Understanding Privacy

Heather Burns

how to put your users first and build a better web

Understanding Privacy

by

Heather Burns

Published 2022 by Smashing Media AG, Freiburg, Germany.
All rights reserved.
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.

FSC
www.fsc.org
MIX
Paper from
responsible sources
FSC® C083411

Please send errors to: errata@smashingmagazine.com

To the centre of the city
where all roads meet

Contents

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

[12] https://smashed.by/databrokers

really doing is contributing to a larger data file, somewhere, which tracks an individual's

- 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 patronizing 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.

[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

The first and trickiest question you'll need to deal with is: who is a child? GDPR does not define that (different EU 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,

[15] GDPR, Chapter II, Article 8

unfortunately, has caused a sort of legislative scope creep which sees parental monitoring and age gating – *of 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]

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

[16] GDPR, Recital 65

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, 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

[17] https://smashed.by/childrenprivacy
[18] https://smashed.by/coppa

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?
- Will the microphone in the device have a physical switch?
- Will the device receive advertising messages from third parties?

[19] https://smashed.by/pesia

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?
- Who has the power in the relationship between the person deploying the product and the person being made to use it?

[20] https://smashed.by/dataethics

- 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:

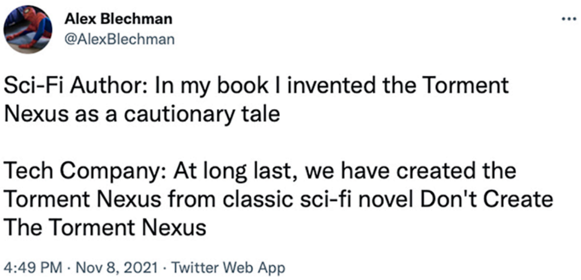
- How am I going to feel about myself if I continue to work for this company and develop this product?

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.



Alex Blechman
@AlexBlechman

Sci-Fi Author: In my book I invented the Torment Nexus as a cautionary tale

Tech Company: At long last, we have created the Torment Nexus from classic sci-fi novel Don't Create The Torment Nexus

4:49 PM · Nov 8, 2021 · Twitter Web App

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.

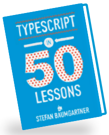
SMASHING MAGAZINE

Smashing Library

Expert authors & timely topics for truly **Smashing Readers**.

Our Latest Books

Crafted with care for you, and for the Web!



TypeScript in 50 Lessons

by Stefan Baumgartner

Inclusive Components

by Heydon Pickering

The Ethical Design Handbook

by Trine Falbe,
Martin Michael Frederiksen
and Kim Andersen

Image Optimization

by Addy Osmani

Art Direction for the Web

by Andy Clarke

Click!
How to Encourage Clicks Without Shady Tricks

by Paul Boag

See all of our titles at smashed.by/library

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