needed. As this book goes to press, the Directive was nearing the end of a revision process that will create a refreshed set of regulations on cookies, consent, and software updates.

Or so we thought!

The draft law has now been fought over for eight years, with special interests on all sides rendering the debate a soap opera that has tested the patience and sanity of even the most dedicated privacy professionals, including your friendly neighbourhood privacy book author. And just when it looked like there might be a glimmer of hope for progress, the pandemic brought the legislative train to a screeching halt. Again.

7. The UK ICO has some useful guidance on the existing law: https://smashed.by/cookies

When the revised law is eventually finalized, check with Smashing Magazine online to learn what compliance obligations will have changed, and how. For now, we can only deal with the existing ePrivacy law. After all, if you serve customers or users in Europe, you are every bit as bound to it as you are to GDPR.

The existing law requires you to:

1. Inform your users of the cookies you are using, via your privacy notices.

2. Explain what function each of these cookies serves and what they do, whether that's something good like remembering their preferences or not so good like feeding in to an ad network.

3. Provide your users with a means of consenting to having those cookies stored on their device, and a means of opting out on a granular level.

It's important to note that it's not just about cookies. Any form of tracking, such as a Facebook pixel or the beacon in an e-newsletter, falls under this law. They require consent and opt-in all the same. And it isn't just about pop-ups on a monitor or mobile screen. Any sort of device engaging in tracking – whether that's a wearable or a smart TV – falls under this law too.

And yes, *third-party analytics require active opt-in consent too*.

There are different rules applicable to session cookies and permanent cookies, and there is also a helpful delineation between essential first-party cookies (such as the ones that remember what is in a shopping cart, or keep a user logged in) and non-essential third-party cookies. We'll dive into the semantics of this in Part Three.

But let's cut to the chase of what you really want to know here: *will the revamped law end those cookie pop-ups*?

Well, you're a bit late to the game. Laws and regulations are made by the people who show up. Design and development communities have been absent from the years of debates and negotiations that are shaping the revamp of the cookie law. Browser manufacturers and adtech companies, by contrast, haven't missed a minute. This means that the law is a tug-of-war between an EU trying to advocate for user privacy, and parties whose intentions are, shall we say, not so user-centric trying to steer the revamp towards their own interests.

What we do know is that the revamp will likely set a series of design constraints for what any consent mechanisms should or should not require. So that's why it's so important for you to understand that the infuriating cookie pop-ups, dropdowns, modals, and overlays were not the EU's fault.

What GDPR and ePrivacy mandated was consent mechanisms, not the appearance or the functionality of the mechanisms themselves. The parties responsible for vandalizing the web with awful consent mechanisms were the ones who had the most to lose from it: the adtech industry. They made consent mechanisms. People who care about privacy didn't. And, for what it's worth, the explosion of really bad cookie consent pop-ups that appeared ahead of GDPR were a completely unnecessary misunderstanding of what GDPR required.

So to anyone who blames the EU for cookie pop-ups, remember two things.

One: the people you really need to be angry with are the profiteers who abused the system to their own ends, not the people who tried to do something for user privacy.

And Two: if you don't like the cookie consent mechanisms that exist, contribute to an open-source project or initiative that aspires to make better ones; or better still, design your own mechanism based on the good work that privacy advocates have already done for you. Be a part of the solution, not the problem.

The US Privacy Approach

Now let's cross the Atlantic. You will often hear the US privacy system referred to as a "patchwork" of laws. As an occasional patchwork quilter, I personally hate that reference, because I have never sewn a quilt with large holes in it.

Let's start by clarifying one very basic term: "data protection" is a largely European expression. The term you're more likely to hear if you live or work in the US is "data privacy." It's the same thing.

That, unfortunately, is the only commonality. The US does not uphold a universal right to privacy, nor is there a single omnibus data protection law as in the European system. What privacy law there is in America tends to take three forms:

1. Sectoral regulation, such as health (HIPAA), children's data (COPPA), and so forth.

2. State regulation, such as California, Vermont, and so forth.

3. Consumer protection regulation, such as the consent decrees against Facebook for violating their terms of service. (It's notable that Americans, almost by default, use the term "consumer privacy"

rather than just "privacy." It's a subconscious declaration that privacy is viewed as a transaction rather than a human right.)

Users who experience the misuses of their data, and who find that those misuses are not covered under one of those regulations, may find themselves with no rights or recourse.

Additionally, without an omnibus privacy law to define concepts and principles, the US view of privacy does not have the common definitions of consent or user rights which exist in the European model.

If you're starting to think that this means the US privacy model is pretty much "anything goes," you're not wrong. I love what the author Woodrow Hartzog said about the US approach to privacy, a quote which reflects both that "anything goes" approach as well as the cultural primacy of free speech:

> *Privacy law in the United States [...] tolerates gossips, paparazzi, peepers (so long as they are "in public"), trolls, and data black boxes. But one thing privacy law will not tolerate is a liar. Prohibitions on deceptive representations and omissions are the foundation for data protection law in the United States.*[8]

8. Woodrow Hartzog, *Privacy's Blueprint: The Battle to Control the Design of New Technologies*, (2018), 67. https://smashed.by/privacysblueprint

In other words, the US approach has tended to be: do what you want with people's data – just don't lie about it. Legal types tend to refer to this as a "notice and choice" regime: what matters is the contractual relationship between the parties, not the data itself.

That is set to change in the next few years, but for now, let's review the state of play. Look on the bright side: it makes for a much shorter chapter to read.

CCPA

In lieu of a federal privacy law, the most important American privacy regulation is a state law, the California Consumer Privacy Act, known as CCPA. In many ways it is as far-reaching as Europe's GDPR – after all, the state of California is the world's fifth-largest economy – so any privacy rules made here go far beyond California's borders.

CCPA took effect on January 1, 2020 and became enforceable on July 1, 2020. A series of amendments called the California Privacy Rights Act (CPRA) was approved in November 2020, and take effect on January 1, 2023 but apply retroactively to data collected from January 1, 2022.

CCPA aimed to grant California residents a set of fundamental privacy rights similar to GDPR's user rights, re-

gardless of where the data about them was held. However, unlike GDPR, it is not a universal law across sectors and situations, nor does it attempt to define any sort of legal basis required for collecting and processing data. Put simply, CCPA is about the disclosure of how data is being used, not protections of that data from abuse.

CCPA applies to any business with California users, or customers, which meets the following criteria:

1. They are a for-profit business with gross revenues in excess of $25 million OR

2. Alone, or in combination, they hold data on over 50,000 households' consumer devices, OR

3. They derive over half of their revenues from selling consumer personally identifiable information.

4. CCPA does not apply to nonprofits.

(Remember our chat about differing cultural approaches to privacy? This is an example of the American approach that qualifies it as a function of consumer protection grounded in a contractual relationship, and not as a function of privacy grounded in a fundamental framework of human rights.)

Businesses that prepared well for GDPR would have found themselves about 75% ready for CCPA, with some supplementary localization required to catch up.

What does CCPA require?

1. Businesses falling under CCPA are required to display a privacy notice that explains a person's consumer rights of access, information, and deletion, as well as the method a consumer is required to use to invoke them. (We'll discuss this in Part Three). This should also include a means of opting out of cookie/pixel consent, although CCPA does not require active opt-in.

2. CCPA requires businesses to delineate consumer data into three categories:

    a. data they have collected

    b. data they have sold

    c. data they have disclosed for a business purpose over the previous twelve months

3. If no personal information was sold or disclosed for a business purpose, the privacy notice must explicitly state so.

4. Consumers must have easy access to a dedicated page called "Do not sell my personal information," which allows them to opt out of the sale of their personal information. That opt-out is only valid for twelve months, at which time the business can ask the consumer to opt out again or face the sale of their data.

CPRA establishes a California data protection regulator, arguably the first in the modern American privacy context. In keeping with the American approach to resolution through litigation, CCPA includes a private right of action for consumers to seek to recoup damages directly from a company.

OTHER STATE LAWS

As of this writing, thirty-seven out of fifty states have proposed, introduced, or passed some form of state-wide privacy law. Some of these bills deal with user rights, some deal with business obligations, and some of them deal with both. Some of them are viable; some of them could use some improvement; and some of them will be merged into other initiatives.

We won't make any attempt to keep track of all of these proposals in this book, although you can try – if you dare! – by bookmarking https://smashed.by/legislationtracker

Now obviously, each of these proposals – even those that stumble and fall – represent some form of progress towards a healthier respect for privacy in the US. But the problem is obvious: there could be fifty wildly divergent laws that a single company might have to follow, an impossible task for even the best of us. And it also means that a US user's privacy rights will continue to be entirely contingent on either the state where they live, the state where the service they use is based, or on neither of them at all.

It's almost as if something bigger is needed.

THE FORTHCOMING US FEDERAL PRIVACY LAW

As this book goes to press, a federal privacy law – one single law to create a baseline for data protection across the US – remains a pressing topic in Washington. In recent years, dozens of draft privacy laws have been proposed, put forward by politicians on all sides of the spectrum, and informed by countless proposals and studies from across the tech sector. Indeed, things have even reached the surreal point where tech companies are begging the US government to create a federal privacy law, to save them from having to follow dozens of state laws and make up the rest on their own.

As if to prove the point, the coronavirus outbreak emphasized the need for a federal privacy law like never before.

While everyone – from the federal government to states to private healthcare companies to billionaire tech bros to open source volunteers – was scrambling to do *something*, they were doing so with no common, accountable, or transparent definition of user privacy and how to protect it. What has ensued is a nationwide real-time experiment where everyone, with the best will in the world, is making it up as they go, while creating an entirely new mess of privacy problems which will have to be cleaned up down the road. European developers, by contrast, have been given a legally compliant toolbox[9] to use in creating privacy-conscious pandemic applications, and can jump right to the important work as a result.[10]

What has also ensued has been companies like Google and Apple collaborating to create contact tracing apps based on privacy principles which *they themselves* are drawing up – which makes them, and not the federal government, the de facto American privacy regulators. While it's easy, and somewhat lazy, to accuse tech giants of acting like sovereign nations – as many often do – they just want to make shiny things for people to use. Engaging in actual international governance is not in their business plan, and at the end of the day, none of them want it to be their job to create, enforce, and police global privacy. That's Washington's job.

9. https://smashed.by/eucorona
10. I had the privilege of reviewing NHS Scotland's data protection impact assessments for their Covid Test and Protect and venue check-in apps. The process was a great example of how it's possible to use data protection law as the foundation for user-centric products – and to also work cooperatively with civil society as a healthy form of accountability for your privacy practices.

Make no mistake about it: **a federal privacy law is coming in the next few years.** It must. The questions are what it will look like, what it will cover, who it will cover, and what will be missing. The lessons being learned through the coronavirus pandemic, and the mistakes being made in real time, will provide the impetus as well as new perspectives that the issue has lacked thus far. While the ensuing federal privacy law is not likely to be as comprehensive as GDPR, it will still involve a lot of work, and a lot of debate. We can make a few predictions about how that debate will play out.

First, because the US does not uphold privacy as a human right, the federal privacy law is likely to be consumerist: privacy will be qualified as a function of a commercial transaction, regardless of whether money was exchanged. We are already seeing this in news stories about a "federal consumer privacy law" – that C word, "consumer," is always there. The federal law will not establish privacy-centric human rights: it will only establish "consumer" ones. This will leave many situations, and privacy violations, uncovered and unaccountable.

Second, the US is a litigious society. The right of individuals to sue companies will be much more prominent than it is in the European model, well beyond the class action law-

suits we already see today. Private rights of action will be as important in any American privacy legislation as user rights are elsewhere. While this will empower people with new tools to protect their privacy, it will also give rise to "privacy trolls," the cousins of the "accessibility trolls" who have already exploited human rights laws for personal profit.

Third, a privacy law needs a privacy regulator. Who will take on that role – be it an existing body or a new one – as well as how they will evaluate privacy violations, and what enforcement is carried out, will be highly contentious issues in a political environment which seeks to shrink the state rather than grow it. We'll talk about the likely candidates for the job shortly.

Finally, federal laws, by nature, override state privacy laws. Yet state privacy laws, at the moment, are all the US has. And *because* of the lack of a federal law, some state laws have gone much further than anything created in Washington. This means it may be possible, at the end of the whole messy issue, for the US to end up with a federal privacy law that is *weaker* than some current state laws, and may even claw back some of the privacy rights granted within them.

If you are a US web professional, it will be important to stay on top of these developments, and to participate in the shaping of the eventual law; I'll talk about this later on in the

book. But I can't stress this enough: **the lack of a federal privacy law should not mean the lack of a healthy and accountable approach to user privacy**. This book will give you the tools you need to get you there.

PRIVACY SHIELD AND TRANSATLANTIC DATA FLOWS

Let's stay on the subject of politics.

One of the fundamental principles of EU data protection law, both past and future, is that personal data cannot be transferred outside of the EU to a third country unless that country ensures an equal and adequate level of data protection.

This means that a European person's data must be safeguarded by an American (or any other international) company as if that data was still in Europe under EU data protection rules. And this means that those international companies must implement a data protection system equal and adequate to GDPR for their European users' data.

Most of the technology giants which dominate our data lives, as you know, are based in the US, as are many essential SAAS providers. The size and scope of the data constantly flowing between America and Europe led to the need for a standardized means of ensuring compliance with EU data protection law.

That led to Privacy Shield, a framework provided by the US Department of Commerce to support American businesses handling European data. Privacy Shield allowed US businesses receiving European personal data, as well as the European businesses sending it, to self-certify that all parties adhere to EU data protection principles. The common framework allowed businesses to work to established guidelines rather than having to come up with them on their own.

However, in July 2020, concerns over the US surveillance apparatus's access to European people's data, which bypassed the safeguards in the Privacy Shield framework, led to the Privacy Shield system being invalidated by the Court of Justice of the European Union.

This means that US businesses collecting or processing European data can no longer use the Privacy Shield system, and must make alternative arrangements.

To keep your data legally flowing from the EU to the US and back again, you'll need to do two things. First, you'll need to make sure your data has safeguards against surveillance.

Then, you'll need to safeguard yourself and your business with alternative means, such as standard contractual clauses.

Max Schrems, the privacy activist whose work brought about the ruling, has provided some FAQs for both requirements.[11]

As of this book's publication date, a new transatlantic data sharing agreement is being hammered out "in principle" in Washington and Brussels.[12] "In principle" means don't wait for the details, and don't count on it to come into effect anytime soon.

> Structuring your international data transfer processes around the Privacy Shield standards, regardless of the invalidation of the actual system, has two more advantages. The first is that given the lack of a comprehensive US privacy law, the compliance process is as good an opportunity as any to shape your work around an accountable data protection framework. Doing something is better than doing nothing. The second advantage is that when the US federal-level privacy law does eventually come into play, healthy compliance to

11. https://smashed.by/eucompanies
12. https://smashed.by/transatlanticflows

European standards is likely to see you halfway there – if not ahead of the pack.

REGULATORS, OR LACK THEREOF

So who are the data protection police in America? Nobody, really. Without an omnibus federal privacy law, regulation of privacy law in America becomes a function of the law used to approach it. If that is not through a sector- or state-specific privacy law, it becomes a matter of squashing privacy into contract, property, or tort law. That also means the responsibility for enforcing privacy falls to individuals acting on their own initiative, not to a regulator acting out of a statutory duty.

The class action lawsuit filed against video conferencing platform Zoom is a classic example of that. The lawsuit was filed by a private shareholder who accused Zoom of failing to disclose that the platform did not have end-to-end encryption and had overstated its privacy standards. In other words, their weapon was contract and corporate finance law; personal privacy and user security were merely background noise.[13]

To date, the closest bodies the US has had to privacy regulators are the Federal Communications Commission (FCC), a

13. https://smashed.by/zoom

body originally set up in the 1930s to regulate radio frequencies, and the Federal Trade Commission (FTC), a body set up a century ago to handle antitrust issues. Like collaring Al Capone for tax evasion, they can only deal with privacy issues through other means. The FTC's $5 billion fine against Facebook in 2019, for example, was for infringements of privacy as a violation of consumer protection law. That approach, unfortunately, reinforces the US perception of privacy as an advanced legal issue rather than one based in simple human rights. Until an omnibus federal-level privacy law exists in the US, a person whose data has been leaked, or feels their human rights have been breached, has to find another avenue to seek recourse.

The lack of a privacy law or data protection authority also means that there is no single easy place for US web professionals to go for guidance on privacy practice. That information gap has to be filled elsewhere, and it usually means being told to "consult with your legal counsel." In the European system, thanks to data protection authorities and data protection officers, a lawyer would be the last stop for guidance. Even then, it would only be for a specific reason; for example, double-checking the contractual aspects of a data-processing agreement. In the US, by contrast, because privacy is shoehorned into a contractual approach without regulatory guidance, a lawyer becomes the default first stop for privacy – despite very few of them being privacy lawyers.

So if your work truly necessitates a lawyer, it's critical for you to find one who understands privacy beyond having sat through a lunch seminar; look for a qualified privacy lawyer. Before you do, though, take this advice on board: **you do not need a lawyer for your everyday privacy work, and anyone who tells you so is scaremongering**. Lawyers absolutely have a role to play in certain advanced aspects of privacy law compliance, but integrating user-centric privacy into your work is not their job. It's yours.

> When speaking with American audiences, I often hear a misperception that the European privacy model and laws such as GDPR are not working, because they have not seen big court cases or fines. That expectation comes from the combative litigious approach which is standard practice in the US. The European regulatory model tends to work opposite to that: it's rather quiet and keeps its head down. Put another way, Europeans don't do podium-thumping press conferences to announce huge criminal penalties. Nor would they: because European privacy

regulators work on a cooperative basis, court cases are the rare last resort, not the first port of call. That does not mean that action is not taken, companies are not punished, or fines are not issued. Far from it. The absence of big headlines, big press conferences, or big criminal cases, as would happen in America, does not necessarily mean the European regulatory system is not working as it should.

Privacy through Soft Regulation

It's worth taking note of non-legal privacy standards. After all, in the absence of a legal framework, privacy can also be addressed through soft regulation, which means an internal agreement to follow an agreed standard such as an ISO framework or an industry code of conduct.

Although soft regulatory standards can provide a healthy foundation for good privacy practice, they are not externally accountable to any legal system or data protection regulator. In other words, they are only as good as the people using them. For this reason, soft regulation should

never be used as a substitute for legal compliance; in fact, companies using these standards will need to work *even harder* to keep themselves on top of the task.

INDUSTRY CODES OF PRACTICE

GDPR encourages organizations that oversee many companies, such as industry bodies or trade unions, to devise codes of conduct for best data protection and privacy practice. These codes would be guidelines for healthy privacy compliance, written around the specific needs of that industry or sector, which companies could use as their standard of accountability.

Organizations that devise these codes will need to have them approved by their national data protection regulator. The organization would then act as a sort of intermediary regulator, supporting members to help them reach a healthy level of compliance in lieu of using the data protection regulator as the first point of contact, and helping them to ensure that their ongoing data protection practices are solid within their industry context.

While the industry code of conduct plan sounds like a great idea, to date only two industry bodies and sector groups in Italy have ever done it. And until the web profession matures enough to become an organized industry, a developer-specific code of conduct is an impossibility.

Standards

Two soft regulatory standards worth mentioning are the US NIST framework and ISO standards.

NIST PRIVACY FRAMEWORK

The National Institute on Standards and Technology, a US government body that does exactly what its name suggests, has recently released a comprehensive framework for organizations to use to mitigate privacy risks on the enterprise level.[14]

The framework, which is entirely voluntary and highly technical, sets forth a series of difficult, open-ended questions – which is exactly how good data protection practice should work – on how companies identify, govern, control, communicate, and prevent privacy risks.

In the US privacy context, NIST's framework is something, and something is better than nothing. US companies handling substantial amounts of data should consider the framework a healthy model to follow for both CCPA and GDPR compliance, and as a means of getting ahead of the compliance requirements likely in any inevitable future US privacy legislation.

14. https://smashed.by/nist

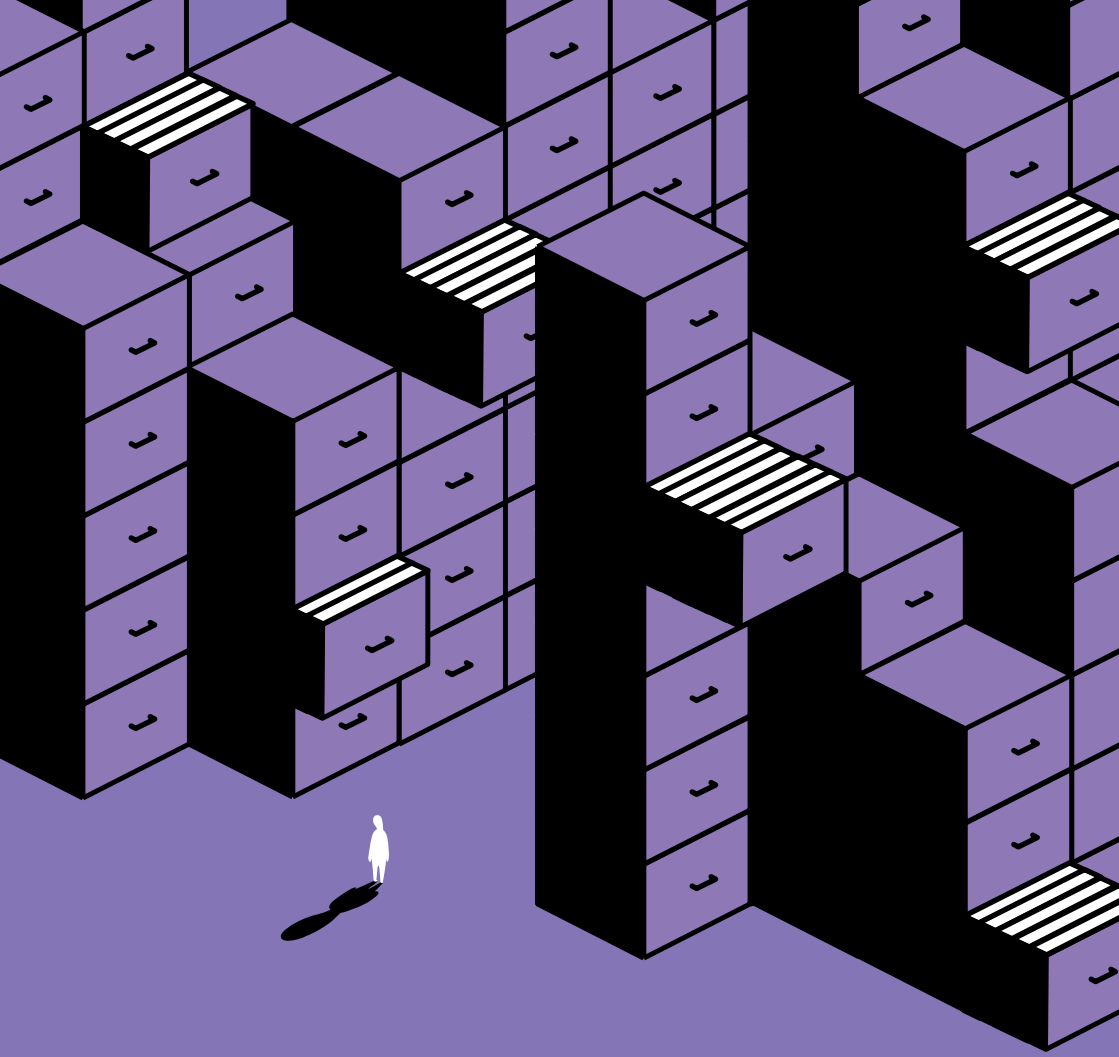
ISO Standards

Outside GDPR, many larger companies use ISO 27001 in information security management. While it is not a substitute for GDPR compliance, it can provide the baseline for about 75% of GDPR compliance issues, and certification in ISO 27001 can put a company in a good light with data protection regulators.

There is also an ISO standard (31709) for Privacy by Design (PbD) for consumer goods and services.[15] There is no need, however, to wait for that standard in order to implement good PbD practice into your workflow.

Speaking of Privacy by Design, let's move on.

15. https://smashed.by/consumerprotection



PART TWO

Privacy and Your Work

“Tech people rarely, if ever, have a sense of the broader applications and policy implications of the projects to which they’re assigned. […]

In retrospect, maybe that’s what got us here.”

—Edward Snowden, *Permanent Record* (2019)

PART TWO

Privacy and Your Work

Now that you understand the fundamental concepts behind privacy and data protection, as well as the legal frameworks which safeguard them for many of your users, let's discuss how to integrate them into your work. We'll do so from the concepts and expectations of the European data protection framework, not because it is a legal obligation, but because of the strong basis it provides for a user-centric approach to privacy.

Privacy in Project Management

In the following pages, we make some very broad assumptions. We will presume that the users who visit your website, or use your app, or sign up to your service, expect to have their privacy protected. We presume that they do not expect bad things to result from their use of what you have built.

We also assume, however, that they are generally passive individuals who will not speak up when their privacy is at risk, or if the service you provide does not give them the safeguards and options they need to protect it.

The way you approach that last presumption will ultimately serve as the measure of how well you build the web.

PRIVACY BY DESIGN

The foundation of a healthy approach to privacy in project management, regardless of the presence or absence of a legal obligation, is using an accountable framework to structure and measure your work. Fortunately there's one ready and waiting for you, and there always has been. It's called Privacy by Design (PbD).

The Privacy by Design framework[1] was developed in Canada way back in the 1990s, and it hasn't aged a day. It is built around simple, common-sense principles which, if implemented correctly, can help to prevent many privacy problems from occurring. The principles nudge teams to ask open-ended questions about the privacy implications of their output, and to also consider the wider political and ethical environment which exists around their users.

Privacy by Design has always been available for anyone to adopt and use, but under GDPR, data protection by design and by default is a legal requirement. The PbD principles are the foundations of good data protection practice, so the PbD principles should become your chapter and verse.

1. https://smashed.by/privacybydesign

The framework has seven principles:

1. **Privacy must be proactive, not reactive, and must anticipate privacy issues before they reach the user. Privacy must also be preventative, not remedial.**

   This means that you should do whatever it takes to stop privacy issues from ever arising in the first place. In doing so, you should not make it your users' responsibility to deal with privacy problems that you have created for them.[2]

2. **Privacy must be the default setting. The user should not have to take actions to secure their privacy, and consent for data sharing should not be assumed.**

   This means that all privacy settings should be maximized from the moment a user accesses your site or service. If that is in something like an account settings area, all privacy options must be set at their highest level on account setup, and users should have to make an active choice to diminish their privacy. On a consent

2. The process of placing the responsibility on users to safeguard their own privacy is known as "privacy labor", and it is a concept which we should all discuss more. https://smashed.by/privacylabour

pop-up, all third-party sharing should be switched off by default, regardless of the legal basis.

3. **Privacy must be embedded into design. It must be a core function of the product or service, not an add-on.**

   This means that privacy options should be in a product's core. They should never be an add-on, a widget, a plug-in, or a module. And privacy options should absolutely never require a premium payment.[3]

4. **Privacy must be positive-sum and should avoid dichotomies. For example, PbD sees an achievable balance between privacy and security, not a zero-sum game of privacy or security.**

   This means that users should never have to choose a lesser standard of service if they want to exercise their privacy rights. Nor should they have to delete an account if a service changes its terms and conditions and requires the user to consent to diminish their privacy to continue using the service. (This, sadly, is exactly what too many services do.)

3. Zoom's notorious announcement that it would offer end-to-end encryption only to premium paid users is exactly how not to do privacy by design.

5. **Privacy must offer end-to-end life cycle protection of user data. This means engaging in proper data minimization, retention and deletion processes.**

   This means collecting as little data as is required, only using it for the sole purpose it was collected for, only storing it for as long as it is needed, and deleting it when it is no longer needed.

6. **Privacy standards must be visible, transparent, open, documented, and independently verifiable. Your processes, in other words, must stand up to external scrutiny.**

   This means disclosing all your uses of data, as well as third-party sharing, in your privacy notices; making yourself accountable through the honoring of user rights; and making yourself accountable to data protection regulators.

7. **Privacy must be user-centric. This means giving users granular privacy options, maximized privacy defaults, detailed privacy infor-**

mation notices, user-friendly options and clear notification of changes

This means remembering that the things you make on the web aren't about you – they're about your users. Give them choices, give them options, give them the means to exercise their rights, give them control panels, give them settings, give them information, give them clarity, give them assurance, and give them your consideration.

You may be using many of these principles in your work already, but if you aren't, they give you a fantastic starting point for putting user privacy first and foremost.

The UK's data protection regulator, the Information Commissioner's Office (ICO), has suggested a few open-ended checkpoints[4] you can use to evaluate your PbD health:

- ✓ We consider data protection issues as part of the design and implementation of systems, services, products and business practices.
- ✓ We make data protection an essential component of the core functionality of our processing systems and services.

4. https://smashed.by/ico

- ✓ We anticipate risks and privacy-invasive events before they occur, and take steps to prevent harm to individuals.
- ✓ We only process the personal data that we need for our purposes(s), and that we only use the data for those purposes.
- ✓ We ensure that personal data is automatically protected in any IT system, service, product, and/or business practice, so that individuals should not have to take any specific action to protect their privacy.
- ✓ We provide the identity and contact information of those responsible for data protection both within our organization and to individuals.
- ✓ We adopt a "plain language" policy for any public documents so that individuals easily understand what we are doing with their personal data.
- ✓ We provide individuals with tools so they can determine how we are using their personal data, and whether our policies are being properly enforced.
- ✓ We offer strong privacy defaults, user-friendly options and controls, and respect user preferences.

- ✓ We only use data processors that provide sufficient guarantees of their technical and organizational measures for data protection by design.
- ✓ We use privacy-enhancing technologies (PETs) to assist us in complying with our data protection by design obligations.
- ✓ When we use other systems, services or products in our processing activities, we make sure that we only use those whose designers and manufacturers take data protection issues into account.

Pay attention to that last checkpoint, because we're going to come back to it.

PRIVACY IMPACT ASSESSMENTS

A framework, be it Privacy by Design or anything else, is only as good as the documentation which validates it. Where PbD is concerned, that documentation is called a privacy impact assessment, or a PIA. In certain contexts, you'll hear it referred to as a data protection impact assessment (DPIA), and while the semantics may differ, the broad concepts are the same.

Whatever you call it, it's the most important process you will engage in to protect yourself, your users, and your work.

A PIA is the way to document the issues, questions, and actions required to implement a healthy PbD process into a project, service, or product, and to make sure that your work proceeds with user privacy placed first and foremost. Put another way, it is the series of questions you should ask in any case before you do a single click's worth of work, and it's the documentation you create in response to those questions to keep yourself accountable.

PIAs proved their worth during the rollout of coronavirus tracking apps, with digital rights groups insisting – and then litigating – for governments and private companies to publish their PIAs before rolling out the apps at scale. Any reluctance to publish those PIAs must be taken for what it is. It's a great example of how the European privacy framework is doing exactly what it was meant to do by giving the public a means to evaluate how seriously their privacy is being taken; or, as is more likely, taken away.

In your PIA, you will use the PbD principles to:

- Outline what personal data you will collect, and why.
- Outline whether you can collect that data, both as a function of legal compliance and of ethics.

- Outline how you will safeguard user privacy in their interests.
- Outline how you will communicate with users about your data collection, its impacts, and their rights.
- Outline how you are ensuring accountability for user protection within your organization or project.

Do I Need a PIA?

Under most implementations of GDPR, a PIA is a requirement for a project that:

- captures a substantial amount of user data.
- captures high-risk or sensitive data such as location, biometrics, etc.
- engages in profiling or aggregation of data with third-party sources.
- concerns a product or service geared towards children.

My rule of thumb is that if you think you need one – GDPR or not – you probably do.

In the event of a public complaint or an enquiry from a data protection regulator, they can and will ask to see your PIA.

If your response to that question is "What's a PIA?" you will then have two problems. Some regulators will also request to see the PIA of a high-risk project before a public concern has been raised; indeed, some very high-risk projects will require you to proactively submit a PIA.

For that reason – whether GDPR applies to you or not – I highly recommend conducting a PIA before commencing any project. I also recommend running a retrospective PIA process on any data-intensive projects you have created without one, and making any adjustments to your work accordingly.

Most data protection regulators recommend that you create your own PIA template unique to your workflows or business models.

What's in a PIA?

The questions you include in your PIA should not be too prescriptive or narrow; rather, they should follow seven broad areas and themes:

1. Identify Why You Need a PIA

Describe your project, what it does, what sort of data collection and processing is involved, and what aspects of that have created the need for a PIA.

2. Describe the Information Flows

Map out your data collection and processing activities. First, you should be prepared to list the flows of information into, around, and out of your project or service. This needs to include flows between the:

- user to the service provider
- user to user
- service provider to user
- user to third parties
- service provider to third parties

You should include active data (such as user inputs) as well as passive background data (such as third-party services, including social media sharing.)

Having listed your data flows, you need to take a deeper dive into the processes and relationships around it. This should include:

Describing the nature of what you're doing: How will you collect, process, retain, and delete user data? Where are you getting that data from? Are you sharing it with anyone?

Who else has access to it? Do any of these activities involve high-risk actions?

Describing the scope of what you're doing: What sort of data are you collecting and processing? Is any of that data considered to be in a special category or high-risk? How much data is there? How much of it are you using? How often are you using it? How long are you keeping it? How many individuals or households is the data about? Where are your users located – and what legal implications does that bring?

Describing the context of the processing: What is the nature of your relationship with the individuals in the data? What rights and control will they have over your uses of their data? Do they know and expect that you are using their data in the ways that you are? Are any of these data subjects children or people considered vulnerable? Are there any current issues of public concern, such as the pandemic or a child protection concern, that you should consider?

3. Discuss the Risks

In this section, you'll document the privacy and data protection risks to users, to the organization (that means you and your business), and to the technical and systems setups which hold the data.

Describe how you will consider everyone involved: How will you seek the views of the people who need to consider the risks in the data? If you're not consulting with them, can you justify the reason why not? Who in your organization needs to be aware of this? What about your security team, your board, and your legal department? Have you discussed the data risks with your third-party processors, and have you verified that they are safe hands for the data?

Describe how you will meet legal compliance: Is your data collection and processing necessary and proportionate? What is the data retention and deletion life cycle? Can you get the same data in a more privacy-friendly way? What is your legal basis for processing? Have you ensured that your third-party processors have signed data processing agreements? How are you legally safeguarding international transfers? How are you providing for user rights?

4. Solutions

Identify and evaluate how you plan to mitigate all of the risks you've identified, both passively and actively. Be as specific as possible, noting roles and responsibilities.

5. Outcomes

Here's where you document and record the outcomes of your PIA process. Accountability comes into play here. The PIA should be signed off by a responsible member of the team, and preferably one working in a leadership role.

6. Integration

Put that document to work! Integrate the opportunities and constraints you identified in the PIA process into the project or service's life cycle.

7. Communication

Your PIA should be a living document available to everyone who participates in or works on a project, including external contractors. Update your PIA often, keep it in an accessible location, and communicate any changes to everyone on the team.

Your PIA does not have to be made public.

It goes without saying – and yes, I have seen this happen – that if there is something going on with user data in your project that you do not want to document in your PIA, the problem is not the PIA.

> The traditional approach to privacy impact assessments has presumed teams working in corporate-style company structures where roles are clear and goals are shared. Yet much of the work you do will take place in contributory settings, such as

open-source software initiatives, collaborative projects, and even hackathons. It's important to remember that a PIA isn't just a bureaucratic tick-box for corporations.

If the work you are putting into the world involves any of the mandatory requirements for a DPIA, or is likely to be controversial, your project should take the time to create one and make it public. Collaborative and open-source project PIAs should note who you are, where you come from, what your project governance structure is, and who funds you. If you don't provide that information transparently, people will draw their own conclusions.

DATA AUDITS

It's easy to integrate PbD and PIAs into your work going forward. Looking back at the data life cycle can be a bit trickier. In all of the work I did with digital professionals and agencies to help them get ready for GDPR, one of the most surprisingly positive aspects was the opportunity it presented for them to conduct data audits.

A data audit is an inventory of what data you hold, why you have it, how long you've had it, what you do with it, why you still need it, and whether or not you should get rid of it. It's where you map out where your data comes from and how it got there. (If you don't know where your data came from, how it got there, or why you need it, that might be a clue about why you needed an audit.)

When you are making your inventory, be ruthless about distinguishing between the data you have, and the data you need. That need must be present and active: data you have that you think might be useful someday for a yet-undetermined purpose is not data that you need.

The data audit process applies to individual projects as much as it does to your businesses as a whole. It applies to physical files as well as virtual ones. It applies to in-house records as well as those held by your third-party suppliers and partners. And it should apply to people too: who exactly has access to the data? Who used to have access? Do you still have active login accounts for employees and contributors who left years ago? You might be surprised at what you find.

A data audit is also a great opportunity to bring out your dead. Ahead of GDPR, I had clients discovering yellowed storage boxes, ancient Zip drives, and mystery file folders for projects nobody could remember. They also sifted through cloud storage, third-party accounts, old desktops,

SAAS applications, and hosting accounts to clean out the flotsam and jetsam of project development – which inevitably included database backups full of customer data. There was no commercial, legal, or practical reason for any of that data to still be on file. Purge it, delete it, and recycle it. It feels great.

> When conducting your data audit, you are not obliged to comply with one law by breaking another. You can, and should, keep any data you are required to keep for other legal compliance purposes, such as taxation, employment, or human resources, indefinitely.

DATA PROCESSING AGREEMENTS

Recall our PbD checkpoint which said:

> *When we use other systems, services or products in our processing activities, we make sure that we only use those whose designers and manufacturers take data protection issues into account.*

Taking all the privacy precautions in the world does not mean a thing if you are working with suppliers, partners, or third-party providers – in other words, your data processors – who take a sloppier approach to user privacy. Many of the high-profile data breaches we have seen over the years, such as the Equifax breaches of information about pretty much anyone in America who is either alive or dead, have been at the hands of the data processors who held personal data rather than the data controllers who owned it.

Because of that, one of the things I love about GDPR is that it requires you to make sure that the businesses you work with are pulling their socks up too. Under GDPR's provisions, if the data you send to your data processors goes somewhere it should not, you are both liable for the leak and the damage. So you need to make sure that the people you work with safeguard that data – and that you protect yourself in the event they do not.

The way to do that is through a document called a data processing agreement. Yes, it's a contract. (This is as legalistic as this book will get, I promise.) You should have your data processors sign one for any project you do with them.

Your data processing agreement must set out the following arrangements:

- The subject matter of processing; in other words, what personal data you are exchanging.
- The duration of the processing; in other words, how long you are using the data.
- The nature and purpose of the processing; that is, what sort of data processing you are doing, and why.
- The type of personal data involved; in other words, what sort of information you are exchanging, and whether any of that is sensitive personal data.
- The categories of data subject; that is, who this data is about.
- The controller's obligations and rights: a reminder that for the purposes of the project, it is your data.

In addition to those agreements on the scope and nature of the project, your data processing agreement should remind your data processors of their obligations over the data you send them:

- They must only process the data as you instruct them to do.
- They must ensure that any people processing the data are competent and confident to do so, through their terms of employment, a confidentiality agreement, or another binding obligation.
- They must take appropriate measures to ensure the security of your data.
- They must take appropriate measures to ensure the security of the data, and can justify those measures to you or to a third-party auditor.
- They must not engage a subcontractor as a sub processor without your authorization as well as a supplemental contract.
- They must take appropriate measures to help you respond to requests from individuals who wish to exercise their user rights over their data.
- They must assist you in making sure your own data security procedures and your data protection impact assessments meet your own GDPR obligations.

- They must specify the kinds of information, as well as the timeframes for notification to both you and to the data subjects, they will supply you with in the event of a data breach.

- They must delete or return all personal data to you at the end of the contract, and the processor must also delete any copies at their end unless they are required to keep it for another legal reason.

- They must submit to audits and inspections as requested from you or from a third-party auditor.

Your data processing agreement is not the main contract you sign with your data processors for the project itself, although it should be considered part of it.

There, that's the scary legal stuff done. Back to the fun bits.

STAFF TRAINING AND PROFESSIONAL DEVELOPMENT

It's no secret that we all need to get better about the privacy knowledge we bring into our workplaces. Privacy regulators, however, are tired of waiting for us to catch up. Under GDPR, and in a provision being replicated across many draft privacy laws, you are expected to make sure that the people working on your project are competent in the privacy con-

cepts and regulations that apply to your work. That knowledge must be documented and signed off by an accountable individual. "I didn't know" won't fly anymore.

In the event of a privacy concern or data protection complaint, a regulator may ask you some difficult questions about the knowledge you and your team have brought to the table. Those questions might include:

- Who has access to the data?
- What data protection training have those individuals received?
- Are they competent in the European data protection and privacy framework?
- Are they competent in any industry or sector privacy regulations (health, finance, etc.) that also apply to your work?
- Are they competent in the software development standards you use, such as ISO27001?
- Are they competent in the development frameworks and methodologies you use?

- Are they trained in the security testing, threat, and risk assessment methodologies you use?
- Is there documentation of this training in their HR records?
- Did you provide them with an overview of their data protection and privacy obligations in their workplace induction?
- Do you provide them with professional development and refresher training on privacy laws?
- What security measures do those individuals work with? Most data breaches, after all, are internal.
- What notification and alert procedures are in place for them to report a data breach – whether that is external or internal? Would they be protected for reporting a concern – or whistleblowing?
- What about management and leadership? Are they competent in all of the above? Do they understand their professional risks and obligations?

If these questions scare you now, I promise you they would be a lot scarier (and humiliating) after a preventable data

breach hit the headlines, with your work squarely in the middle – and your professional competence in question.

So force the issue.

Speak with your employer, if you have one, to help them understand these expectations, and ask them to commit the professional development resources needed to fill them. If your employer won't provide training in privacy as a form of professional development, or rejects privacy as both a concept and a legal obligation, consider it a warning sign that it's time to take your talents to a safer workplace.

> If you are a student reading this book, and privacy is not a part of your educational curriculum – either in theory or in practice – ask your teachers and professors why, and ask what it will take for them to change. The harsh truth is that they should not be sending you into the world of work as a future web professional with gaps in your knowledge about something as fundamental as user privacy.

DATA PROTECTION OFFICERS

Earlier we talked about how data protection under GDPR becomes everyone's job – as it should be. However, if your work involves large-scale data processing, or deals with the profiling of individuals, data protection becomes an actual job for someone known as the data protection officer, or DPO.

Your DPO is a specific, named individual who will carry formal responsibility for your organization's data protection compliance. They will ask difficult questions, sign off accountable documents, and act as your point of contact for regulatory queries. In other words, this is not a vanity title or a tick-box health and safety guy: it's an obligation you need to take very seriously. It's also important to remember that the DPO is not there to be the bad guy or the enforcer. They are there to help you.

While a DPO does not require any specific set of qualifications or accreditations, and certainly not a law degree or a privacy certification, they should be chosen based on their experience and expertise in data protection and privacy, their professional qualities, and their ability to fulfil the task at hand.

A DPO is required if your organization is in one of these groups:

1. A public authority, such as state, local, and national government bodies.

2. Organizations whose core activities involve regular and systematic monitoring of personal data. "Core activities" means that data use is intrinsic to everyday functioning, and that might include many development scenarios. The phrase "regular and systematic monitoring" also encompasses the advertising and marketing industries.

3. Organizations that engage in large-scale processing of sensitive personal data. "Large-scale" is a subjective term determined by:

    a. the number of data subjects

    b. the volume of data or the range of data processing

    c. the length or duration of the data processing.

    d. the geographical reach of the data processing

Based on these definitions, a useful rule might be: if you think your work is large or complex enough to require a DPO, it probably is.

Even if you are not required to name a DPO, I would highly recommend that you name one on a voluntary basis. This can be an add-on to an existing role, a part-time position, or even an external contractor. What better way to keep good privacy practice part of your everyday operations? Think of the DPO as the good cop who will keep your data protection processes on track, but also as the bad cop who will pull everyone's socks up from time to time.

The DPO must also be prepared to make themselves available as the point of contact for external communications, and by that I mean concerns from your national data protection regulator. The DPO's contact details should be published where they would be needed, for example, on an organization's privacy policy pages. Their name and details must also be submitted to their data protection authority as the designated point of contact in the event of a public complaint.

If you do decide to name a DPO, there are certain rights and protections they must be given, similar to the rules around whistleblowers. The role has to be adequately resourced with whatever they need to do the job. Where applicable, they should regularly report to your directors. They must also be protected within the role: they cannot be fired for raising concerns or asking uncomfortable questions, nor can they be told to ignore a problem.[5] Don't shoot the messenger.

5. That being said: getting fired for raising a privacy concern is not a source of shame: it's a source of pride. In fact, you will never have to pay for a drink in Ye Olde Privacy Pub again.

PREPARING FOR DATA BREACHES

Finally, integrating good privacy practice into project management means preparing for the worst. While we all can and should do everything in our power to prevent data breaches and misuse from happening, we know that data will go places it shouldn't.

GDPR – and, for that matter, being a good person – requires you to do everything possible to prevent data breaches from happening, and also to prepare for data breaches in advance. These preparations are technical, and they are human too.

You'll need to audit your technical systems for issues that could open the door to a data breach, whether that is unpatched software, poor antivirus software, or even ex-employees' accounts remaining active on systems.

Data breach preparation also means looking at what human aspects of your operations could contribute to a preventable disaster. Are new staff given data protection training in their inductions? Does everyone share one admin password? Can staff raise a concern without being punished for trying to cause trouble? Is there an escalation process for when a breach is discovered?

Remember that a data breach does not necessarily mean that the data was externally accessed or misused. Data in

places it should not be, seen by people who should not see it – even *internally* – is a data breach.

Data Breach Reporting

Under GDPR, certain kinds of data breaches must be reported to your data protection authority **within 72 hours of discovery**. The threshold for reporting is that a breach "is likely to result in a risk to the rights and freedoms of individuals."[6]

A high-risk breach must be reported to the individuals affected immediately *in addition* to the notification you are required to make to your data protection authority.

In the event of a breach or misuse, your data protection authority will expect you to provide them with the following information:

- Details about the nature of the breach, such as:
    - what category of data has been breached
    - how many individuals are affected
    - how many data records are involved (as opposed to individuals affected)

6. https://smashed.by/eurlex

- Information on how you were alerted to the breach, and by whom (an internal reporting mechanism or a customer complaint, for example).
- Any available information on who was responsible for the breach, or how it happened.
- What consequences will occur as a result of the breach.
- What measures you have taken to deal with the breach, such as contacting affected customers, mass resetting all passwords, and so forth.
- What measures you will take to deal with any results, such as unauthorized charges to customers' accounts.
- The name and contact details of your DPO or the individual taking the lead on the issue.

Could you pull all of this information together in real time? Run a drill to find out, and work out a reporting template.

You also need to give some long and hard thought about how you will communicate the data breach to the people whose data was misused, and what support you will provide to them for as long as it takes to put things right.

When you are reporting the data breach to your regulator, you are not required to reveal any information that would jeopardize an ongoing investigation, such as the identity of a rogue employee. For this reason, you may provide updated information to your DPA in phases.

It should also go without saying that if a data breach is a law enforcement issue, such as one involving criminal activity or which could put users at immediate risk of bodily harm, you should notify the authorities (such as the police) in addition to the data protection regulator.

PREPARING FOR REGULATORY QUERIES

Let's say that a member of the public raised a complaint about your service, or perhaps your app scaled a bit too successfully. What sort of questions should you be ready to answer?

Between August and December 2019, Ireland's data protection authority, the Irish Data Protection Commission, sent these questions to dozens of domestic and international tech businesses as part of an official audit of their compliance with the ePrivacy Directive.[7] These questions will give you a good sense of what a data protection investigation might look like.

7. https://smashed.by/dpcreport

1. List, in a table where necessary, the names, types, functions, security, origin and lifespans of all cookies deployed when a user visits your site, either as a first-time visitor, when a user is redirected to your site from another site, or as a return visitor. This list should indicate for each cookie whether it is a first-party or third-party cookie and which domain is its host. Indicate whether a cookie is determined to be "strictly necessary" or optional, and if so how this determination is made.

2. List all the third parties whose cookies or assets, including "like" buttons, plugins, pixels, beacons, audience measurement tools or otherwise that are deployed on your website. Describe the purpose of each of these and how they are used and processed by your organization, including for analytics.

3. Where third-party cookies or assets are deployed describe whether the data controller of the website is a joint controller with such third parties, or otherwise.

4. Please describe how you ensure users are aware of any third-party activity, such as analytics or advertising, taking place on your website, and what information you are providing to users about how to control that third-party activity via their browser.

5. Please provide screenshots of the information presented to users in relation to cookies when they visit your website. Include, where necessary, all interstitials, banners, notices, pop-ups and other means used to draw a user's attention to the use of cookies.

6. Demonstrate in your response how a user's consent is captured prior to the storage of information, or the gaining of access to information already stored, on the user's terminal equipment.

    a. Provide details of how this consent meets General Data Protection Regulation (GDPR) requirements for precise, unambiguous and affirmative consent, in particular how consent is recorded and can be demonstrated by the data controller, as per Article 7(1), and how it can be withdrawn as per Article 7(3)

    b. Provide details of any privacy controls implemented, including information on sliders, buttons, UX, push notices or any other methods used to alert users to the use of cookies and to enable them to make choices about the use of such technologies. Describe the intended functionality of each control.

c. Confirm whether storage or access to information on a user's terminal equipment occurs before or after consent is obtained and recorded.

d. Describe how a user may, subsequent to an initial visit and interaction with any consent mechanism, vary their initial consent choices.

e. Where applicable, describe the circumstances and reason why consent may again be sought from a user who has initially refused consent.

f. Describe any differences in the consent capture mechanism when accessed from a mobile device, compared to a desktop computer.

g. Describe how your cookies and consent mechanism interact with any installed "cookie blocker," or "ad blocker" technology, including detection of such.

h. If any such "cookie blocker" or "ad blocker" is detected, please describe if, and how, this affects the user's ability to browse and view content on your website.

7. Does the user have any control over the cookies which could be stored on their terminal device?

    a. If user controls exist, please describe the default settings for controls in the cookie consent mechanism used for your website.

    b. For each cookie that is enabled by default and cannot be turned off via any user controls, please outline

        i. The name of each cookie that falls into this category

        ii. The reason for no controls being in place to prevent storage of the cookie.

8. Demonstrate how the information provided to subscribers or users is clear and comprehensive, prominently displayed and that it includes, without limitation, the purposes of the processing.

9. Please provide a full electronic copy of your cookies notice and all information available on your website in relation to the use of cookies. Include, where possible, a screenshot of any headers or footers contain-

ing information about cookies, and the URLs where this information may be found. You should be able to demonstrate that this information is both prominently displayed and easily accessible.

10. Please indicate if users are redirected to any third-party sites in order to access information about third-party cookies placed on terminal equipment when they visit your site. Please provide the URLs or domain names.

11. Please provide a copy of your privacy policy or notices made available to users of your website and indicate how and where on your site this information is displayed.

12. If your organization has not achieved compliance with the ePrivacy Regulations, please explain why this is the case, with a clear timescale for when compliance will be achieved, and specific details of what work is being done to make that happen.

13. Please provide any additional or supplemental information that you feel may aid your response to this sweep questionnaire that may not have been covered by any previous questions.

PRIVACY IN PROJECT MANAGEMENT CHECKLIST

I spent the better part of two years helping digital agency leaders get ready for the European privacy system. Your souvenir of those years is this checklist which you can use, on your own time, to evaluate your business's level of compliance with its best practice principles on the project management level.

That being said, remember that good privacy practice isn't a checklist or a one-off task. It's about your ongoing everyday processes, whether they're about people and administration or data and tech. Your privacy practices must be constantly reviewed, renewed, and refreshed as your work and your data flows change.

Short List: Evaluate Where You Are

- Review your staff awareness of relevant privacy laws.
- Inventory and review all the data you hold, both online and offline, internal and external.
- Review your public facing privacy information notices for all products and services.
- Review your consent processes across all projects.
- Review your subject access request process.

- Review your data breach process.
- Review your technical security standards.
- Decide whether you need to appoint a data protection officer.
- Review your internal security standards such as staff training, HR documentation, and network access.
- Implement PbD into your workflows for all future projects.
- Decide whether you need to create a PIA template specific to your business's needs.
- Review contracts with any third parties with whom you give or receive data.
- Review your legal basis for sending or receiving data outside the EU.

Long List: Kickstarting Your Privacy Journey

Awareness

- Have you devised a privacy awareness and implementation plan for all employees, ranging from senior management to line staff?

- Have you allocated appropriate human and technical resources to privacy implementation?

- Have you spoken with your contractors and suppliers about their own privacy implementation levels?

The Information You Hold

- Have you conducted an audit of the information you hold online?

- Have you conducted an audit of the information you hold offline?

- Does your audit contain records of all processing activities?

Your Users' Individual Rights

- Are you aware of the rights that individuals have over their data?

- Do you understand how these rights work in practice?

- Are you aware the user can invoke any of their rights at any time over any aspect of their data?

Subject Access Requests

- Have you created an SAR process?
- Is your SAR process detailed in your privacy notices?
- Do you have the technical and staffing capability to respond to subject access requests within thirty days?

Privacy Notices

- Are your privacy notices written in plain language, with no "legalese"?
- Are your privacy notices broken down into clear sentences and short paragraphs?
- Do your notices provide a clear and transparent description of what data is collected, how data is processed, how data is used, who data is shared with, and what the user's rights are?

Consent and Legal Basis

- Have you determined which aspects of your data collection and processing are grounded in consent, and which aspects are grounded in a legal basis?

- Have you ensured that your consent processes are active, positive, granular, unbundled, named, do not create an imbalance in the relationship, are verifiable, and are documented?

- If not grounded in active consent, can you document and prove that your collection and processing of data is grounded in a legal basis?

Information about Children

- Have you documented your processes for data about under-16s?

- Do children provide their information directly? If so, have you written a privacy notice for children in language they can understand?

- Are you documenting evidence that you have parental consent for any data processing for under-16s?

Data Breaches

- Do you regularly audit your systems and processes for potential data breach issues?

- Do you know the criteria for a high-risk, reportable breach?

- Have you created a template for GDPR's data breach reporting requirements?

Privacy by Design

- Have you familiarized yourself with the principles of Privacy by Design?

- Have you reviewed your existing sites, apps, and processes for best PbD practice?

- Have you developed a privacy impact assessment template unique to your business's needs?

Data Protection Officers

- Have you determined whether you need a DPO by law?

- If not required, have you considered appointing a DPO voluntarily?

- Have you published your DPO's details in your privacy notices?

International Data Transfers

- Are all of your partners and third-party service providers in non-EU countries familiar with the new requirements under GDPR?

- Are your US-based partners and third-party service providers meeting European data protection standards?

- Are you including and requiring GDPR compliance in your contracts with partners and service providers?

Privacy in Development

Let's move on to the ways you can integrate the best privacy principles from Part One ("Privacy and You") into your development workflow.

Over several years of giving conference talks about privacy to development communities, I couldn't help but notice that the topic often made audiences feel deeply uncomfortable. In a classic case of the phrase "We don't know what we don't know," these talks were often the first time that privacy principles had ever been explained to them. And that, in turn, triggered a lot of soul-searching about the gaps in their training, knowledge, and workplace practices. That was bound to cause a bit of discomfort.

So I'll say to you what I said to my audiences: the information that follows in this section is being presented to you because I am on your side and I want to help you to do better. I'm not out to shame you, or to question the competence of your employers, or to make you feel dumb or incompetent. This book exists to give you a hand up, not a slap down.

That said, there are plenty of others queueing up to give you the latter.

BEST PRACTICE PRINCIPLES

In Part I, we were able to create a reference index of universal privacy principles based on existing best practice frameworks. All of those principles, in their surprising simplicity, apply to development practices too.

What's more, within those basic frameworks, there are additional checks and safeguards that you can add to your toolkit. That hard work has already been done for you by several European data protection agencies: the Datatilsynet in Norway,[8] the CNIL in France,[9] and ENISA, the EU agency for cybersecurity.[10] I'm grateful to them all for doing work, which to the best of my knowledge no developer advocate has ever assembled.

In this section, I'm going to tie those frameworks together to create a holistic approach to developing for privacy. These principles apply no matter what programming language you use, or what product you ship.

We'll break those principles into four stages:

1. Before you begin a project

2. Before you begin to code

8. https://smashed.by/datatilsynet
9. https://smashed.by/cnil
10. https://smashed.by/enisa

3. As you develop

4. After you ship

In addition to these frameworks, as well as what you'll learn in this part of the book, the W3C has published a self-review questionnaire on security and privacy in development. It covers the areas you need to consider in far more detail than this book allows. I highly advise you to get to know the questionnaire[11] and integrate it into your development workflow.

BEFORE YOU BEGIN A PROJECT

Identifying Team Knowledge and Methodologies

Let's get the uncomfortable part out of the way first.

Earlier on, we discussed staff training and professional development (page 114), and the fact that regulators, lawyers, and the public now expect you to have qualified competence in the work you create. For developers, this is an issue that must be addressed head-on at the start of a project, or as a part of the hiring and induction process.

In other words, you need to sit down with everyone who will be working on a project, from management down to

11. https://smashed.by/privacyquestionnaire

code, and find out what they know, what they don't know, and what they need to know. The holes in your team's privacy knowledge, be they legal or conceptual, need to be filled through some form of education.

If this book is the only education you receive on privacy, it is better than nothing.[12] However, your workplace owes it to you to provide you with proper training.

Developer training in a workplace environment should have two components. The first component should be conceptual and legal, covering the best principles of privacy practice as well as the legal frameworks applicable to the project; Part I of this book has been your head start on that.

Now let's be clear here: no one is expecting you, or your development team, to become lawyers or data protection experts. You do, however, need a basic working competence in the principles and regulations which will define the integrity of your work, and will – I hope – protect you from the consequences of getting it wrong.

The second component of your training should be technical. Good privacy practice and avoiding unnecessary data capture, exploitation, or loss requires everyone in your project to work from a clearly defined set of code libraries, tools, frameworks, and procedures. For that reason, a healthy

12. As was mentioned at the start of this book, I am not a lawyer, and you should not base your legal compliance on privacy, or anything, on books written by random Scottish women.

approach to privacy should involve defining your standards and methodologies, and ensuring that everyone on your team is working to them. I would break this into six areas:

1. Data protection regulatory frameworks (if applicable), including definitions, concepts, and user rights.

2. Any sectoral frameworks applicable to what you are coding for, that go beyond universal data protection laws, such as regulations pertaining to health, financial, or children's data.

3. Information security frameworks.

4. Software development frameworks.

5. Security testing frameworks.

6. Threat modeling and risk assessment frameworks.

Privacy laws, as well as principles, do not define a list of right or wrong frameworks, version control systems, or testing tools. (Nor will they ever, as regulations are drafted to be future-proof.) What matters in development is that the stack you use is clearly defined and followed for each and every situation you use it in. You may, of course, modify your standard tools and infrastructure at any time, as long

as you ensure they are acknowledged and documented as the frameworks which must be used.

I highly recommend conducting an internal audit to identify what you and your colleagues know – and don't know – about both of these components. Work with your management and HR to fill any gaps with remedial technical training and support.

And for what it's worth, if your education as a developer involved one of these components but not the other, you may wish to have a word with your teachers about why they supplied you with only half an education.

Preparing for Internal Accountability

The next step to take before beginning work on a project is setting up your internal accountability processes and documentation. Whether you're developing on your own or working as part of a team, these steps are the same.

First, you'll want to identify who will have privacy oversight for your project from the development perspective. This could be a formal position, such as a DPO, or it could be a senior developer experienced in threat modeling who is best placed to support the DPO. Either way, they need to be someone who takes a firm-but-fair approach to privacy without threats, sarcasm, or scaremongering. So be sure to

choose someone who isn't afraid to do their homework, ask uncomfortable questions, or issue difficult requests.

Next, support that person to create the processes needed to protect user privacy. These processes will be internal, such as the creation of a privacy impact assessment and a data flows map (more on that shortly), in addition to creating records of data processing activities and third-party sharing. These processes will also be external, such as the creation of pathways for user-facing subject access requests and notifications of data breaches. Remember, this is about your development practices, not your legal compliance, so keep the focus on the code and the decisions that inform them. Let your DPO sweat the fine print.

Once those processes have been identified, support that person to create and maintain the documentation that records your progress towards them. Again, your DPO should take the lead on this, but work closely with them to make sure the development procedures are recorded throughout the project life cycle. As always, that documentation should be regularly amended by everyone working on a project.

No privacy law or regulator will tell you exactly what that documentation must say or how you should format it, of course. As a rule, however, nothing you document should stop you from sleeping at night.

BEFORE YOU BEGIN TO CODE

Now that you have your training, your oversight, and your documentation processes in place, you're ready to begin planning your project. While your privacy impact assessment will be your project's backbone, it can't do all the heavy lifting on its own. Some additional development-specific procedures will do the rest.

Identify Your Development Safeguards

I am not here to tell you what to code or how to do it. However, there are a number of basic technical considerations that will go far to protect your users' privacy, safeguard their content and communications, and maintain the integrity of the project itself.

At the bare minimum, the considerations for users' front-end experience should include:

- The end-to-end encryption of all data and all communications as the default (that is, not as an optional add-on).
- Please use *https://*, because seeing *http://* this late in the game is not the sort of '90s flashback I enjoy.
- The use of first-party resources as much as is humanly possible, including CSS, media, fonts, images, comments, social sharing, and captchas.

- This means the minimal reliance on the use of third-party resources as much as is humanly possible, to the point where dependence on a third-party resource should be regarded as a point of failure.

- This also means minimal reliance on third-party infrastructure-as-a-service, platforms-as-a-service, and software-as-a-service – and while I hate to name specific examples, it is worth reflecting on how dependent web development has become on Amazon Web Services (AWS).

- No usage of beacons, trackers, or invasive analytics, none of which are necessary for any reason.

- Likewise, no usage of adtech, marketing, or non-functional cookies, which are a waste of everyone's time, resources, and energy; and this means:

- Minimal reliance on third-party compliance processes required to manage those adtech, marketing, or non-functional cookies, trackers, and beacons, because you wouldn't need those third-party compliance processes if you didn't clutter your work with those unnecessary privacy blights in the first place.

- Minimal reliance on embedded third-party content and fallbacks for that content – such as static maps,

text-only representations of social media posts, and direct contact forms – for those who are not able to access embedded content, due to (for example) workplace security rules or wartime sanctions.

A useful creative exercise to engage in is to consider how the thing you are building would work if it was a static site. Would it still be functional, in a privacy-conscious way, or would it be a blank screen? Could users still do the thing they need your work to do – for example, get information or seek emergency assistance – without any single point of failure getting in the way of that?

Another useful exercise is to consider how the thing you are building would work in a browser's private/incognito mode, or through a VPN, or through any connection outside the conventional definition of a normal user experience, such as a slow and expensive data-only connection on an ageing mobile. Would their use of your site or app be degraded or made impossible without an exchange of personal data?

Users in Europe who wish to access American news content in the era of GDPR have become accustomed to one of two experiences.

The most notorious, common to local news sites, is a splash screen saying: "Unfortunately, our website is currently unavailable in your country. We are engaged on the issue and committed to looking at options that support our full range of digital offerings to your market. We continue to identify technical compliance solutions that will provide all readers with our award-winning journalism."

What that means is that the news site is not actually a news site; it's an adtech data harvester which happens to contain a certain amount of authentic journalistic content between the ads, the tracking, and the clickbait. That authentic content, through no fault of the journalists who wrote it, has become so parasitically dependent on a business model based in privacy-eradicating adtech that when faced with the horror of forcing readers to consent to the abuses of their data, those news sites would rather engage in the self-censorship of their own journalism than wise up.

But there's another experience European readers have become familiar with in the age of GDPR, one much less common but much more wonderful. To single out an example, if I visit the website of US public radio network NPR from Europe, I am redirected to *https://text.npr.org*. It's a simple, minimalist, '90s-style text-only site that contains all of the journalism, none of the clutter, and – crucially – none of the privacy-eradicating adtech bloat which has come to characterize online news sites as a whole. The text-only site, for what it's worth, has also benefited US users experiencing emergencies, such as people evacuating from natural disasters that knocked out the Wi-Fi and the phone networks.

Those two examples are a stark illustration of how badly privacy-invasive adtech has degraded the original promise of the open web – and how easy it can be for you to reclaim that promise through simple decisions at the development level.

Identify Your Technical and Security Safeguards

In addition to protections for your users' front-end experiences, we need to consider how to protect your work from posing a threat to the integrity of your systems and to the open web as a whole.

These development practices stretch across system integrity, threat modeling, and cybersecurity, and you'll want to make sure that your team includes people with expertise in all of them.

These practices could include:

- Securing your workstations and laptops, and securing your internet connections, using configuration management tools.[13]
- Keeping your secrets and passwords out of your source code repository.
- Using preventive coding standards, such as disabling unsafe or unnecessary modules in APIs and third-party libraries.
- Defining what constitutes an unsafe module or third-party library in the first place; for example,

13. If I had £1 for every time I have witnessed someone leave a work laptop unattended in a coffee shop while using an insecure connection, I would be on a tropical holiday.

the unnecessary capture of personal data, or adtech sharing without consent.

- Establishing a content security policy that blocks the loading and execution of specific external resources, and can mitigate against things like cross-site scripting (XSS) attacks.[14]

- Requiring secure strong passwords, never stored in plain text, and options for two-factor authentication (2FA) if the user so chooses.

- Requiring accounts and passwords unique to the site, not through an identity provider, and absolutely never through a social networking site.

> All of the questions you ask about the privacy standards you bring to your development environment should apply to the tools you use internally as a team as well. Privacy regulators are as concerned about SAAS tools such as Slack, GitHub, and AWS as they are about the products you create using them. So whether you use commercially available

14. You can test your site at https://observatory.mozilla.org/

applications to discuss personal data or roll your own, they need to be technically and legally watertight.

Model Your Data Flows… and Threats

Identifying Your Data Flows

You knew there was going to be a part in this book involving Post-it notes, magic markers, and a big wall. You have reached your destination.

Let's map out our development plan of attack by modelling your data flows and threats.

As with all things privacy, it is good to work to an externally accountable standard. I personally love the LINDDUN privacy engineering model, which was developed at the University of Leuven in Belgium.[15]

First, you'll create a diagram of what it is you intend to build from three perspectives: the users, the processes, and the data stores. Map out all the interactions – and the ways data flows – between, through, and across those three perspectives, across the user journey, both on the front end and on the back end.

15. https://www.linddun.org/

Modeling Your Privacy Threats

Sticking with the LINDDUN model, now you'll map out your data flows against these privacy threats:

- Linkability: are two pieces of data about a subject linkable?
- Identifiable: can a data subject be identified by different pieces of data?
- Non-repudiation: is it impossible for a data subject to deny the data evidence linking them to a certain action, whether that is good (e.g. this is the owner of the account) or bad (e.g. this is the whistleblower who posted this data)?
- Detectability: is it possible to detect that a piece of data exists without having access to it?
- Disclosure of information: is an adversary able to learn the content of an item of interest about a data subject?
- Unawareness: is the data subject unaware of the collection and processing of their data, and their rights over it?

- Noncompliance: does the system fail to comply with data protection principles or privacy law?

For a deep dive into mitigating these threats, climb the LINDDUN threat trees at https://smashed.by/threatcatalog.

Bonus Political Problem!

While you are mapping out your data flows, you should also take time to map them – literally – by identifying which countries they are hosted in, and, if applicable, which countries they flow through to get there. There are two reasons you should do this.

First, identifying the countries of hosting will help you stay within your legal compliance obligations, which may oblige you to ensure that hosts provide the highest possible level of data protection. It may also help you to make safe and compliant decisions regarding the hosting of content that enjoys enhanced legal protections, such as health or financial data. Typically this takes the form of choosing to deploy local resources, such as an in-country deployment of AWS or an EU-compliant analytics application, or to remove third-party processes from pages containing sensitive personal data.

And second, identifying the countries your data flows through en route from the user to the host can mitigate the growing problem of data laundering – the tech equivalent of money laundering – where data is "washed" through a country with stronger data protection principles into a country with weaker ones. Privacy activists are becoming finely attuned to the practice, and it's likely to be a political flashpoint for years to come; so make sure that flashpoint isn't your work.[16]

AS YOU DEVELOP

Developing for User Rights

Recall that our Privacy by Design principles ask you to develop to ensure that you:

- Inform your users about their rights over your uses of their data through privacy notices and information.
- Give control over users' data to those users through maximised user consents.
- Provide a means to exercise the rights of subject access, data export, and data deletion mechanisms.

(Who said privacy was hard?)

16. For more on this practice, read *Privacy Is Power* by Carissa Veliz (https://smashed.by/privacyispower).

Let's walk through those checkpoints from a development perspective.

The Right to Be Informed

Your users need to know what data you are collecting about them, why you are collecting it, what you do with it, and what rights they have over it. This applies whether that data collection and processing is done by yourselves as the first party, or is done through a third party. And it applies whether that data is actively provided by the user or passively collected by a service.

Your challenge as a developer is to find a way to note all those forms of data collection and processing – regardless of where they come from or why – in the privacy notice. Hooks and filters can help here.

The Right to Consent

Strive to develop in a way that ensures user consents are maximized by default in a way that does not detract from the functionality of the service. Ensure that the functionality exists to give them control over those consents, at any time, in a granular manner. You will need to work closely with your front-end designers here to ensure that consents are approached holistically.

And no, legitimate interest is neither a valid form of consent, nor an alternative to it, nor a thing that should ever have a place on anything you build. Full stop.

The Rights of Data Access, Portability, and Deletion

As you develop mechanisms to allow the user rights of subject access and data export, think in terms of interoperability and portability first. In an ideal world, a user should be able to download their data from you and upload it to another service just like that. (You wouldn't be working on the web if you weren't an idealist.)

Data protection laws generally require these files to meet three criteria: they must be structured, commonly used, and machine-readable. At this point in time, this tends to mean CSV, XML, or JSON.

The subject access and data export utilities you create should produce a file that the user can actually, well, use. We've all seen anecdotes from people who filed a subject access request and received a CD-ROM, a postal printout, or a .zip folder containing dozens of CSV files in return, none of which were remotely usable. So ensure that you're giving your users a data file that they can read, reuse, and recycle. Don't give them the code equivalent of a passive–aggressive sulk.

Developing for data deletion should make it as easy and frictionless as possible for your users to part company with you. Ensure that if a user deletes their account or removes an app, all the data held about them goes away too. (Covid test-and-trace apps have been a surprisingly good example of best practice on data deletion.)

Additionally, it's more than a good idea to allow users to delete old data without necessarily deleting their account: it's best privacy practice. Fifteen-year-old forum posts, ten-year-old tweets, and five-year-old playlist histories serve no purpose to either service providers or users. That data also creates problems for you, as your data retention periods are stretched out for several years after the data was actually needed. As you develop, think of ways to build in the functionality to allow users to delete old data after a certain and very generous period of time.

If deletion seems a step too far, consider implementing ways to de-identify and anonymize old data.

All of your development processes for user rights, including all forms of consent or opt-in, should generate some form of time-stamped documentation of what the user did, what they agreed to, what consent they gave, how they gave it, and whether or not they have chosen to with-

draw it. These largely internal logs should be secure and, if possible, stored separately.

Testing and Maintenance

You don't need me to tell you how to do prelaunch testing. But you do need me to ask you to think of the ways you can check for adherence to the principles of Privacy by Design and data protection by default in your testing processes.

Recall that those principles ask you to:

- Minimize and limit the data you collect, process, and use to the least amount possible, and only the data that is required for the specific action.

- Hide and protect the personal data you collect from being viewable or accessible, either publicly or privately.

- Separate the data you collect so that it is processed and retained in the most distributed form possible.

- Aggregate data in order to process it with the least possible detail necessary.

Your tests for those checkpoints should supplement existing procedures in your development testing, like your unit and

functional tests, as well as your security testing, such as penetration testing, fuzzing, and end-user beta testing.

Your privacy testing procedures should predict the ways that malicious actors would access actual data on your system. Would a suspicious search for user data, or an alteration to a record, be logged as a security vulnerability? Is data stored in login cookies? Could someone gain access to data by intentionally triggering an error? What do you do about users who have used plain text passwords? What about internal controls?

If you are applying privacy by design retroactively to an existing project, have you tested how easy it is to access legacy data? This is where you have to think really creatively – and somewhat maliciously – about how and where data can escape.

Oh, and please remember to use dummy data for your testing. Please.

Keeping It Clean

The golden rule of good privacy practice is *document it or it didn't happen*. It applies here too. Document your privacy preparations, testing, methodologies, and mitigations along with your other project documentation and, if possible, within your code and repositories.

AFTER YOU SHIP

Logging and Analytics

Finally, use public-facing analytics and internal-facing logging to understand how system resources are being deployed and where those resources might be going places they shouldn't.

Now, with no apologies to the privacy purists: analytics are good! It is entirely possible to use privacy-conscious analytics, which help you to understand the usage of your sites and apps, and identify irregularities and issues, without exploiting your users or their personal data. We will discuss how to make good choices on analytics in Part Three ("Privacy and Your Users").

Where routine system logging supplements the use of user-facing analytics in a way that collects personally identifiable data for security purposes, be conscious of the privilege escalation which results as threats are identified and more people have access to the personal data within that threat.

It goes without saying that you should ensure your internal system logs are safeguarded and that you have an adequate retention and deletion cycle. It's also worth noting that you may be required to retain system logs for legal purposes, but

in doing so you should also consider how hostile actors – including governments – may seek to misuse those logs to target the people in the data.

Planning for the Future

On page 120, we discussed how to prepare for data breaches as an organization. Your development practices should create a pathway for how those data breaches, as well as common errors and vulnerabilities, are reported and addressed. Do you have a responsible disclosure programme? How are reports processed and escalated internally, and how are they prioritized along a scale from common bug fixes to critical emergencies? Do you participate in a bug bounty programme? Whichever paths you choose, make them good ones.

Another maintenance consideration is your long-term dependence on third-party applications, including software, libraries, or SDKs. You'll need to make sure that all of these are viable in a way that does not create a privacy threat. How are these updated and how often? If they are open-source applications, are they maintained by an active community working under transparent and open governance? Do you contribute to those OSS projects' maintenance? If your third-party dependencies are commercial products, what are their life cycles? Do they collect and process per-

sonal data from your users as "payment"? Regardless of who owns them, what's your Plan B for when they are deprecated or abandoned?

A CASE STUDY ON DEVELOPMENT GUIDELINES

Here's a creative lesson from the front lines of real privacy battles. It's one I'm rather proud of.

We're all painfully aware that the majority of web professionals and everyday users will never take a holistic view of user privacy. As far as they are concerned, achieving privacy means cutting and pasting a legal statement in the footer, and it apparently involves setting up some BS pop-up windows too. What that means in practice is that they look for – and expect – what I call the "magic plugin" that will do the job for them. Just install, activate, click, and hooray, they're GDPR-compliant. If only.

That's a battle you will never win, so you have to pick a smarter battle. You have to make sure that users understand that there is no such thing as the magic plugin or the one-click software that achieves privacy compliance – either in law or in practice – and make it clear to them that they still retain all the obligations and responsibilities to safeguard their users regardless of what they've installed. You also have to protect your ecosystem against reputational damage caused by developers who, either innocently or maliciously, are misrepresenting what your software can do.

The way to do that is to make this explicitly clear in your project-wide development guidelines, which define how the things you develop, and any extensions to them, are presented to the public.

Here's an example of how to achieve this. When I was an active contributor to the WordPress.org core-privacy team, I worked with the plugins team to amend the project-wide plugin development guidelines with one game-changing line of text. The guideline in question states: "Developers and their plugins must not do anything illegal, dishonest, or morally offensive," and provides a list of examples of practices that abuse the freedoms and rights of end users. We added an entry to that list: developers and their plugins must not imply that a plugin can create, provide, automate, or guarantee legal compliance.[17]

And just like that, a serious risk to site administrators, everyday users, and the reputation of the project itself vanished overnight. Well, it did take a few days. A quick scan of the plugin repo produced a list of over 1,200 plugins claiming to offer instant legal compliance – not just in privacy and GDPR, but in other issues like accessibility and, incredibly, legal contracts. Those plugins had over a million installations. That's a lot of people who thought they'd magically achieved GDPR-compliance by simply clicking a button.

17. https://smashed.by/wpdisclaimers

To keep their plugins in the repository, developers were required to amend their plugin descriptions to remove any claims of legal compliance. We sent out an email offering some constructive suggestions on how to do this:

> *While a plugin can certainly assist in automating the steps on a compliance journey, or allow you to develop a workflow to solve the situation, they cannot protect a site administrator from mistakes or lack of compliance, nor can they protect site users from incorrect or incomplete legal compliance on the part of the website. In short, plugins are helpful tools along the legal compliance journey, but should never be presented as a solution, nor should they give users a false sense of security.*

We also provided an FAQ, which gave some thought to issues of third-party dependencies.[18]

In taking this simple action, we proved that safeguarding user privacy doesn't have to involve lawyers, bureaucracy, or complex technical fixes. Sometimes all you need to do is take a step back and look at your development environment's bigger picture. You'll be surprised at what you find.

18. All praise for this work should go to the amazing Mika "ipstenu" Epstein.

Privacy in Design and UX

Finally, we'll dive into how to make your privacy-conscious work look great too. This is one aspect of a healthy approach to privacy where the hard work really has been done for you already – it's simply a matter of taking advantage of the outstanding resources that are out there, and making the most of them.

Before you get creative, though, this section will help you understand what you need to know to make good design choices. As with all of our approaches to privacy, we're going to be positive and constructive, but we also can't ignore some of the negative problems with privacy design which will require some defensive maneuvers on your part.

It's worth noting that Smashing Magazine's Vitaly Friedman has a wealth of interactive visual content available online to inspire you, including:

- "Privacy Concerns And Privacy In Web Forms"[19]
- "Better Cookie Consent Experiences"[20]
- "Better Notifications UX And Permission Requests"[21]
- "Privacy-aware Design Framework"[22]

19. https://smashed.by/formsprivacy
20. https://smashed.by/cookieconsent
21. https://smashed.by/permissionrequests
22. https://smashed.by/privacyframework

DESIGNING FOR USER RIGHTS

Let's review what your users' rights are, regardless of the presence or absence of a legal framework which requires them:

- The right to be informed about how their data is being collected, processed, and shared, including the data you send to or receive from third parties.
- The right to access the data you hold about them, download it, and correct any errors within it.
- The right to control what data you collect, process, and share.
- The right to ask you to stop collecting, processing, and sharing their data.
- The right to delete their accounts and data, notwithstanding any data whose retention is required for other legal reasons.

While your development colleagues will provide you with the technical means for these things to happen, your job is to design visual interfaces for them, which:

- Help your users to understand that they have those rights.

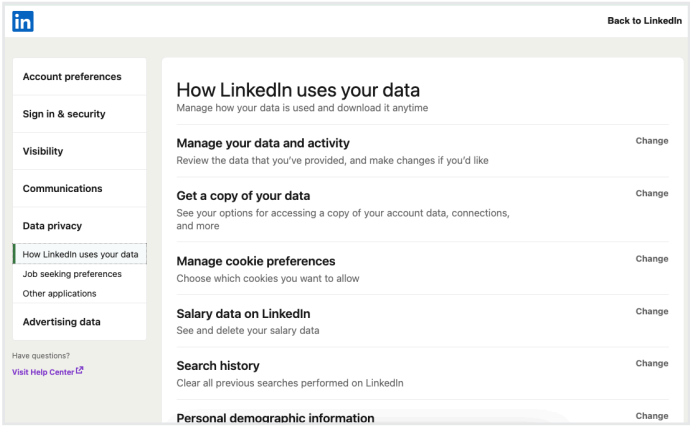
- Provide them with reminders to exercise those rights.
- Keep them informed about how you're helping them to do so.

There are three places where these rights, and interfaces, should reside.

The first is in a comprehensive and clear privacy notice, which we'll get to shortly. This is where you educate your users about the data you hold in the first place, which in turn leads to their understanding of their rights over it.

The second is in a central privacy area or dashboard. This could be a "Privacy" page in a user's account settings, an area in their control panel, or someplace within an app's options. These areas are the most logical place to house data export requests, data deletion requests, and account closure requests.

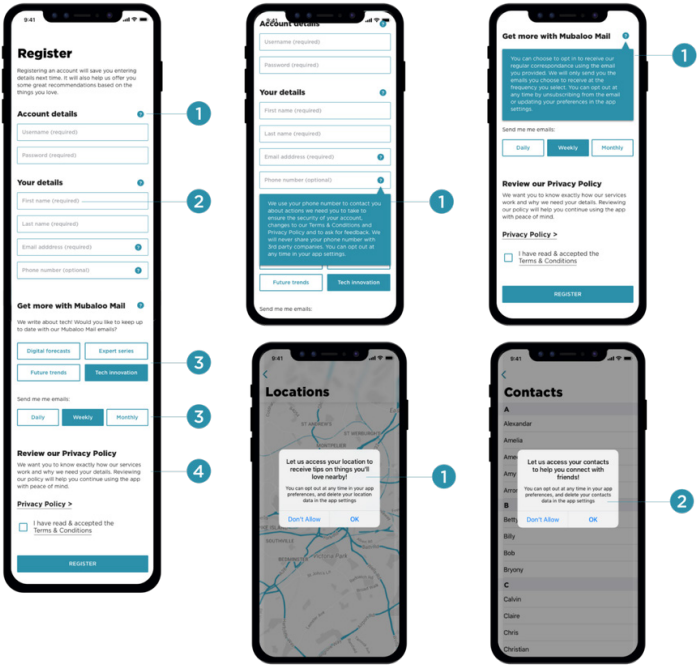
And the third is what we call "just-in-time": notices, leading to options and choices, displayed at the point where data is being requested for collection and processing, or where rights are being invoked. These interfaces are where to get your data consents right or, as it happens, very wrong.



LinkedIn's post-GDPR privacy dashboard brought a lot of options out into the open. Many of these options had been opted-in before GDPR, without the user's knowledge or consent.

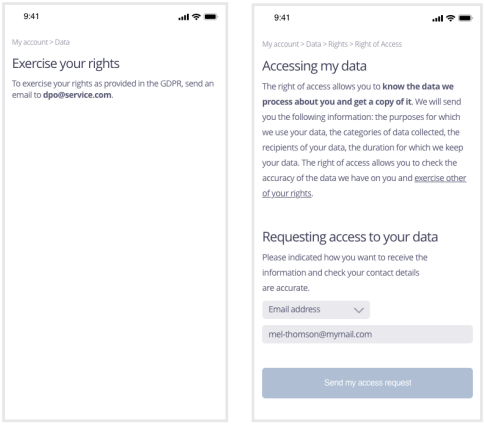
These places are also where you reassure your users that you are respecting their rights.

All of these rights and options, you'll recall, must be granular; a user must be able to invoke any aspect of control over their data at any time. Just because they granted consent for something at account sign-up doesn't mean they have to keep that consent forever. So ensure that your interface designs make those choices easy, and even periodically remind users to review and refresh them.



Smashing's article on privacy-aware design frameworks contains some great examples of just-in-time privacy notifications like these. Learn more at https://smashed.by/privacyframework

The interfaces you provide for data export, data deletion, and account deletion don't have to be works of art, and let's face it, they're not going to be. But they should provide the clearest possible path for the exercise of those rights, in a way that just works.



France's data protection regulator, CNIL, has done some impressive work on iterating examples of interfaces for data rights. You can view more of their examples at https://smashed.by/cnilrights

The interfaces you provide for information and consent require a lot more work.

DESIGNING TO INFORM: PRIVACY NOTICES

One of our universal privacy principles is transparency and notice: in other words, informing your users about everything you are doing with their personal data. The European privacy model knows this as the "right to be informed."

In my view, this is one area where GDPR's reforms couldn't have come soon enough. As we all know, under the previous

data protection regime, privacy notices had become long, lazy, and hostile. They tended to be called "privacy policies" because that is precisely what they were: legal contracts, drawn up by lawyers, for lawyers, and written to protect the site owners' legal backsides. They didn't give you options or choices: they told you what the deal was, like it or not.

The GDPR overhaul reclaimed privacy notices as concise, transparent, and intelligible dialogues written to protect your users, and that is what they should be. And whether you are beholden to GDPR or not, its approach to privacy information is a great starting place for yours.

That being said, it is very easy to have a privacy notice that ticks every box of GDPR as well as good practice, and yet is still part of the problem rather than the solution. So let's get it right from the start.

Who It's For

A privacy notice is how you tell your visitors the things *they have the right to know* about what you are doing with their data – not what you *want* them to know, and not what you are *legally obliged* to let them know.

That means that everything you are doing with your users' data – *everything* – needs to come out into the open.

So it needs to be designed and written for your users. Not you, not your company, and not your lawyers. In fact, if your privacy notice does require approval by your company's lawyers, leave them to the very end. After all, they had their fun in the good old days writing privacy notices, and look where that got us.

Sidelining the legalese also means that your privacy notice should be separated out from general terms and conditions pages, or the terms of use for the ownership of an account; indeed, these notices should not resemble each other in any way.

How to Write It

You should write your privacy notice in simple, clear language that anyone can understand. (If you're reading this book in English, think "plain English"). Don't use any legalese, at all, especially that awful form of legalese that scares, threatens, and berates the reader. Keep it positive and upbeat.

That being said, I've seen a few privacy notices that tried too hard to be cute and funny, and just came off as patronizing. I have also seen privacy notices stuffed with sarcasm, bitterness, and spite about the whole concept of privacy rights and European privacy rights in particular. Please remember

that your privacy notice is neither a stage nor a soapbox, and that's enough said about that!

Your privacy notice is a conversational dialogue with your users. A dialogue, of course, works two ways. So use your notice to remind your users about their data and privacy rights, as we discussed in the previous section, and perhaps even include interfaces for those options within the privacy notice. To facilitate the ongoing conversation, be sure to provide clear contact details for your company, your point of contact for subject access requests, and your data protection officer, if these things are applicable; if not, just include an email or a contact form to allow users to raise concerns with you directly.

If your web site or app is aimed at children, the European model requires you to present your privacy notice in language that your child users can understand. This means taking extra care not to overwhelm them with the uses (or misuses) of data, which should not be happening in the first place. And don't try to fool them, because they're a lot smarter than you.

OH AND BY THE WAY, EVERYONE, WRITING YOUR PRIVACY NOTICE IN ALL CAPS IS AN INDICATION THAT YOU HAVE COPIED AND PASTED IT FROM AN AMERICAN BUSINESS CONTRACT YOU FOUND ON GOOGLE.

IF THAT IS HOW YOU ROLL, YOU PROBABLY NEED TO GO BACK TO SECTION ONE OF THIS BOOK AND START AGAIN. IT ALSO MEANS THAT YOU ARE SHOUTING BECAUSE YOU LIKE TO HEAR THE SOUND OF YOUR OWN VOICE AND THAT IS REALLY NOT COOL EITHER.

What to Include

Whether your privacy notice is short or long, and whether it reflects basic functionality or a world's worth of data sharing, your notice should inform your users about:

- What data you are collecting, how that data is processed, how that data is used, and who that data is shared with.

- What legal basis you are using for your collection and processing of user data, whether that is active consent or some other form – and remember this is granular, so you must justify your collection of each kind of data, as opposed to collecting it all under one definition.

- List all third-party partners and services providers with whom you share data, and note what that data is and how it is used. This means all of them, whether they provide functional services such as payment processing or content distribution networks (CDNs), or whether they are advertisers and data brokers.

- Inform users about their privacy rights, including who to contact to discuss their concerns, and what third party (such as a data protection regulator) they can contact if they feel you are not respecting their data rights.

- Provide clear granular options for users to exercise their consent and data rights, such as subject access requests and deletions.

- Contact details for your company, your privacy person, and your data protection authority (if any).

How to Design It

There's no way to make the content on a privacy notice less overwhelming, but there are lots of presentation tricks to make it easier to digest.

First and foremost, you should break down your notice into clean and distinct sections. Use short paragraphs and tons of headings. Smashing's own privacy notice does this quite well (and they didn't pay me to say that).[23] I personally like the use of accordions, which instantly transform a cluttered page into a tidy space, and also give me an odd sense of control.

Second, think of ways you can use visual cues to soften the blow. A gently shaded table is a far better way to present a list of third parties than, well, a list. Likewise,

23. https://smashed.by/smashingprivacy

using an icon associated with the use of location data (for example) is an instant pointer to a user's rights about it, as opposed to mere words. Apple's privacy labels are a brilliant example of this.[24]

Additionally, if your privacy notice is going to be quite long, consider a table of contents. I like the one used by *The Atlantic* magazine, which despite leaning on the legal side, sets out clear sections about data rights for readers located in the US and EU, and even discusses children's privacy.[25]

Before you publish your privacy notice, a useful test to apply is to consider what a data protection regulator would think about it if they were asked to review it, for example, if a visitor raised a concern about your privacy practices. Would the tone, content, and design of your privacy notice assuage their concerns, or would it be just the start of your problems?

Keep iterating until you feel you've got it right – and don't hesitate to ask your authority for help if you need a hand getting there.

For more great tips on designing better privacy notices, read "Do Website Policy Disclosure Pages Always Have To Be So Ugly?" by Suzanne Scacca.[26]

Like your data protection impact assessments, your privacy notices should be revisited and updated several times a year

24. https://smashed.by/appleprivacy
25. https://smashed.by/atlanticprivacy
26. https://smashed.by/policydisclosure

as your data flows and commercial relationships evolve. Set a calendar reminder to review them every few months.

If you're beholden to the European privacy model, you'll need to inform your users of any major changes you make to your privacy practices, such as sending data to a new third-party processor, and get fresh consent for this new processing. This requires some visual work too.

DESIGNING FOR CONSENT

The visual design of consent mechanisms isn't the beginning and ending of good privacy practice, that's for sure. But it is a single point of failure for privacy as a whole. Whether it's awful cookie consent pop-ups or deceptive designs, the visual language of consent might feel like a battle which has been lost. I'm counting on you to turn that battle around.

Let's recall our universal elements of user-centered consent, regardless of the presence or absence of a privacy law requiring them. You should strive to:

- Give your users and visitors choices and options over your collection and processing of their data, including the data you send to or receive from third parties.

- Require clear, specific, and informed opt-in consent for all users of a user's or visitor's data, and do not require unnecessary consents in order to use a service.

- Give your users and visitors a means to control their consent options and rights at any time through settings, user accounts, or control panels.

This is where you need to become really good at designing for just-in-time consent – and that goes far beyond those dreaded cookie pop-ups. After all, you've got to master the visual language of supporting users to:

- Give active consent that is freely given, specific, and unambiguous.

- Give consent that is informed, meaning that your users know what they're giving their consent to and what rights they have over what happens next, and that they know every third party you're sharing their data with and why.

- Give consent that is positive, meaning you have not presumed or forced their consent.

- Give consent that is granular, meaning it's presented as multiple choices which can be changed at any time.

- Give consent that is unbundled, which means you're not forcing users to grant non-negotiable consent for one thing – or give away their data rights – in order to receive another thing.

- Give consent that is specific, which means the consent is just for one thing, not many things, and certainly not third-party advertising things.

- Does not create an imbalanced relationship, such as an unfair abuse of power between the service provider and the user.

- Gives consent that is verifiable and documented, showing exactly what the user has agreed to, what information they were given to support that decision, when they consented, and whether or not the user has withdrawn their consent.

In other words, it's the exact design challenge you're looking for.

With that in mind, the interfaces you design should alert users to the fact that they have not yet exercised their data rights, or granted opt-in consent to any applicable choices and options, rather than steamrolling over their rights to opt them in first and ask them later – which, as you know, is probably illegal.

To kick-start your thinking on how to do it right, check out the data patterns catalogue created by design agency IF.[27] The library presents clear, basic design patterns, some

27. https://catalogue.projectsbyif.com/

insight into the psychological advantages and disadvantages of each, and links to real-life examples of those patterns in action.

WHAT ISN'T CONSENT

Let's remind ourselves of what does not constitute consent. This isn't a matter of personal taste, remember: these reflect the judgments which privacy regulators have made in previous cases.

Actions that do not count as valid, freely-given consent include:

- Silence, inactivity, or no action at all (such as closing the consent window).
- Consent that is pre-ticked, or opted-in, by default.
- Clicking the only button available, such as "Accept all," with no choices or options.
- Scrolling down or swiping through (gestures, such as a facial recognition nod, can constitute consent if that is explicitly clarified up front).
- "Click fatigue," such as making the user withdraw consent for every tracker through separate means,

including features, vendors, and legitimate interest, or making the user withdraw consent for each vendor one at a time, with no "Reject all" option.

- "Userism," which means expecting the user to both understand and successfully navigate a deliberately layered consent process that is more complicated than a 1990s CD-ROM adventure game,[28] and then calling them stupid for not winning on the first try.

- Requiring convoluted, difficult, or diversionary means to withdraw consent, such as having to phone a call centre or send an email to a dedicated address.

- Using legitimate interest as an opt-in, alongside or in lieu of active consent.

- Bundling up consent as part of general terms and conditions.

- Blocking access to a site, such as a news site, behind a "cookie wall."

- Requiring consent to things not related to a transaction, such as marketing, in order to complete the transaction, or bundling up the consent with the transaction.

28. I see you, Peter Gabriel.

- Putting in a time limit for a user to decline consent before they are assumed to have opted in (there is no time limit in the European model).

Many of these invalid consent examples cross the line from passive laziness to calculated malice. There's a term for those.

DECEPTIVE DESIGNS

If you don't know what a "dark pattern" is, you certainly know what one looks like. Dark patterns – which should more appropriately be called deceptive designs – are visual interfaces deliberately, knowingly, and maliciously created to deny people their data rights, deprive them of their freedoms, manipulate them towards handing their data to those who misuse it, and undermine the principle of freely given consent.

They're nasty things, deployed by nasty people.

When Harry Brignull invented the term "dark patterns" in 2010,[29] he had no way of knowing that his observations would evolve into a professional discipline for academics[30] and researchers.[31] (He also had no idea he was about to have a second career as an expert witness in court cases against companies that have deployed deceptive designs, but he has indeed.)[32]

29. https://www.deceptive.design/
30. https://dark.privacypatterns.eu/
31. https://darkpatterns.uxp2.com/
32. https://smashed.by/arenavintuit

Since Harry's initial work, many new taxonomies and terms have been devised to classify the dozens of commonly deployed patterns, but all of them engage in one of roughly five practices:

- *Confusing* the user by overloading and overwhelming the user, or manipulating their emotions, which causes them to make decisions they normally wouldn't make.

- *Interfering* with a user's interface, in a such way that they simply can't do the thing they want, or exercise the consents they would prefer.

- *Obstructing* the user's path with unnecessary virtual clutter in ways that prevent them from making good choices.

- *Sneaking/hiding* the information that a user deserves to see, or the rights they can invoke, in a way that pushes them into a choice they did not want or expect.

- *Forcing* a user to do something they don't necessarily need or want in order to do or get the thing they do need or want.

Deceptive designs feed directly into the abuses of data, which we'll discuss in Part III, that have diminished the

open web for so many. They have no place in any respectable work, least of all yours.

If you're keen to know more, there's an entire book from Smashing on how to create good design patterns without resorting to deceptive designs. *Click!* by Paul Boag also includes some good advice on how to curtail the use of dark patterns (by others, of course) by appealing to their business's bottom line rather than their emotions.[33]

REGULATION IS COMING

In the years to come – very soon, in fact – deceptive designs and dark patterns will become the highest priorities for legislative action around the world. Indeed, some excellent work has gone into advising policymakers on how to integrate meaningful action against deceptive design into future legislation. We can only hope that the worst design patterns will become a matter of regulatory enforcement rather than public shaming, and that the laws put in place will deal with the issue in a fast and fair manner.

However, you shouldn't wait for deceptive design to become an issue for laws and regulators. Don't engage in the practice, and call it out when you see it, but always do so in a way that encourages positive mitigations and also points to the resources that will make them possible.

33. https://smashed.by/clickbook

In a world of dark patterns, be the light.

Professionals who are looking into the potential regulation of dark patterns should study *Dark Patterns and Design Policy*,[34] *Dark Patterns: Regulating Digital Design*,[35] *Regulating Privacy Dark Patterns in Practice—Drawing Inspiration from California Privacy Rights Act*,[36] and the EDPB's guidelines on dark patterns.[37] These works reflect a healthy difference of opinion on whether the regulation of dark patterns should be a function of privacy law or consumer law, and whether the solution is new regulations or better enforcement of existing ones.

34. https://smashed.by/datasociety
35. https://smashed.by/stiftungnv
36. https://smashed.by/californiaprivacy
37. https://smashed.by/edpbguidelines

PART THREE

Privacy and Your Users

“If you think your job is writing code and not understanding politics and the political implications of technology

Not only are you bad at your job, you are dangerously bad at your job and a threat to others”

—Aurynn Shaw, Twitter, August 28, 2019
https://smashed.by/aurynn

PART THREE

Privacy and Your Users

So far we've covered the legal and foundational values behind a healthy approach to privacy. In this section, we're going to learn how to consider the power dynamics of what you create, regardless of the role you play.

After all, it's never just about your own privacy. You may feel that you have nothing to hide and nothing to fear. And you may feel that information wants to be free.

But the work you put into the world isn't about you, and isn't about your own concerns. Sidelining your own privacy sidelines the privacy of others too. They may not be as safe, as privileged, or as protected as you.

And as I know all too well, there may come a day when you find yourself needing those protections because life hasn't unfolded the way you might have hoped it would. So let's take a user-centric look at the biggest obstacles to privacy on the web, and the role you can play in mitigating them.

Many of these areas involve the interplay of regulation and the courts, but I'm going to avoid discussing them as much as possible – after all, this book is about general best

practice principles, not a legal reference manual – but you do need to take the time to learn about these regulations and the issues around them as you progress your work on the open web.

Cookies and Adtech

If you thought online privacy was just about cookies – and for some reason so many people do – it's taken until page 190 of this book for you to get there.

In fact, cookies – or rather, the misinformation around them – made it far harder to teach developers about privacy than it should have been. By the time I'd finished clearing up that misinformation (and answered audience questions that were really comments that were really proxy rants about the European Union directed at me) there wasn't much energy left to get to the other stuff. But get through cookies we must.

As you learned on page 66 ("ePrivacy"), the rules on cookie consent in Europe aren't from GDPR, nor do they have anything to do with it; they come from the ePrivacy Directive. That Directive, as you're aware, is currently the subject of a long-running soap opera ahead of its revision and modernization. For now, though, we'll deal with the law as it is.

The Directive requires you to:

1. Inform your users about what cookies you're using.

2. Inform your users about why you're using them.

3. Provide your users with a means to opt-out of those cookies' use.[1]

Most cookie consent pop-ups will distinguish between essential cookies, which help a service to function, and nonessential cookies, such as advertising. Most will also distinguish between first-party cookies, which reside on a service, and third-party cookies, which send data externally.

What, as they say, could possibly go wrong? Well, we all know. There's no doubt that cookie consent pop-ups have been misused, abused, and corrupted to a point where they do not protect anyone's privacy in the slightest. Whether it was the misuse of legitimate interest, the obstinate insistence that all data tracking is "necessary," or the sheer amount of tracking – in the thousands – deployed on most commercial sites, the pop-ups are now the web's number one source of grief.

In fact, the main provider of cookie pop-ups in Europe, the Internet Advertising Bureau (IAB), was found to be in com-

1. https://smashed.by/cookies

plete violation of the European privacy regime, and was ordered to delete all the data it collected about anyone who ever had the misfortune to encounter one of their cookie pop-ups.[2] Which, of course, means every single person in Europe.

Still, the law as it currently stands on the books requires you to use some form of consent mechanism to give your users those rights over the cookies you set. The law does not specify what those consent mechanisms should look like or how they work. So there are many things you can do to make your users' cookie consent process as painless – and legally compliant – as possible.[3] They could include:

- Setting all nonessential consents and legitimate interests to **off** by default.

- Providing universal settings that allow opting out of all consent and legitimate interest, as opposed to making users manually trigger both settings for every single provider.

- Not forcing users to go through the triple hell of universal settings, partner settings, and legitimate interest settings – a process which is clearly designed to confuse people into giving consent even when they think they haven't.

2. https://smashed.by/iabdecision
3. Smashing has some inspiration for you here: https://smashed.by/cookieconsent

- Perhaps most important of all: Not using privacy-invasive adtech, tracking, or data harvesting in the first place, so that your users don't have to opt out of those consents or use those awful pop-ups in the first place. Magic!

> There are services such as Your Online Choices, where you can opt-out of behavioural and advertising tracking across the web,[4] but the problems here are obvious. First, those preferences are reset every time you clear your browser cache, including (ironically) cookies. And second, those services let you decline consent, but most will then opt you in without your consent under the abuse of legitimate interest. To protect your privacy across the web, you'll need to combine the use of a service like this with browser extensions, ad blockers, and universal browser settings. You can also educate your users and clients about ways they can protect themselves that way. And no, privacy should not be this hard.

4. http://www.youronlinechoices.com/

As the future of cookie pop-ups returns to the political sphere, let's be clear: everyone hates cookie pop-ups. I certainly do. But getting rid of those pop-ups, but not the adtech, the tracking, the surveillance, or the data harvesting that those pop-ups inform you about, is like taking the batteries out of the smoke alarm to stop that annoying beeping sound. The thing is, your house is still on fire. The pop-ups tell you who is tracking you and why, and what they're doing with your data, and blocking those pop-ups or getting rid of them altogether won't change that.

We all need to play a role in finding a better way forward, both technically and politically, to protect our own privacy as well as that of our users. I know it might seem that there's very little you can do to make a difference in a world where it's acceptable for newspapers to put over 1,400 trackers and data harvesters on a single news story (really) through the abuse of legitimate interest, or where your TV is snitching on you to a data broker through consents you didn't realize you were opted into in "Settings." But you can ensure that your work doesn't use privacy-invasive third-party trackers or is dependent on adtech – or hopefully both – in a way that means you don't need those hellish pop-ups in the first place.

By the way, don't forget that the rules on cookies and consent don't just apply to websites. They also apply to

apps, wearables, IoT devices (yes, your television, your car, and your refrigerator), and any other system or device that deploys them to capture personal data.

Analytics and Tracking

As I've mentioned elsewhere in this book, I am not an analytics absolutist. I rely on a responsible analytics application to tell me which of my content is popular, to provide me with insight into where my content is shared, and to help me learn which institutions are reading my content. (I see you, UK and European Parliaments. You know you miss me.)

And for what it's worth, when I have had trouble with harassment and stalking (as most internet professionals do), analytics have provided me with a layer of security, particularly when that harassment crossed the line from online annoyance to real-life threat.

Through the responsible use of privacy-conscious analytics, I have been able to gain those insights without invading the personal privacy of my visitors, or linking their visits to their actual human identities (stalkers exempted), or inadvertently sharing their data with third parties for marketing purposes. That experience is living proof that it's possible to achieve a happy middle ground with analytics.

The hard part, however, is getting there. Because, as we're all aware, analytics are one area where most site and service administrators have been guilty of collecting too much data and violating their users' privacy without even being conscious or aware of it. And we all know why. For many years, it was perfectly normal to be told "just add Google Analytics" to your site as simply another step in the pre-launch process, whether that advice came from a conference speaker or a startup advisor. with no pause or consideration. It was just a thing you did.

Sadly, that has meant that the first and only time that Google Analytics' privacy risks (and legal complications) came to the attention of most site administrators was in the aftermath of regulatory action, or worse, harassment and threats. Additionally, as of this writing, Google Analytics is part of the wider transatlantic battle on data flows,[5] and you've got enough battles of your own to fight without being dragged into that particular drama.[6]

So my advice to you, whatever analytics package you use, is this.

First, choose a package that collects *the minimal amount of data you need to make useful decisions and nothing more.* If at all possible, select this as a first-party utility that rests on your own servers.

5. https://smashed.by/privacyshield
6. This article will teach you how to use Google Analytics in a legally compliant manner in Europe, but it's not for the faint-hearted: https://smashed.by/googleanalytics

Second, choose a package which *does not collect, share, or aggregate your users' personal data, their browsing histories, or their internet use outside of your service, for any reason.* That will mean choosing a package that does not use advertising or adtech tracking, and that may well mean that you have to pay for the service.

And third, once you've settled on the right utility, *tweak the settings* to ensure that you're getting the clarity you need without inadvertently collecting additional personal data, which – regardless of whether anyone ever accesses it or not – still exists somewhere as personally identifiable data about real people. Set a realistic data retention period, and ensure that the data is fully encrypted.

I'll not tell you what service to use, but I will remind you that Google Analytics isn't the only service out there. Self-hosted utilities include Matomo, Fathom, Koko Analytics, Simple Analytics, GoatCounter, Plausible Analytics, Countly, and Ackee.

It's also worth noting that Google Analytics provides far more functionality than most people actually need. You may well decide that just a simple counter showing how many views a page got, which countries those visits came from, and which referrers sent those visits there – as you may have seen in the WordPress.org blog dashboard – is just the ticket.

I'll also remind you that **the use of analytics requires consent.** Make sure you choose a utility that allows your visitors to decline that consent if they so wish.

There are, of course, some situations where you should never use analytics, period. These include any service or application that deals with sensitive personal data, which you'll recall covers information about someone's health, sexual orientation, religion, political views, and so forth. Keeping those sites and services free from analytics and tracking isn't just a way to protect you; it's a way to avoid causing secondary damage to the very people you may be trying to help.

...BUT IT'S NOT JUST ANALYTICS!

As you review the analytics you've deployed into the things you've built, always remember to bring that same scrutiny to any form of tracker that collects personal data about your visitors and their use of your services. You may not be aware that European privacy law treats those trackers exactly the same as analytics, with the same precautions required and the same penalties applicable. You are now.

The most common form of tracker to fall afoul of this is Facebook pixels. As with Google Analytics, many very good site owners were given very bad advice about this form of

privacy-invasive tracking, and were told to "just put them in" without any further thought or scrutiny. Unfortunately, their use makes you complicit in some fairly astonishing abuses of privacy, and also puts you in violation of the European privacy model. Save yourself any further headaches and just get rid of them.

The same applies to the trackers in e-newsletters and emails which help you to understand what links your visitors clicked on. Because that data is directly linked to the identity of the person who clicked on those links, these trackers are particularly intrusive. Work with your email provider to find a way to capture click-through data that is aggregated and de-identified, and if they can't make that happen, take your business to a better provider.

Let's cover some further areas that will keep you on your toes about tracking, privacy notices, and consent.

Third-Party Sharing

As you learned in Part II, the third-party resources deployed on an average site or app are likely to include:

- Content delivery networks, including AWS and Cloudflare

- Image hosting services
- Contact form and survey providers
- Backup services
- Google Fonts
- Analytics, as we've just discussed
- Commenting utilities, like Disqus
- User avatars and comments
- Social media integrations
- Code embeds
- Location tracking services that show you the nearest shop, or help you find your friends
- Social media and multimedia embeds
- Shopping carts and payment gateways
- Screen-recording utilities that show where a visitor moved their mouse

- Error reporting and crash detecting services; and so on.

Not all third-party sharing is a privacy risk, of course; indeed, decentralization of your user data across services can actually help to protect user privacy. But you still have an obligation, both ethically and legally, to inform your users what data these services are collecting, how they are using it, and what you – as the data collector or processor – are doing with that data.

That's easy enough if you are a developer, but if you're not, there's a good chance that you will be surprised by how much data your site is sending out. First you have to look.

How do you find out what third-party sharing you've actually enabled? If you're reviewing a website, use a tool like the the European Data Protection Supervisor's Website Evidence Collector,[7] or the Mozilla Observatory.[8] If that's above your technical ability, you may be able to find a plug-in or module like Snitch, which works with your CMS.[9] For Android apps, use a tool like Exodus Privacy.[10]

These tools will not do the job for you, but they will give you an informative view of the traffic flowing out of your site. That, in turn, will help you to understand what data is being sent to these third parties, what portion of that data constitutes a privacy risk, how these services handle this data,

7. https://smashed.by/inspectionsoftware
8. https://observatory.mozilla.org/
9. https://smashed.by/snitch
10. https://exodus-privacy.eu.org/

and how they safeguard the privacy of the users it is about. You'll also gain a sense of how many of these services are abusing consent, legitimate interest, or both. Along the way, it will also give you a steer on which third-party services may not be necessary at all.

You'll need to note all of these third parties and the nature of the data sharing in your privacy notice (see page 171), as well as the legal basis (consent if it's on the level, legitimate interest if it's not) they use to collect your visitors' data. If those services are not essential to the site's infrastructure, such as screen-recording utilities, you'll need to ensure that visitors are able to decline their consent for those services.

More important than that, you'll also need to be prepared to answer questions from your users about whether or not some of those services are truly necessary, and why you rely on so many privacy-invasive services to build your product.

Social Networks

To many observers, the Cambridge Analytica scandal was a wake-up call about how deeply social networks had integrated themselves into web development practices as a whole. Silly games and quizzes, published on Facebook, were fronts for voter targeting and manipulation that cracked the foundations of democratic integrity. And one of

the many lessons we learned from that scandal is how hard we have to work to protect ourselves and our users from the data practices used by some social media sites.

In other words, you have a responsibility to not be complicit in these abuses. You can do that by being conscious of how dependent you are making your users on social media sites, and removing those dependencies.

For example:

- Don't require your users to use a social network login to access your site, service, or app. Allow them to create a standalone account.

- Allow your users to set their profiles to private, and to remove and/or block followers at any time.

- Do not set the social sharing of anything – user actions, data, or login status – to on by default, and do not make your users have to take specific actions to stop that default sharing.

- As we've already discussed, do not use any social sharing pixels, cookies, or trackers set to on by default without user consent – remember, in Europe that's illegal anyway.

- Do not use any social sharing pixels, cookies, or trackers that send user data to social networks even when they don't have an account on that service – Facebook is notoriously guilty of this.

- If you're embedding videos, use the privacy-enhanced mode, which does not utilize tracking cookies. You should also disable any options to show suggested videos once the embedded video finishes playing, as this can take your users into an algorithmic data collection rabbit hole.

- Consider using privacy-friendly alternatives to default social sharing options, such as buttons, which have all the functions your users need without sending their personal data along with it. Social Share Privacy[11] and Sharingbuttons.io are good places to start.

> I had to go to war with Spotify over their refusal to allow users to remove or block followers. Countless users had complained about the inability to remove or block followers, which facilitated stalking and harassment, often from violent former partners. Even when harassment was not overt, many users weren't even aware that

11. https://smashed.by/socialprivacy

> Spotify was set up as a social network to allow following by default, and had no idea that every song they listened to was being monitored by strangers. Spotify eventually capitulated and implemented what should have been a simple feature from the very start, but it never should have taken eight years and thousands of desperate pleas.
>
> See *https://smashed.by/spotifystalkers*

Location Data

If your site or service uses location data, I want you to pay particular attention to the ways it can be misused. Thankfully, managing location data is one area that is becoming easier, largely thanks to system-wide changes deployed on iOS and Apple. But don't rely on your OS to do the job for you.

As you design, program, or iterate, make sure location data and Bluetooth are always turned off by default, and that the user always has total control of it at all times. Make sure that any location data is not retained, and make sure that the location data is not attached to other forms of personally identifiable data.

What do I mean by that? As I write the very final edits of this book, teenagers in Ukraine are using TikTok to post videos of their everyday lives in hiding from the war raging above. Those videos' internal metadata include the location data showing where they were when they uploaded them. That means that someone with access to TikTok's internal systems – for example, a hostile government – could locate exactly where those teenagers are hiding. Likewise, it has taken a recent high-profile court ruling in the US for Americans to learn that their private visits to their private healthcare providers, inclusive of location data linked to their full personal identities, are marketed and sold by data brokers to anyone who wants it - including those parties who might object to the healthcare that person was seeking. What could follow from that does not bear thinking about.

But it is your job to think about it, and to understand why the responsible deployment of location data is about much more than getting your dinner delivered to the right place.

Data Profiling and Brokers

Now let's discuss some of the wider issues around user privacy which impact all of us, in ways that go far beyond the code and compliance of the things we build. You can't solve any of these problems on your own, but you have a small but important role to play in fixing all of them.

The first and most urgent issue is data profiling, a practice that for many of this book's readers is the biggest threat to their personal privacy, and one far more nefarious than adtech or social networks. That's because data brokers work in the shadows in a barely regulated sector, and most people aren't even aware of their existence – or the control these companies exercise over their daily lives.[12]

Profiling is about more than the basic datasets held about individuals. Profiling is when that data is mixed with other sources to create profiles of individuals, and those profiles are used to make often life-changing decisions about them. Combining a user's browsing habits with the data on their Facebook profile to serve them targeted ads is a form of profiling. So is a bank using data about the other people who live on your street to decide whether to give you a loan. So is a health insurance company using a list of everything you've bought at the supermarket – conveniently located on your supermarket loyalty card – to decide how much to hike your premiums.

Where your work on the web contributes to this is obvious: if you are sending data to third parties, you are contributing to data profiling. You may even be doing so without realizing it; for example, if you have included an ad network in your app, or if you use social media pixels. What you are really doing is contributing to a larger data file, somewhere, which tracks an individual's

12. https://smashed.by/databrokers

- salary and performance at work
- economic situation
- health and medical history
- personal preferences
- reliability and character
- behavior and conduct
- location and movements, often in real time
- family members and relatives
- friends, and their friends
- home addresses, and their family members' home addresses

and uses all of that information for entirely negative purposes.

The European privacy model has some safeguards to provide user rights over data profiling, mostly within GDPR, which includes provisions related to the automated processing of personal data, and the use of personal data to evaluate individuals without their knowledge. While these

provisions were aimed at advertisers and marketers, they apply just as clearly to the roles of data brokers.

Unfortunately, the brokers don't care. That means the responsibility falls to you to make sure that you're not contributing to the power abuses inflicted by data profilers.

So whether your business model includes the active collection and processing of data about people, or if that information is merely a byproduct of it, take steps to minimize the amount of data that brokers have at their disposal to exploit.

- Build in Privacy by Design principles, including a privacy impact assessment that considers the information which could be passed to a data broker.

- Explain clearly and transparently to your users what data is being collected, what it is being aggregated with, and where it is being sent, including any information shared with data brokers.

- Obtain explicit and verifiable consent to collect data for profiling.

- Take all the precautions required for any sensitive personal data that could be used or aggregated for the purposes of profiling.

- As the European model allows, stop processing the data of individuals for the purposes of behavioural tracking or data profiling when they invoke their rights to do so.

- Ensure that your contracts with third-party providers prohibit the sharing or reselling of your users' data with data brokers, both through consent and through legitimate interest, and end commercial relationships with those providers who engage in the practice.

Children's Privacy

For many of you, this will be the part of online privacy that causes you the most sleepless nights.

We all want to keep our children safe online, whether those risks come from adtech surveillance, edtech monitoring, bullies from school (be they students or teachers), and from people with malicious intentions. But children have a right to privacy too; indeed, that right is critical to allowing them to form their own identities, beliefs, and worldviews.

The trick is to get that balance right and to provide young people with a safe online environment that protects them from data abuses and other harms, and allows them to form their own critical and thinking skills, without pa-

tronizing them, restricting their rights, or infantilizing the open web for adults.

After all, children need privacy from adults as much as they need to be protected by them. Achieving that balance is your job.

WHAT THE LAWS SAY

Children's online privacy is one area where you really do need to do your homework on the laws, regulations, and privacy guidelines which are applicable to your target markets. These include GDPR's provisions relating to children, as well as the Children's Online Privacy Protection Act (COPPA),[13] the main US law (as of this writing) dealing with children's privacy.[14] We'll do a very quick overview here, but the rest is down to you.

The European Model

As ever, the European privacy model will give you a good baseline to follow regardless of where you are. It imposes some common-sense requirements on your data collection and consent processes.

The first and trickiest question you'll need to deal with is: who is a child? GDPR does not define that (different EU

13. https://smashed.by/coppa
14. If you participate in any lawmaking process to create children's privacy regulations, the UNICEF principles on better governance of children's data, which I was privileged to contribute to, have some great suggestions on achieving the right balance. https://smashed.by/childrensdata

member states have different legal definitions of a child, currently ranging from under 13 up to 16). GDPR does, however, define children as vulnerable individuals who require specific protection. Check if the jurisdictions you work in have a fixed definition of what a child is, though that is not a license to disrespect a child's privacy the day they reach the age of maturity.

The second question you'll need to deal with is what data you're collecting on child users and why. You'll need to give this some extra thought in your PIA process, but I'll make it easy for you: don't use automated data profiling, don't use adtech tracking, don't use ads, don't use cookies, don't use third-party monitoring, don't use opted-in consent, don't use opted-in legitimate interest, and don't use any of the other privacy threats we have discussed in this book, of any kind, for any reason. Nothing whatsoever, and no excuses. Got it?

The third question you'll need to deal with is how you collect and process the good data you do need to provide the service. (This is a useful time to remember that your PIA can be requisitioned by a data protection authority, who will want to see the homework you did on children's privacy.)

To put it as simply as possible: where children are concerned, you need to take all the processes you've already

established around user rights and supercharge them. For every point of data you collect, every service you use, and every consent basis you use to justify it, you must carefully document your reasoning for doing so above and beyond the requirements that apply to adult data.

For example, under GDPR, children must give consent to the collection and use of their data, and to do so they must be given the opportunity to read a comprehensive privacy notice, as is standard under GDPR. The difference here is that any privacy notice targeting children must be written in language that a child can understand. This means explaining what data you are requesting, why you are requesting it, and what you are going to do with it, in words that an older child or young teenager can easily comprehend. And this means you have to be completely honest and upfront with kids, using words crafted for their benefit, not for yours.

Forget long legal paragraphs or dark pattern doublespeak. Think simple language, a friendly tone, and big icons. Don't be sarcastic or overly clever, though, and don't patronize children either. In fact, you should use this challenge as an opportunity to set children on the path to exercising responsible privacy behavior for life. For example, remind them not to reveal personal details about themselves or their families as they use your app.

Parental Consent

If your website or app targets children 16 or under, GDPR requires you to obtain adult consent for the processing of that child's data. The consent that a child gives to the use of an online service, such as the acceptance of the terms of the child-friendly privacy notice, is contingent on the consent of the parent or guardian. A child's acceptance of your privacy notice without parental consent, for example, is not valid consent.

GDPR requires data controllers to make reasonable efforts to verify parental consent. This may include an extra step to make the parent confirm their identity, which can cause additional issues that we'll get to in a minute.

The only exception to the parental consent rule applies to online services providing preventative or counselling services directly to children, such as apps provided by helplines.

Scope Creep

GDPR requires data controllers to make reasonable efforts to verify parental consent, "taking into consideration available technology."[15] For online services targeting children, age verification solutions are often deployed as well. This, unfortunately, has caused a sort of legislative scope creep which sees parental monitoring and age gating – *of*

15. GDPR, Chapter II, Article 8

all content, for all users, regardless of age or risk or harm – as the magic technical solution to online safety. (Think cookie pop-ups, but for age verification.)

As these proposed laws approach reality, I want you to be aware of the three issues you'll face because of them.

The first is the paradox that safeguarding children's data by technical means, such as parental monitoring or age verification, can actually involve collecting *more* data. It is not unheard of, for example, for social networking sites to request a scanned copy of a child's birth certificate as proof of age and the parental relationship. If that birth certificate is transferred outside the EU for the verification process, there are now three issues – the child's age, the parent's sensitive personal data, and an international data transfer – which you must be prepared to address in full accordance with GDPR's wider standards.

The second issue is that children can and will lie, as will adults. You must prove that any age verification and parental consent mechanisms you have deployed have been exercised in good faith regardless of the user's intentions. You must also be prepared to take quick action when a lie has been caught out. For example, if a parent contacts your app studio with a screengrab of an account their child has

created without parental consent on a friend's phone, you should be prepared to delete the account without subjecting the parent to an intrusive identity verification process.

And the third is that parental monitoring age verification, if mandated by law in a disproportionate manner, is a form of age gating. It imposes a requirement on service providers, like you, to engage in the business of collecting multiple points of personal data on individuals, before they would be allowed to do something as simple as read your content. For what it's worth, it also blocks off vast swathes of innocent and non-harmful content behind an age wall (like a paywall) in the name of child protection. As these restrictions draw closer to reality, you need to make clear that they are not the way to protect children or anyone.

Growing Up Online

Among the best things contained within GDPR are provisions on the "right to be forgotten" in the context of children's data " where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet. The data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child."[16]

16. GDPR, Recital 65

What that means is that any data you have collected about a child – *even if that child is now an adult* – must be removed at their request, regardless of the consent basis.

And yes, that also applies to the data placed on the internet by parents, grandparents, and other well-meaning family members who overshared every private moment of a child's life without their consent. Children have the right – even before they reach adulthood – to request that a service take down that oversharing and delete any data connected with it. I highly recommend you help those children and adults to do so.

A Quick Note on COPPA

COPPA has been amended several times and is constantly evolving.[17] Its administrative agency, the Federal Trade Commission, has clarified that COPPA applies to non-US websites that "are directed to children in the U.S. or knowingly collect information from children in the U.S."[18] Other US regulations pertaining to children are in the draft stage.

COPPA applies to children under the age of 13. It requires operators of sites and services targeting children to – well, do everything we've discussed above: provide clear routes for user rights, consent, and deletion. It imposes those rules,

17. https://smashed.by/childrenprivacy
18. https://smashed.by/coppa

however, without the backing of a universal data privacy law, or a recognition of privacy as a fundamental human right.

In other words, that means that you have extra work to do to make sure that COPPA's provisions don't provide a privacy-safe environment for children which evaporates on their thirteenth birthday.

HEADING INTO THE FUTURE

By now, you may be reflecting on how good-faith efforts to get children's online privacy *right* can so easily get it *wrong*. Legislators do precisely that, a lot. Some of the standards and regulations drafted around children's privacy risk creating a two-tier internet, or one which is highly infantilized. Others propose so many restrictions and limitations (in a "won't somebody think of the children" way) that they amount to a curtailment of privacy and freedom of speech for everyone.

While those policymakers and legislators duke it out, your task is to protect children's privacy in a way that eliminates risks and data abuses in the first place, provides a strong baseline of privacy for everyone, and does not create new wrongs in an attempt to put things right.

In other words: stick to your common-sense privacy principles (from page 32), and a healthy respect for user rights, regardless of a person's age, and you're already halfway there.

IoT and Connected Technology

For many of you reading this book, your careers will be spent developing for the internet of things (IoT) and connected technology, and not for screens. This could mean everything from smartwatch apps to healthcare devices to domestic robots, and that's to say nothing of Coronavirus tech. (Will we ever get used to having our temperatures taken by tablets at the entrances of public buildings? I hope not.)

In that regard, the IoT could become a battleground for user privacy. But if it's developed in the right way, by the right people, the IoT could help us achieve the greatest promise of technology with the fewest abuses of our privacy. Making that happen will be your job. If you approach your work on IoT and connected technology with a thorough understanding of the privacy principles we've discussed in this book, as well as a keen understanding that the IoT is as much about metadata privacy as it is about actively provided information, you will be able to build IoT applications that benefit all of society while avoiding the mistakes which could exploit it.

Fortunately, there is some incredible work being done right now to assist developers working in the IoT on building healthy approaches to user privacy. One of them was the VIRT-EU consortium, a European project dedicated to developing best practice frameworks for IoT developers. They have published a privacy impact assessment framework specifically for IoT devices.[19]

VIRT-EU's approach goes beyond the legal aspects of compliance, such as GDPR, to cover the ethical and societal risks of emerging technologies, such as:

- Are the IoT device and associated software used for predictive purposes, or for classifying users according to their conditions, behavior, and preferences?
- Does the data collection take place in a publicly accessible area?
- Does the technology allow the users or other people affected to be aware of the monitoring in process?
- Does the device display any signs when recording video and/or audio in its surroundings?
- Will users be monitored by the device in private areas such as bathrooms?

19. https://smashed.by/pesia

- Will the microphone in the device have a physical switch?
- Will the device receive advertising messages from third parties?

These checkpoints will give you a great foundation for your work in IoT, and provide you with plenty of creative inspiration for tackling tomorrow's challenges.

Domestic Surveillance and Imbalances of Power

In response to the threats inherent to our digital lives – online abuse, harassment, and exploitation – a market has sprung up promoting a range of products, services, and innovations designed to mitigate those threats. Some of these products are sold as parental monitoring and child protection software to help parents keep an eye on their kids' online activity; some of them are sold as content filtering applications to block harmful content, though "harmful" is a matter of personal opinion; some of them are sold as employee monitoring software to supervise home-based remote workers and keep them productive; and some of them are grouped under the marketing name of "safety tech."

But I'm here to tell you that two wrongs don't make a right. You don't protect privacy by violating it, you don't defend freedom of speech by censoring it, and you don't foster autonomy through surveillance. Without a healthy regard for privacy, and the basic rights of end users, the development and deployment of these products can cause far worse harms than the threats their glitzy marketing pitches would claim to fix.

What's scarier still is that many governments are looking towards these troublesome digital solutions, and even promoting them, as a means of solving societal problems while boosting their homegrown tech sectors. What, as they say, could possibly go wrong?

Well, hopefully not much, with a little help from you. If you are developing software, applications, or devices that fall under these descriptions, you have an obligation to ask yourself some serious questions about the products you are building. These questions go beyond the legal requirements of a PIA, or the philosophical aspects of an ethics questionnaire,[20] to force you to think about the ways your product can – and will – be misused and abused.

These questions might include:

- Who does this product serve, if not the user?

20. https://smashed.by/dataethics

- Who has the power in the relationship between the person deploying the product and the person being made to use it?

- How could this product enable abuses of power from the person deploying the product over the person being made to use it?

- Who has access to the data about the person being made to use it, in addition to the person deploying it?

- Will the user of the product be consulted about its use?

- Will the user of the product be informed about its use?

- Will the user of the product be allowed to give consent to its use? (Remember, even if the user is a child, they must give their active and informed consent.)

- Will the user of this product fully understand that they are under digital surveillance?

- Will the user of this product fully understand who is surveilling them, for what purpose, and what rights they have over the data collected within that surveillance?

- What are the consequences to the user of the product if they decline to give their consent to its use?
- Could the harms inherent in the misuse of this product exceed the promised advantages?
- Is the product or service supported by adtech, trackers, or other forms of commercial surveillance in addition to the content-based monitoring within the product? Do third parties have access to the user's data? Are they monetizing it?
- How is the product being marketed? Is it clearly being sold in a way that implies it is a tool for control and coercion?
- Could this product enable domestic abuse?
- Could this product enable stalking and harassment?
- Could this product enable control and coercion in a personal or professional relationship?
- What mitigations have you put in place to prevent those abuses?

- What is our contingency plan for how we will respond when a news story appears about a way that our product was misused?

- What is our legal strategy for when a criminal case comes to trial centred around the misuse of our product?

The final question should be the one which weighs on you heaviest:

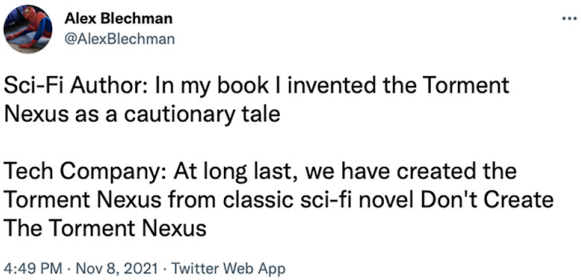
- How am I going to feel about myself if I continue to work for this company and develop this product?

State Surveillance and Persecution

The open web didn't create the world we live in, but it ties us together despite it. Technology can save us and bring us together, or it can damage the people we love and the societies we live in.

I know that thinking of the ways the things you build could be misused, for domestic surveillance and imbalances of power, was a difficult exercise for you. But now I want you to go beyond that.

As you design, develop, or iterate, you must always – *always* – think of the ways your work could be abused, whether through scope creep, exploitation, or deliberate misuse, by governments and authorities with malicious intentions. Privacy, after all, is the first and easiest right to destroy. Other rights follow on from that.



https://smashed.by/blechman

It may be helpful to think of these threats as encompassing two areas: *targeted* surveillance, where particular groups are singled out for monitoring and persecution; and *mass* surveillance, where all citizens are at risk regardless of who they are.

None of these questions are the stuff of sci-fi anymore. These are the lives of the people you know. And someday soon, it might be you.

- What is the vision for your product in five or ten years' time?
- How is your product being marketed and sold, and to whom?
- Where is your product being marketed, in which countries?
- How will your product work in a country defined by the repression of minorities? By the restriction of human rights and civil liberties? By international condemnation and sanctions?
- Who is on your company's board? Who is on your management team? What are their backgrounds? Who are their connections? What are their political views?
- What internal processes does your company use to ensure your work complies with privacy laws and human rights frameworks? How are those processes reported to the board and management? Who signs off on them?
- Does your service collect data about people's sexual orientations in countries where that might be a crime?

- Does your service collect data about people's religions or ethnicity in countries where they are persecuted minorities?

- Can the adtech and tracking you use be used to identify people, like journalists and activists, who hold governments to account?

- Can the adtech and tracking you use be used to identify people, such as people of a certain race, nationality, or religion, who are at risk?

- Could the biometrics in your system, such as facial recognition, be used to identify and oppress vulnerable minorities?

- Can the data in your system be used for mass profiling, also known as social credit scores?

- Does the lack of end-to-end encryption in your system make the data interceptable by malicious governments and authorities?

- Does the use of location data in your system make it easy for an oppressive regime to find someone?

- Can the metadata in your system be linked to other information, such as data profiles or government databases, about people?

- Have you thought about how you will respond when a government or authority with malicious intentions asks you to provide them with data on specific people or groups of people?

- Have you thought about how you will respond when a government or authority with malicious intentions demands access to your systems, or even attempts to nationalize your company?

- Have you thought about how you will respond when a government or authority with malicious intentions makes personal threats against your company's management, employees, or even you, because you refuse to compromise the privacy – or humanity – of the people in your data?

And last but not least:

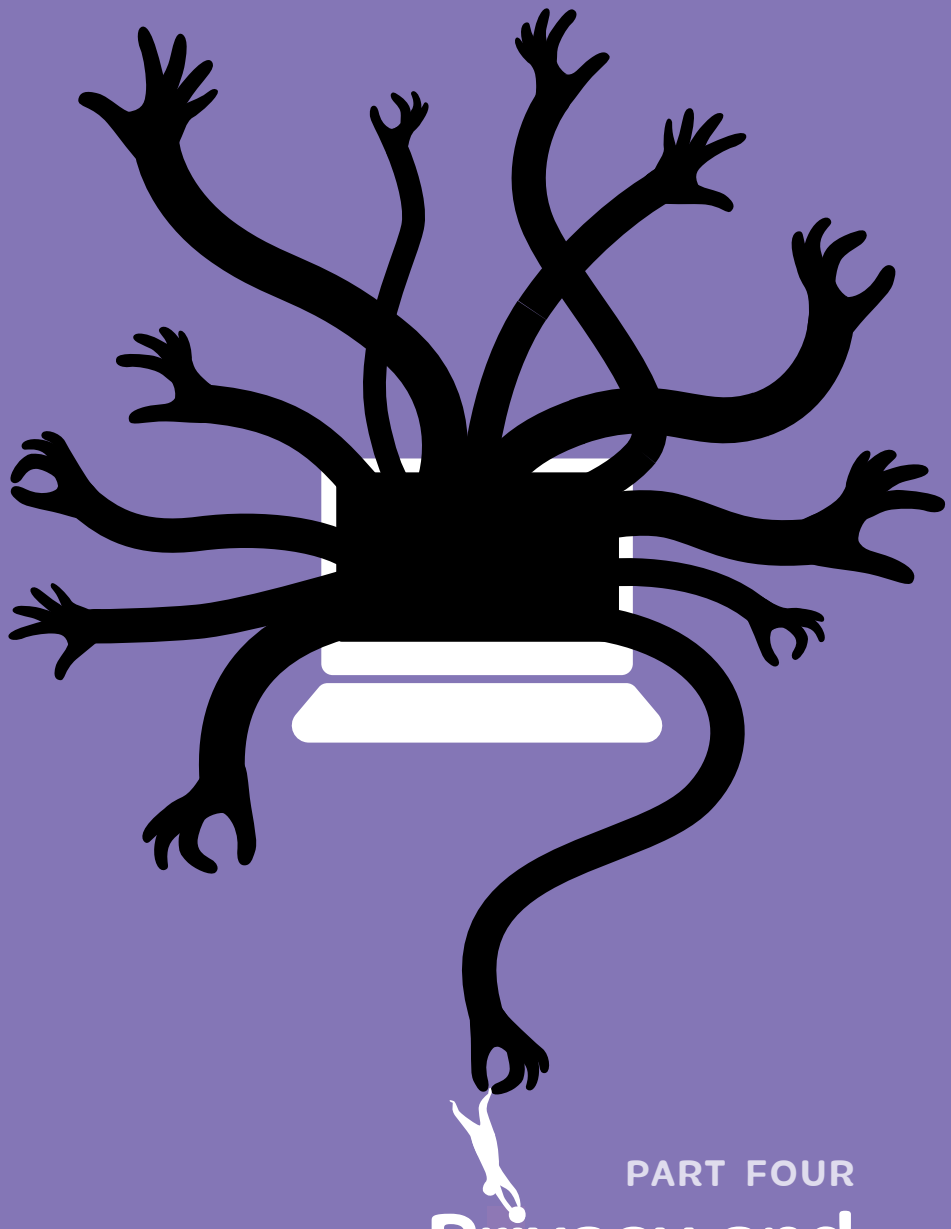
- Have you implemented a backdoor to regain control over a system?

- Have you implemented a means to delete personal data about people?

- Have you implemented a kill switch to destroy the system?

You see, the most important thing you might ever do in your career on the web might be to drop a table.

When the time is right, you'll know.



PART FOUR

Privacy and Your Future

Stop stop talking 'bout
who's to blame

When all that counts
is how to change

—James, "Born of Frustration" (1992)[1]

PART FOUR

Privacy and Your Future

Everything this book has discussed so far is reactive. It is a response to the world which has shaped your work on the web today. As a privacy-conscious web professional, though, the future of your work and the web you build it on is in your hands. You have a role to play in making the web a better place for your users, but you have an equally important role to play in making the web a better place for the developers, designers, and project managers who will follow in your footsteps. How can you lay the ground for them to build a better web for tomorrow's users?

I want to suggest a few critical areas where you can make a difference right away. They're as much about the positive and constructive actions you should take as they are about the negative and ugly actions you should avoid.

Let's do this.

Shape the Future of Privacy Legislation

The upcoming years will see new privacy laws, regulations, and frameworks coming into play around the world. Some of them will be very good. Some of them will be very bad.

1. This and other tunes you'll find in this book - some more visible than others – can be heard here https://smashed.by/tunesfromthebook

Some of them will be drafted in the interests of users. Some of them will be drafted in the interests of corporations. Some of them will be grounded in universal privacy principles like the ones I've described in this book. Some of them will be grounded in an ulterior motive to restrict, censor, and control the open web. Some of them will take on board the best lessons learned about protecting user privacy during the pandemic. And some of them will take on the worst lessons learned about restricting civil liberties during the pandemic.

How can you distinguish a good draft law from a bad one? What does it really come down to after all the heated rhetoric passes into the hands of a drafting committee? Here are a few things I want you to look out for in the laws which will shape the future of your work.[2]

WHAT'S GOOD

- **Active opt-in consent for user data**. This, after all, is the root of most privacy problems. Active opt-in consent should apply to all users in all situations. It should apply to background and third-party sharing as well as to the direct relationship a user has with a service.

- **Brutally honest disclosure** of what companies are doing with your data, where they got it from (including

2. Many of these checkpoints were inspired by the Electronic Frontier Foundation https://smashed.by/eff

third parties), who they are sharing it with, and what rights you have over it.

- **The right to data portability** for users who want to take their data to another service – and as a means of promoting innovation and competition.

- **The right to data deletion** without costs, explanation, or undue burdens. In the coming years, this will become especially important to uphold the privacy rights of young people whose parents have overshared every moment of their private lives online without their consent.

- **The requirement to prepare for, respond to, and pay the price for data breaches**. Nobody should need to feel that the only thing they can do when a company loses their data, yet again, is shrug helplessly.

- **Universal application of privacy laws at a national/federal level**. One omnibus privacy law is easier to comply with than twenty, or thirty, or fifty.

- **Universal application of privacy laws across businesses of all sizes**. Exempting small businesses from privacy protections would have exempted the companies within the Cambridge Analytica scandal. Compli-

ance burdens must be reasonable and proportionate, but they can never be absent based on size alone.

- **User recourse** for misuses and abuses of their data. Users should have public rights, such as the enforcement options available through data protection regulators, as well as private rights, such as the option to file class-action lawsuits.

- **A well-funded and empowered data protection regulator**. The best privacy rules in the world can only be as good as the regulator behind them. They need the tools to educate the public on privacy, and the teeth to enforce the law. They also need the funds to hire the right people and to keep them; data protection authorities are often seen as revolving doors to private sector jobs paying exponentially higher salaries. It is also critical that the regulator exists as an independent government agency, not connected to, or unduly influenced by, any other branch, and the leadership should be civil servants, not political appointments.

- **Treating privacy as its own law and principle**. Privacy must be established as its own set of rights and values, grounded in international human rights standards, which stand alongside other rules about contracts, property, or terms and conditions. Privacy cannot be a subcategory of any one of them.

WHAT'S BAD

- **Consent fatigue**. Consent rules should not mandate excessive pop-ups, dropdowns, modals, cookie walls, or any of the other things we've grown to know and hate. Legislation must find the happy middle ground between facilitating active-opt ins and creating consent blindness.

- **Abuse of legitimate interest**. Privacy laws need to find better ways of allowing for "just in case" uses of data which are not exploited so badly – as GDPR's legitimate interest use is – that they create a loophole big enough to drive a juggernaut through.

- **Privacy as a means of overriding other legal rights and protections**. Good privacy legislation should never be exploited as a means of evading scrutiny, responsibility, or accountability for actions which had legal ramifications beyond privacy.

- **Data portability as an abuse of other users' rights**. In a world where our data is entangled, the right for me to extract my own content should not give me ownership over content I may have contributed to, but which is owned by others.

- **Data deletion as a means of censorship**. The right to be forgotten, as I discussed earlier, is never the right to fly under the radar. Data deletion can never be abused as a means of shutting down difficult conversations, impeding free speech, or covering up illegal activity.

- **Privacy laws which undermine stricter protections**. Good privacy laws should form the baseline for compliance and enforcement. If a jurisdiction covered within those laws wishes to go further, they should be empowered to do so. Of course, they should never be allowed to take a lighter approach.

- **Treating us all like Facebook**. Legislators draft privacy laws to aim for the big fish, but catch the rest of us in their nets. Privacy legislation cannot be drafted on the assumption that we all have a fully budgeted legal compliance team – or, for that matter, that we are all complicit in Facebook-sized abuses of data. Data protection authorities need to provide compliance support and guidance which gets that right.

- **Making privacy a numbers game**. Legislation and enforcement must target the places where the privacy risks are greatest and where the number of users affected is the most substantial. It should never be about creating a scorecard, working to quotas, or setting companies against each other based on numbers alone.

- **Unaccountable regulators**. Data protection authorities, whether old or new, should be accountable to the public, via legislators, through regular reviews and scrutiny. Legislators, in turn, should maintain a healthy professional distance between themselves and data protection authorities. It's a shame that this is rarely the case.

- **Undermining privacy with contract law**. No user should be able to sign away their privacy rights by entering into a contract, creating an account, or accepting a service's terms and conditions.

There is one more bit of advice I would like to offer from the policy frontlines. Many criticisms of existing privacy laws attack them on principle but make no attempt to offer constructive suggestions or alternatives. What does that mean? In my political day job, I regularly encounter policymakers from both sides of the Atlantic who would quite happily throw their citizens' privacy rights under a bus just to spite the EU as punishment for GDPR. What's their alternative idea for privacy? They don't have one.

Spite is no way to conduct public policy.

The fact is, privacy laws that protect user rights are here to stay. Rejecting the concept of privacy, as well as the need for legislation to protect it, is a ship which has sailed.

Beware of Ethics Washing

While it's important to be positive about privacy, we cannot deny that there are some people who exploit that positivity – and privacy itself – in very selfish ways. There is a term for this: *ethics washing*. If you haven't heard that term before, you've definitely seen ethics washing in action, whether you realized it or not.

Ethics washing is what happens when ethics projects, such as codes of practice or public pledges, are devised and adopted *in lieu of* a healthy approach to compliance with privacy laws and the rights they grant users. If privacy law is about safeguarding and empowering the people that data is about, ethics washing is about safeguarding and empowering the people holding and, more often than not, misusing the data.

As privacy becomes a mainstream issue, ethics washing occurs when companies and projects attempt to pass off their newfound love for privacy as a noble gesture they are doing out of the goodness of their hearts. Which means that, more often than not, ethics washing is a means of tiptoeing around the fact that a company was breaking privacy law in the first place. It's also a way for the people who have been directly responsible for many of the privacy problems we face today to present themselves as the solution and take credit for the fixes.

Let's look at an example. Here was the description of a recent podcast episode on privacy:

> ***Embracing innovation by creating privacy-friendly apps:*** *Following the revelations from Cambridge Analytica, the laws on consumer privacy are becoming more strict and the penalties more significant. Ensuring your app or game is privacy friendly has always been good for your users but now it is just as important for your business.*[3]

That is classic ethics washing in action, and it even manages to get a few facts wrong while encouraging developers to think of themselves first.

Here's another example. Do you remember companies making a lot of noise about removing tracking pixels from their e-newsletters because privacy is cool? None of them mentioned that the real reason they removed the pixels was because that form of tracking had just been ruled illegal in Europe.

That's ethics washing too.

Ethics washing, as a trendy thing, often sees companies devising ethical frameworks or internal guidelines about

3. https://smashed.by/androidprivacy

the ways they will handle user data, and which are inevitably announced to great public fanfare. US companies have been particularly guilty of this as they publicize policy principles to stand in lieu of a federal privacy law. However, when you read most of these frameworks in detail, it becomes clear that they have not been designed to complement or inform privacy laws and the rights they grant users. Just the opposite: they have been designed to *circumvent* privacy laws and the obligations they would place on companies.

After all, who would question a company that's "doing ethics"?

It may sound innocent and even a little bit cheeky, but ethics washing causes far more damage than it pretends to fix. There are two reasons for that. First, when companies use privacy compliance as an opportunity for self-promotion, in ways which never mention the laws that ultimately regulate their work, what they are actually saying is that they believe they are *above* the law. Instead of seeking to work cooperatively with regulators and policymakers, they are really subverting the whole process. At a time when data protection regulators and governments are looking to crack down on the profession as a whole, and will seize on any evidence they can as proof that tech companies are rogue actors who are out of control, that is exactly the wrong message to be sending, and it will backfire on all of us badly.

Second, ethics washing shifts the focus of privacy practice from the user to the company, and thus shifts the responsibility for protecting privacy from the company to their users. It goes beyond the userism we'll discuss on the next page (e.g. what do you mean you didn't find the privacy setting we hadn't put in?) to outright trolling (e.g. we have a code of privacy ethics, so perhaps it's *you* who doesn't understand privacy). Put more bluntly, it shifts the blame for abuses of privacy, and the rights that users were denied, from the perpetrator to the victim. Users are left with all of the burdens and consequences of a code of privacy ethics dreamed up for a press release, and none of the safeguards or recourse of an accountable privacy law.

None of that sounds very ethical to me.

At the end of the day, privacy isn't about *you*. Please don't run it through the wash. And when you see companies and public figures engaging in ethics washing, be the brave voice who calls them out.

Avoid the Ugly Side of Privacy

As someone passionate about privacy as a fundamental human right, I would be remiss to pretend that the privacy sphere does not have its ugly side. There are three varieties of that ugliness which I would like you to be aware of so

you can call out those behaviors in others and, hopefully, avoid engaging in them yourself.

USERISM

The term *userism* was coined by tech policy writer Maria Farrell, who defined it as "victim-blaming by privacy-hostile system designers" (and, I must add, the people around them). Userism is the human side of the deliberate use of deceptive patterns, and the rejection of privacy's best practice principles, delivered in a sandwich of bullying and sarcasm.

You have probably met a userist or two, even if you did not realize it at the time. They are easy to identify. For example, userist designers actively blame users for not being able to negotiate a rat's nest of deliberately configured deceptive patterns. Userist developers respond to questions about their project's privacy standards by ranting about European Union bureaucrats. Userist project managers blame their customers for not reading a terms and conditions document longer than a Shakespeare play. And userist lawyers blame their customers for using their own service at all.

Userists are gaslighters with laptops.

I've had the misfortune to encounter all of these userists, and here's what it has taught me. If userism serves a pur-

pose, which I believe it does, it's to help us identify designers, developers, project managers, and lawyers who probably should not be working in their professions. The energy they put into deception, whataboutery, and spite creates bad design, bad code, and bad projects.

You, on the other hand, are better than that.

ABLEISM

Privacy shaming gets uglier than that, and that ugliness is ableism. Ableism, as you know, is discrimination practiced by the able-bodied against people with disabilities. As it relates to privacy, ableism takes the form of a dogmatic approach to the use of technology by people with disabilities which disregards their additional support needs while casting doubt on their personal judgement.

For example, privacy ableists criticize a person with a disability for owning an Alexa device, taking no regard for the benefit it has brought into the disabled person's life. Privacy ableists will force people with disabilities to use privacy-invasive systems in order to prove that they're really disabled, then cite their ability to use those systems as proof that they're not really disabled after all. Privacy ableists attack people with disabilities who run online support forums for using social media or analytics to help them run those forums better. Privacy ableism therefore creates the exact

sort of binary negativity – you can have privacy *or* accessibility – which healthy privacy practices, like the ones we've discussed in this book, can help to avoid.

Dr Frances Ryan passionately articulated the consequences of ableism in privacy in her article "The missing link: why disabled people can't afford to #DeleteFacebook," calling the post-Cambridge Analytica movement a kind of "social media puritanism" exercised by people with the privilege to exercise that form of privacy ableism.[4] Her article gives plenty of food for thought on why we choose to blame the victim instead of demanding changes from the perpetrators or, indeed, from ourselves in our development practices.

Laura Kalbag's talk at Accessibility Scotland 2019 is also an excellent introduction to the privacy issues to consider for people with disabilities, which include disability-specific tracking.[5]

PRIVACY SHAMING

Without a doubt, the ugliest side of privacy is privacy shaming. This is a race to the bottom practiced by some privacy professionals – though that word should probably be in quotes – which seeks to name, shame, and berate rather than engage, support, and educate.

4. https://smashed.by/deletefacebook
5. https://smashed.by/unethicaltech

And goodness me, these folks are exhausting.

Privacy shamers put your use of Google Fonts in the same moral category as the CIA tapping the undersea cables. Privacy shamers cite the social sharing buttons at the bottom of your blog posts as proof of your collusion with Mark Zuckerberg. Privacy shamers attack your use of third-party scripts as evidence of your unsuitability to ever weigh in on privacy. Privacy shamers harass anyone who is doing their best to change tech companies from the inside as being collaborators on par with the Vichy regime. And so on.

Privacy shamers demand a sort of extremism that is never professional and always personal. Like userists, and ex-husbands, they behave that way because they are highly insecure people. (Dig a little further and you'll find some of them actually do have something to offer: they use privacy shaming as a sales tactic.)

But you can't let your work be defined, or derailed, or hijacked by their personal psychodramas. So don't let their insults and accusations dent your confidence. Take heart: real privacy professionals can't stand them either, and they will provide you with a wealth of support and encouragement without shock tactics, abuse, or shaming. You need only ask.

Privacy Journalists Are On Your Side

One group on the sharp end of privacy shaming is tech journalists and writers, including many passionate privacy advocates, who regularly find themselves personally attacked for the things that surround their words on a screen. Even if they have written one of the best articles on privacy that you'll ever read, those words will be discounted and attacked by privacy shamers who rush to label the authors hypocrites because of the adtech or tracking on the site.

Please remember that privacy journalists – at least those who want to pay the rent and occasionally eat food – have no control over the web development choices made by the sites they write on. Nor are they willing to risk their employment contracts, in response to a privacy shaming pile-on, by demanding those changes from the top down. They are doing their best to contribute to the dialogue, and they are on your side, so please respect them for what they can offer.

As the journalist Shoshana Wodinsky tweeted, "Berating digital privacy reporters for the adtech on their parent site is the editorial equivalent of yelling at a child for something their dad did. It doesn't make you look clever. It makes you look like an asshole."[6]

Don't be a userist, don't be an ableist, don't be a privacy shamer, and please don't be an asshole.

6. https://smashed.by/swodinsky

Raise Your Expectations

Finally, I began this book speaking from the heart, and that's how I'm going to end it.

I wrote this book because I believe that the people we make the web for deserve better from us. But there's something I feel just as strongly about: *you deserve better too.*

And when it comes to privacy, most of you have been very badly failed by the institutions and organizations around you.

That failure began with your education, and with mine too. When I began my career on the web, the principles I have written about in this book should have been as much a part of my foundational knowledge as HTML and CSS. They were not. My main goal for this book, in a way, was to write the guidance I wish someone had written for me.

Here's a scary fact: the first formal training and education I was given on privacy for the web didn't happen until *eighteen years after* I built my first website. Even then, it was in the form of a postgraduate course in internet law, inclusive of 5,000-word homework assignments requiring legal research and citations – which is quite the learning curve when you are not a lawyer. Everything I knew about privacy theory and regulation before that was a matter of satisfying my own curiosity on my own time. The basic

conceptual knowledge, training, and support I needed, at a price I could afford, in language written for me, did not exist, and it still doesn't.

That's absolutely ridiculous.

No web professional, whether you're a veteran of the dial-up era or you're just starting out in your career, should have to enroll in a postgraduate law course to learn fundamental principles other professionals learn from the start. And that education, with all due respect, should not come from a barrister teaching for courtrooms rather than coding. Likewise, the user protections we build into our work should not depend on whether the person planning the project had an early midlife crisis and decided to go to grad school.

As makers of the web, you need to demand more from the institutions that prepare you for your career. We need to demand that privacy, as well as other rights-based fundamentals such as accessibility, are a part of our education and training from day one. That should be true whether you learn your trade in a secondary school course, a code academy bootcamp, a four-year computer science degree, or if, like me, you found yourself making the web with no formal education or training at all. And the education we demand should be positive and foundational, not scaremongering and threatening.

As far as I'm concerned, if educational institutions are sending newly minted web professionals into the world without a theoretical, legal, and practical grounding in user privacy, then those institutions have failed their students badly. Expect better from your institutions, and in fact, demand it. After all, it's your career in the making, not theirs.

As makers of the web, you also need to take personal responsibility for filling the gaps in your education. We can't wait for educators, trainers, and institutions to catch up. Being an actively practicing web professional with little to no knowledge about the standards and legal foundations which shape your work is like being an architect who knows nothing about building codes. What you build may look cool and have some neat features, but the foundations are shaky because the building material is banned in most states. It's not you the building will fall down on.

Let's stay with that building metaphor for a minute. Imagine if an architect went onto a podcast and spoke – somewhat resentfully – about "all these building codes that are changing the ways I design." Imagine if an engineer only learned about the safety regulations they were legally obliged to follow from conference talks and blogs. And imagine if both of them publicly backtracked over those gaps in their knowledge by trying to spin safe building design as the latest consumer trend. Not only would they

lose their jobs on the spot, but there would need to be an emergency inspection carried out on every building they had ever played a part in creating.

Not so for us.

Web development is probably the only field on the planet where not knowing its fundamentals is considered cute and funny, where it is somehow safe to boast in public about how little you know about your job, and where attacking the principles of safe design is considered a bit of banter. **So let's put an end to celebrating our ignorance**. If we don't, we're giving hostile policymakers – and you have no idea how hostile they can be – all the leverage they're looking for to step in and pass laws creating mandatory gatekeeping between you and your job.

Web practitioners need continuing professional development, but that isn't always easy in a field where few employers offer any support for continuing education. For that reason, **development communities, open source projects, and design collectives have a role to play in teaching privacy**, particularly as they may be the closest thing to a professional body that most of us will ever have. Explainer talks, workshops, and refresher training on legal and conceptual issues need to become part of every community's conference cycle. (I don't know about you, but that's

what I *want* when I go to a conference. Sod yoga.) I'd like to challenge every development community organizer reading this to guarantee a permanent privacy slot at every major conference, and to show me your schedules to prove it.

Where user privacy is concerned, you need to knock down a lot of ivory towers. Essential knowledge about privacy, as a concept and as law, should not be hoarded as the privileged knowledge of academics and data protection lawyers. It has been for too long. Treating data protection and privacy as complex matters by lawyers, for lawyers, at a lawyer's hourly billing fee, was one of the reasons we ended up needing the GDPR overhaul in the first place; if the existing privacy rules were missing from most developers' toolkits, it's because it benefited a lot of people's careers for it to be that way. And treating the future of data protection and privacy as complex matters by lawyers, for lawyers, most of whom talk about web development as an abstract concept, is how the mistakes of the past will be repeated in the future.

Even this far into my career, I still find myself looked down upon by privacy lawyers and academics who are appalled by my lack of a legal degree and a PhD (yes, both), as if I am some kid who has crashed their party. Most of them will not consider this book a legitimate publication because it has not been published by an academic press. The snobbery re-

ally is that bad. And that ivory tower they have built around privacy cannot come down soon enough.

Additionally, over several years of unsuccessfully trying to garner support for open-source privacy initiatives, I discovered – to my great sadness – that many privacy academics and lawyers who *could* lend support to web professionals choose instead to look down at us if we're the dog dirt on their shoes. As far as they are concerned, we developer scum are the cause of all the problems on the web, and we should be the target of the blame. But as the saying goes, "the only time you should be looking down on someone is if you're offering them a hand up." **Privacy and data protection experts who can help web professionals make the web a better place should stop looking at you as the source of the problem, and start looking at you as the source of the solution**. And for what it's worth, we have more in common than you think.

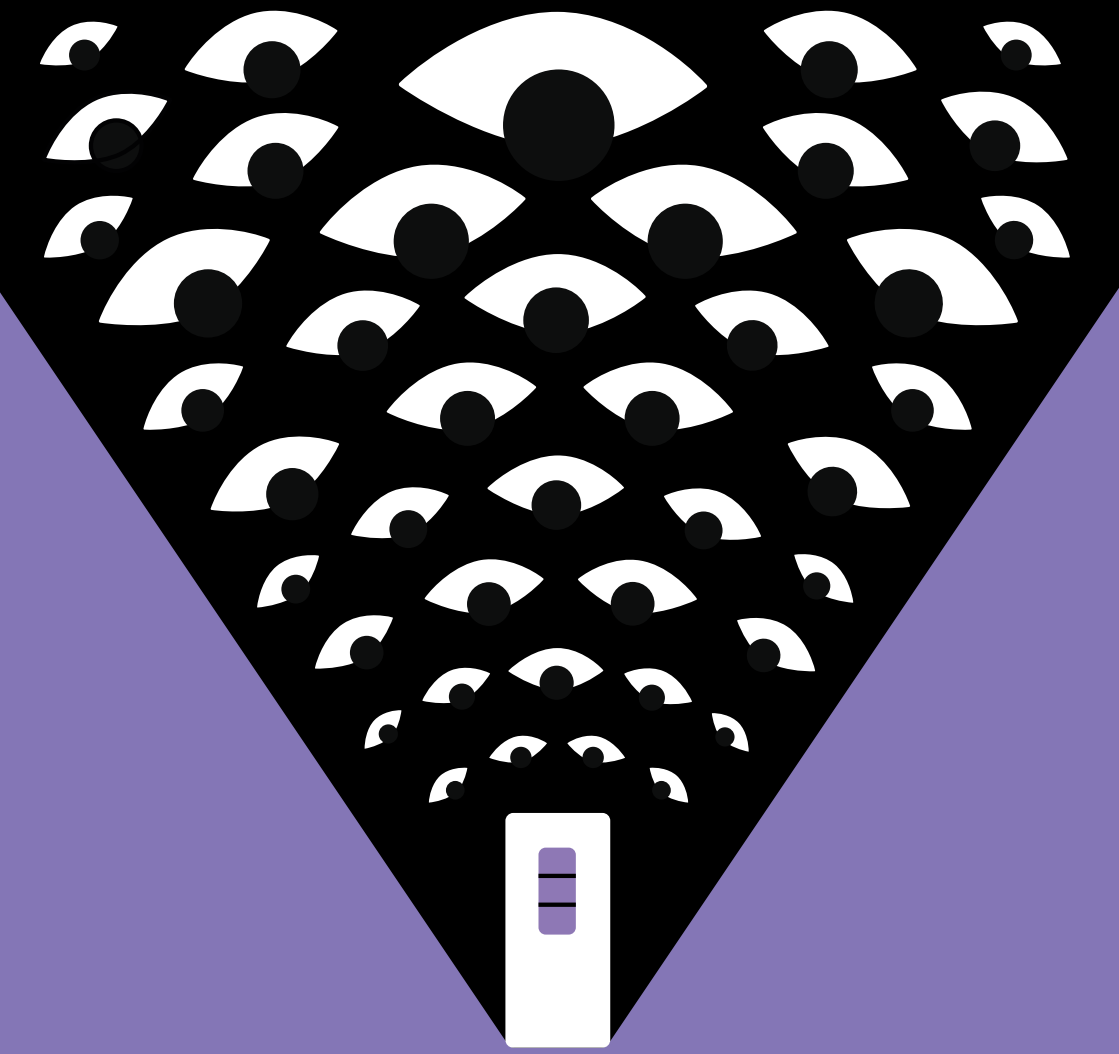
Finally, I'll bring our journey to a close with a nod to my day job. **As makers of the web, you need to find your voice in the political sphere, speaking up and shaping the rules of the web in the interests of your users**. The fact is, we aren't showing up in places like Westminster, Brussels, and Washington as new internet regulations are drafted. And it's clear that many communities have no intention of ever showing up, because tech apparently doesn't

do politics, even when the politics are about the tech. But your failure to show up will not protect you. The companies who have created the privacy dystopia we live in today *are* showing up, and they come prepared for the battle. And politicians want to regulate your work as if you were those companies, because they don't understand that there's a whole other internet beyond them.

Laws on technology, including the future of privacy for ourselves and for our users, can only be shaped by the people who use their voices to speak up, not by those who choose to remain silent. That's why a policymaker at the European Commission told me, almost pleadingly: "*It's very important that people like you keep us real. Multinationals are lawyered up, and we lose perspective.*"

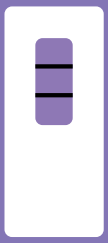
Lawmakers crave the perspectives of the people like you who build the web every day for the greater good. They are waiting to hear your voice.

Let them hear you loud and clear.



POSTSCRIPT

Privacy and Health Data



POSTSCRIPT

Privacy and Health Data

When I began outlining this book, my life involved a lot of planes and airports. As I sign off on the final edits, I haven't been on a plane in over two and a half years. The Covid-19 pandemic changed life – and privacy – for all of us. But I know I'm one of the lucky ones: I stayed healthy, my loved ones did too, I had the support of an employer, my cupboard was and is full, and I had the amazing NHS at my back. As hard as it was, I have no right to complain about anything.

That obliges me to look after others who aren't so lucky, and so follows this postscript on what the pandemic has meant for user privacy and the work you do to protect it. As it turns out, the lessons learned over those years have much to teach us about the next challenge you may face involving the uses – and misuses – of health data.

In addition to the changes we all had to make in our professional work, as well as the difficulties it presented in our everyday family lives, the coronavirus outbreak brought the privacy issues I discussed in this book into focus like never before. *Privacy is real for everyone now.*

Some of those issues have been hard lessons for all of us.

Let's take the video-conferencing platform Zoom, for example. Originally conceived as a business-to-business tool, its on-the-spot adoption for everything from family contacts to school lessons skyrocketed in the first weeks of the pandemic, to the point where "to Zoom," like "to Google," became a verb. As it did, a raft of privacy and security issues hit the headlines.

Consider each of these issues in the context of what you've learned in this book:

- Zoom's densely legalese privacy notice was found to have stated that personal data about meeting attendees was being collected, which they reserved the right to sell.

- Its iOS app used Facebook's SDK to send data about users to Facebook, even if – as is the case with all deployments of the Facebook SDK – the user did not have a Facebook account.

- Attendees could be tracked by meeting hosts without their knowledge.

- Its DIY encryption was poor.

- The macOS installation process did not disclose all the modules it initialized.

- A zero-day exploit allowed remote executions on Windows machines.

- Meeting hosts, again without attendees' knowledge or consent, were able to use a data-mining feature to display their LinkedIn profiles.

- A data leak disclosed thousands of users' email addresses.

- The use of numerical meeting ID numbers, in an easily discernible pattern, led to "Zoombombing," meaning the coordinated hijacking of meetings with grossly offensive content.

- The company claimed the platform used end-to-end encryption, which it did not.

- Calls were routed through third countries with questionable approaches to privacy, such as China, without user knowledge or consent.

- Features such as unverified users' abilities to share their screen and change their names mid-meeting were turned on by default, leading to the Zoombombing of meetings – including one which I had the misfortune to be in – with stomach-churning videos of child sexual abuse.

Any one of these errors would be the end of a start-up, and all of them together, in normal times, would be the subject of a parliamentary enquiry if not a criminal investigation; were it not for the essential role the service played during the pandemic, privacy regulators and public prosecutors would have eaten it alive. In response to the (fully warranted) bad publicity, the company's CEO, Eric Yuan, told the Wall Street Journal in April 2020 that "[W]e need to slow down and think about privacy and security first [...] that's our new culture."[1] Yet all of those issues, which occurred under his watch, were completely unnecessary and totally preventable, and a true privacy- and security-first approach would have made sure of that.

(Note carefully how the decision-maker ultimately responsible for the mistakes gets to ethics-wash them into a personally inspirational leadership journey, while those of us on the receiving end of the mistakes struggle to unsee the horrific imagery they permitted. 'Twas ever thus.)

It should not have to be that way for anyone else when the next challenge arises. While most of you will not be working on platforms of that scale, or on applications that will become household names overnight, you will all have to consider the privacy implications of the work you either create, rely on, or both.

1. https://smashed.by/zoomsecurity

For once, the law is actually quite clear here: privacy and data protection regulations have always allowed provisions for data sharing in the interest of public health or substantial public interest, such as national emergencies, which the pandemic absolutely was. It is what happens with that data *outside* clinical settings, or in response to a public health issue which is more political than personal, that poses the problem. Protecting our vital health data from scope creep, which could easily see it exploited for mass surveillance, discrimination against the vulnerable, or the creation of a protected class with special privileges, will be the true test of your commitment to privacy.

Your challenge lies in the systems, software, and applications you will create, contribute to, and use for:

- **Location tracing** to alert people that they have been near a hotspot.
- **Information capacity** to make sure the right resources reach the right people.
- **Early warning and surveillance** to see new waves coming.
- **Responsible use** of public and private data.

- **Quarantine and social control** to safeguard the most vulnerable.

- **Data-driven research** towards a cure for long-term conditions.

The first category is perhaps the most personally relevant. For most of you, health monitoring data, paired with location tracking, became not just a part of your daily routines, but essential to your ability to travel and work. Many of you were given no choice about using these apps and uploading your personal data, as well as the data about your closest family and friends. The rights you were given in exchange for that data depended on algorithms created by private companies with questionable track records on privacy, and sometimes even on the adtech included within the apps. And the potential consequences for the abuses of your data and rights, whether you were living in isolation or going to work sick because you had no health insurance, were unfathomable.

If the privacy risks that vulnerable people live with every day have never hit home for you, consider the pandemic a thorough grounding: we are *all* vulnerable now. Your health – and your human rights – can change in a matter of hours, and your control over them is out of your hands.

So how do we, as the builders of the open web, take the lessons we learned during the pandemic and apply them to the next challenge?

What the Pandemic Taught Us

By all scientific consensus, the pandemic will be with us for the foreseeable future. Out of that chaos comes opportunity, so we must try to look at the pandemic as a means of advancing user-centric privacy technology for everyone, no matter what health situation they may be experiencing, in the right way.

There is a balance to achieve in protecting our health, safeguarding the vulnerable, resourcing our health care systems, and keeping our societies running smoothly, which should not mean trading away our privacy, our civil liberties, or our human rights. And if you are called on to participate in the creation of technology involving public or private health data, whether you are a project manager, a developer, or a designer, you have a vital role to play in achieving that balance.

The approach you take to ensuring user privacy, in a health context, will depend largely on the legal environment

which exists around you. If you live in a country with a view of privacy as a legally upheld human right, you will take a broader view of the issues in play than someone working in a country where privacy is a function of contractual terms and conditions.

Likewise, if you live in a country with a stable tradition of the rule of law, you may be inclined to develop based on your personal presumptions about the ways society works, which people living in other countries have never known. Your challenge, as I have said throughout this book, is to do everything you can to safeguard user privacy *regardless* of the presence or absence of privacy legislation, as well as a healthy regard for their human rights, and to do so with an understanding of how high the stakes are if you get it wrong.

If you do not have a rights-based privacy law to use to shape the constraints of your work, or if you work in an environment where health data can be misused, mishandled, or exploited as a means of targeting vulnerable groups for mistreatment, the lessons you take from the pandemic should adhere to these guidelines, which we discussed at the beginning of this book, at the absolute minimum:

- **Data minimization**: The data collected by the applications or systems you build must be limited to the

smallest amount of data possible and not aggregated with any other information. When data about a person experiencing a health situation is shared with a contact, that data must be the minimum amount possible, it must never identify the person, and the data given must never put the person at risk of retaliation or harm.

- **Purpose minimization**: The data collected should only be used for the purpose of managing that person's health, as well as for any bona fide public health reason, and not shared with third parties for any reason, whether that is marketing (even for medical treatments) or – and for heaven's sake, please don't do this – a social media SDK.

- **Life cycle limitation**: The data must be deleted as soon as it is no longer needed, even if the person's health condition is ongoing. Any public health authority with access to that data must also delete it when it is no longer necessary or useful. No personally identifiable data should be retained by any third party for future uses. And when this nightmare is over, every scrap of data held within the apps and in the cloud should be deleted, along with the apps too.

- **Information, technical, and security measures**: The applications and systems should be built with the high-

est consideration for security. Decentralization is key. Deidentification, random identifiers, and end-to-end encryption should also be considered. Careful attention must be given to the need to balance privacy and security; for example, biometric identifiers should not be used to verify a person's identification if that data could be aggregated with other data within the app to identify them to others. Thought should also be given to how these systems can and will be abused, such as false positives, scamming, or DDoS attacks, and how to mitigate those possibilities as much as possible.

- **Transparency and notice**: All applications and systems, and the health services which provide them, must provide full disclosure over what data is collected, how it is used, who has access to it, how long it will be held, and what rights the person has over it. When data is shared with any party for any reason, it must be within the scope and constraints of the rule of law, and this basis must be made clear to the person in non-threatening language they can understand. Additionally, the applications and systems themselves should be open-source, and should be hosted in projects with fully transparent governance, including full disclosure of who funds the projects and who makes decisions about them.

- **Choice, control, and consent**: The data about a person's health should be owned by the person and kept under their control. They should be given a choice on where that data lives, which in this context means decentralization: if they want their data to never leave their device, that wish must be respected. The person's data must not be shared with people they know, or people they don't know, without consent. The data collection and the applications themselves should be used voluntarily and with full consent, which must be active and opted in to with full understanding. And it must be possible, as with all good data protection practice, for the user to revoke their consent for any or all uses of the data collection at any time.

As helpful as our fundamental privacy values may be, those principles alone cannot safeguard the rights and freedoms of the people *in* the data, nor can they provide them with the confidence that public health systems are working in their best interest.

That trust matters – and it works both ways.

After all, if technology is meant to be our way out of our public health issues, then the data people share through it must be provided with honesty and confidence. People

will not share their health data if they fear consequences, punishment, or discrimination for providing the "wrong" answers, or if the systems are patronizingly gamified to see who gets a trophy for sharing the most information.

Likewise, if citizens view health-related apps and services as a cynical data grab for private health insurance companies, marketing firms, brand influencers, and funeral plan vultures, their confidence in both the apps and the public health systems providing them will plummet. If the adtech, social media, and tracking SDKs included within an app put vulnerable people at even greater risk than the health issue itself, then the people behind the app have far more than that health issue on their conscience.

And without a caring regard for people who can't afford the latest smartphones, or are not able to use the ones they do have, making their health dependent on technology they have no ability to access to crosses the line from digital exclusion to dystopian social cleansing.

Protecting the People in the Data

Clearly, we all need to get this right for everyone, including our families, our friends, and ourselves. So if you are able to

commit to further safeguards for user privacy which build on the lessons you learned during the pandemic, whether that is through your own work on an everyday level or on a wider stage through proposing national legislation, a comprehensive model exists to show you the way.

In the early months of the pandemic, a draft Coronavirus (Safeguards) Bill[2] was proposed in the UK to ensure the conditions that must exist to protect the civil liberties and human rights of users – above and beyond the existing privacy safeguards discussed above – in the event that contact tracing, early warning, or quarantine apps were made mandatory. The safety net within its suggested provisions integrated privacy law, data protection best practices, human rights principles, and the hard lessons learned from actual experiences around the world during the early weeks of the pandemic.

Those proposed safeguards, which sadly fell victim to politics,[3] included:

- **No sanctions**: Nobody should be sanctioned for failing to install a health data app, use it, or have their phone on their person at all times. This provision could include a ban on sanctions such as civic penalties, criminal charges, being fired from employment, losing

2. https://smashed.by/coronabill
3. https://smashed.by/covidtracing

the right to vote, or non-eligibility for public assistance. This provision would also safeguard people who do not own a smartphone, cannot afford one compatible with the app, cannot afford mobile data, or do not wish to have Bluetooth turned on at all times.

- **DPIAs**: Any health data apps must have a full privacy impact assessment (see page 100), which must be made public for consultation and feedback.

- **No gamification and the right to privacy**: There must be no requirement for people to install a health data app, read the messages on it, contribute data to it, or keep it on their phones (that is, not delete it). Gamification has no place in public health. If installations are to be made mandatory, there must be a strict privacy and human rights basis within the rule of law established within the regulations which mandate it. Additionally, children aged over 13 should have the right to veto parental insistence on their using the app. Privacy, after all, is the right to be left alone, and most teenagers are experts at this already.

- **Not a business opportunity**: Any of the personal data collected and used by a health data app, whether it is about the person or the people they have come into contact with, must not be used, shared, or processed

by any party for any purpose other than the health system's management of the patient. There must be no adtech, advertising, or commercial tracking.

- **No travel passports**: Immunity certificates – app-based or otherwise – must not be made a mandatory condition for leaving the home, using public spaces, or taking public or private transport, and businesses must not be permitted to demand them. (As dark as the thought is, the draft Bill's authors were also mindful here of the physical risks to a person known to be walking around freely with a coveted immunity certificate on an expensive smartphone.)

- **Protected status**: Because of the risks of discrimination and abuse, "health condition status" must be made a protected condition – in privacy terms, a special category of data – akin to sexual orientation or religion. A person's health status cannot create a caste system.

- **Oversight**: Finally, there should be a new independent regulatory body, similar to an equal rights commission, to conduct oversight, provide guidance, and receive complaints about violations of privacy and human rights related to the use and misuse of health data. Systems are only as good as the people who build them, the leaders who direct them, and

> the watchdogs who keep them in check. No one's health, or their human rights, should depend on a black box accountable to no one.

While the failed draft Bill was clearly focused on one medical situation at one particular moment in history, all of those lessons are easily transferable to other health issues, and it's worth thinking creatively about what some of them might be.

The UK's draft Coronavirus (Safeguards) Bill would have been a way to make sure we all did better through common-sense provisions protected by the rule of law. Its model should be followed in more ways than one. For just as the pandemic accelerated years' worth of technological progress into a few short months – for better and for worse – it *must* also accelerate years of stalled progress on privacy legislation, particularly in the United States. There was no worse time for American developers – who, unlike their European counterparts, lack both an omnibus privacy law as well as centralized national public health systems – to be left to make up the rules as they go. Nor was a public health emergency a good time for the private companies who developed coronavirus apps to become America's de facto privacy regulators.

So as stressful as these times were for all of us, you've got to take something positive out of it. Use the lessons you learned during the pandemic to build better systems, create better protections, and fight for a better web, for both good times and bad. If you are in a position to contribute to the debates about federal privacy legislation, the uses and misuses of health data, and the role adtech plays in all of that, make your voice heard. And if there are steps you can take to make your service safer for those who use it, don't wait to be asked. Do it, and do it today.

And if a service or application you are requested to use does not meet the safeguards I've discussed above, regardless of the presence or absence of a legal framework, be brave enough to call them out. You owe it to yourself, and you owe it to the people in the data who need your voice to protect them.

The pandemic was the darkest time that many of us will ever know, and it has changed all of us forever. The technology we build around our health data, in response to those awful lessons learned, must shine a light on our way out of the darkness and not pull us further into it. None of us have a map showing how to get there. But for whatever health challenges lie ahead, I hope this book provides a torch.

Index


The world is a miracle. So are you.
Thanks for being smashing.
SMASHING
MAGAZINE

"Privacy can seem complicated but it doesn't need to be. Heather covers all you need to know with astonishing clarity. This book gives you all you need to understand and handle privacy work, and makes for great teaching material that experts can rely on."

—***Robin Berjon,*** *berjon.com*

"No more excuses for overlooking privacy: Heather's guide is an essential toolbox for user-centric product developers and for anyone interested in building a better web. Expect the full sweep, from historical context and core concepts in US and EU privacy practice, to practical tips and advice – dispensed in highly readable style."

—***Natasha Lomas,*** *TechCrunch*

"Heather's broad knowledge, experience, and ability to articulate these complex matters is nothing short of astounding. I've learned an amazing amount from her. She always informs and entertains, and she does so from the heart."

—***Mike Little,*** *Co-Founder of WordPress*

Heather Burns is a tech policy professional and advocate for an open Internet which upholds the human rights to privacy, accessibility, and freedom of expression. She has educated thousands of professionals on a healthy approach to protecting people and their data.

SMASHING MAGAZINE

9 783945 749647