Illustration by Elliot Stokes

Privacy is UX

by **Alex Schmidt** · September 22, 2015

Published in User Experience

Government snooping. Identity theft. Sale of personal data. Privacy is out there in a big way. But it's not *in here*, meaning on most product development teams.

Article Continues Below

I'm a member of those teams, as an experience designer with a foot in strategy and user research. I'm also a longtime public radio reporter (tech was a big topic of mine), so curiosity is my strong suit. I noticed that, at the agencies and tech companies I've worked for, privacy never seemed to be discussed much. And, as reporters do, I wondered why.

Making the case for bringing privacy into the product development process isn't easy, especially since finding examples of successful companies that value privacy isn't easy. In fact, the opposite is true—the web is littered with products or design methods that tried to promote privacy and failed, or that gained only small, niche adoption (here, here, here, here, here, and here). Knock-on effects are that privacy sometimes sits on the back burner.

There are good reasons for this: so many factors are at play in developing web products, and privacy gives us just one more thing to think about. But designers and product owners can and should work privacy into the process, and I'll explain some ways we can do that.

The basics of privacy

Privacy is one thing, but security is another—and the latter is something that many companies do care about. If users' information gets stolen, or governments snoop on it, that's bad for trust and reputation and hence bad for business. When companies like Apple and Facebook call for security measures or legislation, or encrypt their data, it's because they care about secure user data.

But, even companies that do encrypt (voluntarily—there are no laws around this right now) receive data in an unencrypted fashion, so there's nothing to stop them from making the most of it for their own purposes, or selling that information to other companies (some secure, some not).

Privacy questions come in when we talk about a company collating/snooping on users' behavior and messages, or passing data on to others. Right now, there is no blanket privacy law in the United States, but rather a patchwork covering specific areas of information and users: for example, health and financial data are subject to more intense legal scrutiny under HIPAA and the Financial Services Modernization Act, respectively. Everything else falls under the purview of the FTC, which polices bad business practice and mandates privacy disclosures (not actual privacy, mind you—just disclosures). Those are the sorts of things that would be detailed in a privacy policy. Any future American case

furthering privacy protections could be made upon the Fourth Amendment of the Constitution.

There are many flavors of online privacy violations. Last year's Uber episode, in which the company singled out a journalist and tracked her movements without consent, was a violation of policies and may allow for legal recourse. (Other companies likely engage in these sorts of activities, but we rarely hear about it. Of course, the Facebooks and Googles of the world have access to all the messages their users write.)

Then there's the murky area of things that aren't technically illegal, but are questionable, like companies collecting information on behavior that users are not aware of. Cookies are one example of that. Of bigger concern is something like Target predicting a woman was pregnant before she knew it herself. And, finally, there's the selling of that data—to advertisers, for example, or during an acquisition.

This data is typically made up of a combination of user-entered values and behavior tracked in the background (a.k.a. analytics): geographic location, clicks, time on a certain page, etc. Many companies claim they don't care about individually identifying features, but instead, about user behavior or information in aggregate. However, anonymized or partially anonymized data can often be traced to individuals—take, for example, AOL's search data leak of 2006. One user who had searched for information on murdering his wife was identified—but he turned out to be a TV writer who worked for a crime show.

Making a case for privacy

COMMUNITY-BUILDING REQUIRES TRUST

If a business wants to build some sort of community or audience, it needs to establish trust. You can make the case that privacy will help, and include product requirements and user stories around privacy.

LEGISLATION WILL COME

Following privacy legislation isn't easy, but things are moving. American states pursue their own laws piecemeal, and federal legislation is outdated, though Congress talks about it more and more. Meanwhile, Europe is ahead of the rest of the world when it comes to online privacy laws. If your company has designs on going global, all users will likely be stored in the same online bucket—meaning European privacy protections will need to be extended to all of them. Wherever you do business, being proactive now will save headaches later.

BAD PRESS IS PAINFUL

Uber could've avoided some pain—and legal hot water—if it had adhered to stated policies. When violations and sketchy behaviors are brought to light, users hear about it. Witness the intense reaction to Facebook's "social experiment." Or the response to Edward Snowden.

IT COULD BECOME A SELLING POINT

Some global players are starting to think along the lines of "privacy as selling point," including IBM, Microsoft, Google, and Apple. Mark Cuban even ranted about it!

PRIVACY AFFECTS LIVES

> *The notion that "if you have nothing to hide, you have nothing to fear" is a destructive axiom of Orwellian proportions.*
>
> ——*Alex Winter*

The most common retort you hear when raising issues around privacy is "What are you so scared of?" During a 2014 talk at Carnegie Hall, Glenn Greenwald explained how he responds to this question: he proposes the asker write their email username and password on a piece of paper and give it to him. No one ever takes him up on it. People, he posits, simply want private spaces where they can do things away from others.

There are also very real things to be afraid of—things that we, as user experience designers who care about empathy, should also care deeply about. One example: Weight Watchers sharing personal information in user accounts (weight, health habits, and exercise patterns, for example) with advertisers, which 60 Minutes reported on. In the same report, an expert discussed the emergence of "digital redlining." Historically, redlining is the practice of denying mortgages to applicants of color in predominantly white areas of town. Digital redlining is similar: you could be denied a mortgage if the socioeconomic status of your online social circle deems you undesirable—and Facebook just patented technology for that very thing. Warrantless snooping by the government can have serious consequences too, leading to unjust detention and arrest.

Down the road, it'll really suck when health insurance companies start to get access to data from Fitbit to raise premiums (they're already rewarding users who provide access to their data). And don't forget about users in countries whose lives may be at risk when their data isn't private. If we believe that treating users with respect and honesty is essential to a good experience, then we owe it to them to ponder these issues.

We also need to be aware of the processes we're complicit in—as Mike Monteiro has said, designers have responsibility. Trading in user data is a big part of making a living online today. If you choose to participate, you should know that you're part of further ossifying the web in this modus operandi. You may be okay with that, but know it.

So, to sum up: Arrests based on erroneous or overblown government intelligence. Insurance companies snooping around in messages and health records. Dissenters being punished by dictatorial regimes. The arrival of robot overlords in the form of targeted advertising. Lack of privacy creates real danger. But even if users don't want Google cataloging and analyzing a lifetime of their search history *just because*—well, that's valid, too. It's Article 12 of the Universal Declaration of Human Rights.

Adding privacy to your process

There's no tried-and-true path to building privacy into your process, but there are ways to get started. Here are a few.

USE A QUESTION PROTOCOL

If your site or app uses a form, or asks the user to enter any amount of data, Caroline Jarrett's question protocol is an invaluable tool for digging deeper into what you're doing and why. As she describes it:

> *A question protocol is a tool for finding out which form fields are required and lists:*
>
> - *every question you ask*
> - *who within your organization uses the answers to each question [or, if no one plans to use it now, who can you imagine using it down the line?]*
> - *what they use them for*
> - *whether an answer is required or optional*
> - *if an answer is required, what happens if a user enters any old thing just to get through the form*
>
> *The question protocol is different from the form itself, because it's about how you use the answers.*

Jarrett sees the protocol as bringing web development closer to the rigor of the scientific research process. "For example, during the census," Jarrett explains, "they will be doing extensive research around what questions to ask, how that data will be used, and the delicate balance between the cost of collecting every piece of data and the benefits. Because collecting census data is incredibly expensive, but it's very important."

In the case of product development, every piece of data we collect through a form has a cost, too.

User costs	Business costs

Attention	What about your product might the user ignore if a form is onerous?	**Data storage**	Where will you keep all of this stuff?
Time	How much time does a user really have to contribute to your form fields?	**Data maintenance**	What is the cost of updating, modifying, and potentially disposing of data?
Trust	What happens if users don't understand why certain data is required?	**Data quality**	What will it take to sift through made-up data to get to the real stuff?
Physical cost	What does it take from the user to fill out the form?	**Breach of user trust**	How would users react if data were misused or sold?

You could apply this method of deeper thinking to any piece of data you're collecting on a site, not just what gets typed into a form. Say you want to collect GPS data on users: ask why it's needed, where it'll be stored, how it'll be used, and tally up the costs around breach of trust if it comes to that.

WRITE USER STORIES AROUND PRIVACY

We spend a lot of time designing features—features that users experience. But things that happen in the background of an experience can still constitute bad UX.

One way to bring privacy into the conversation early on is to write user stories around a privacy epic. Here are some examples based on an online store:

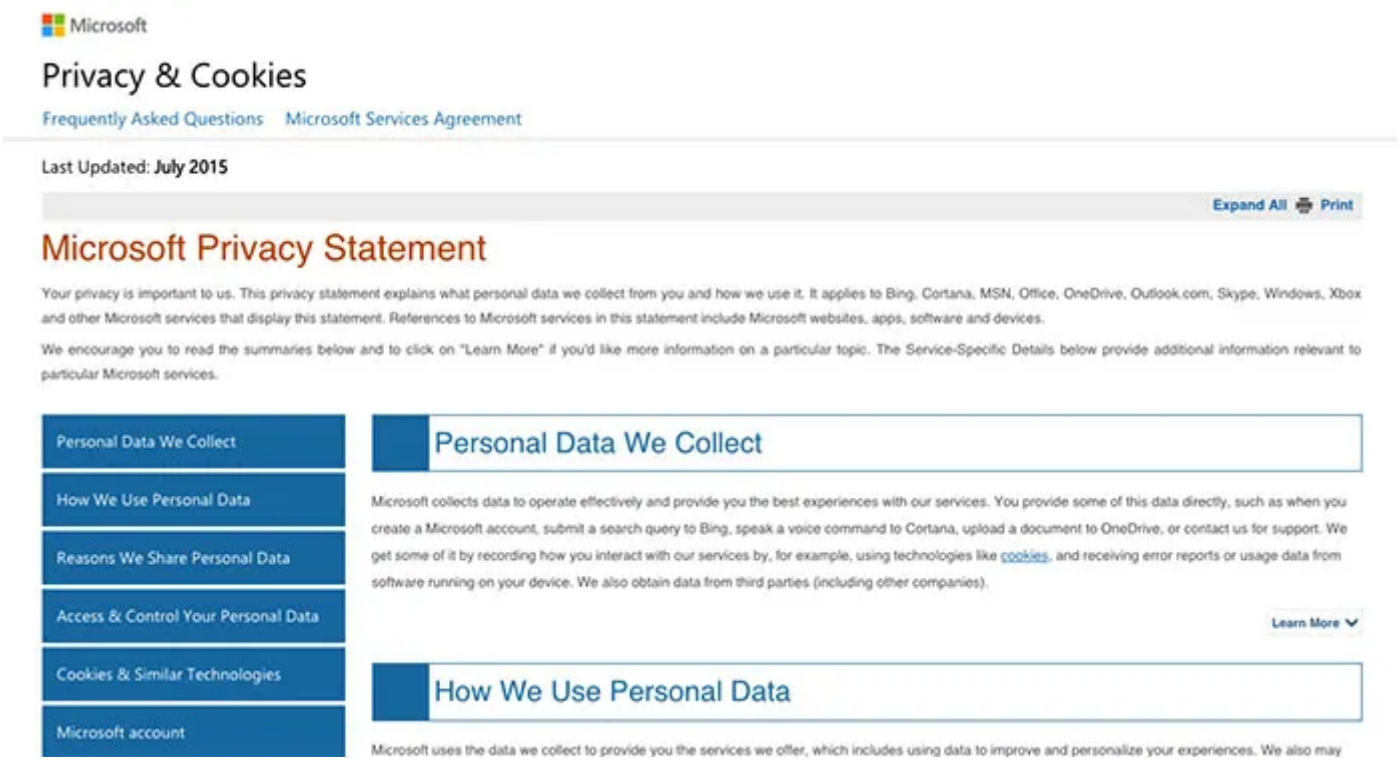
- As an online shopper, I want to know why the store requires my phone number because I feel uncomfortable giving it out, and it seems irrelevant to making a purchase.
- As an online shopper, I want to have a choice over whether and how the store uses my search history so that I have control over my data.
- As an online shopper, I want to have the option for my purchase history to inform recommendations the store makes so that I can shop more efficiently.
- As an online shopper, I want to know how the store uses my data so that I can make an informed decision about whether I want to shop there.

- As an online shopper, I want my purchase history to remain under the purview of the relevant business so that I do not receive unsolicited marketing.
- As an online shopper, I want my purchase history to default to private until I tell the store they may use it.

These stories may affect, or be influenced by, the privacy policy, so be sure to meet with compliance stakeholders about them. If these were your user stories, you might also find that some of them turn out to be non-functional, like the one about keeping purchase history away from third parties. The user may never see anything related to that story, but it could dictate the way databases are built, and how information is stored, tagged, and disposed of. Keep up an open dialogue with developers so they are aware of how certain stories need to be worked into their technical solutions.

TURN PRIVACY INTO A FEATURE

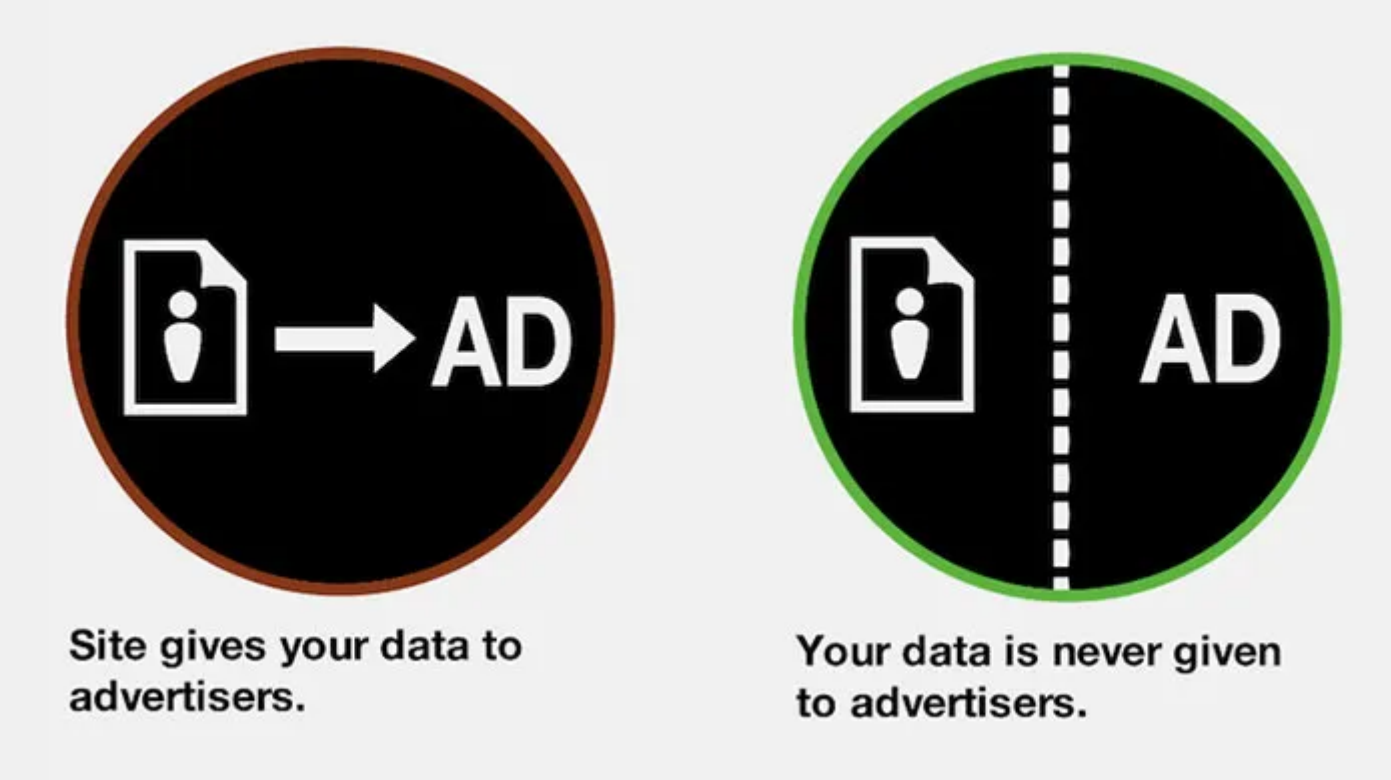
Prioritizing privacy can also lead to clearer product designs, as in Microsoft's recent expansion of its privacy policy:



Approachable language with content presented in an organized fashion.

There's nothing fancy or groundbreaking about this design (and in fact the content itself leaves many questions unanswered). But one thing that is innovative is how it pulls the privacy policy out from the tiny legalese fine print in the footer, and expands on it to try to make it comprehensible to users.

Here's another example:



Privacy icons by Aza Raskin.

Former Mozilla designer Aza Raskin created a whole slew of privacy icons to instantly communicate to users how their data is used.

These examples are more about informing users than allowing them to take action. Much more could still be done to give control. But explaining—whether through approachable language, content organization, or design—is a great first step.

MAKE PRIVACY A CORE TEAM SKILLSET

Developers oftentimes don't know optimal storage configurations to help protect users. ("Let's anonymize the logs" is a typical, and unsatisfactory, solution.) Advocate hiring

someone for this expertise, such as someone who went through a program specifically studying online privacy—like Carnegie Mellon's IT master's with a privacy engineering specialization. Or bring in a consultant to advise on a specific project, like the Privacy Guru. If you're part of a bigger company, maybe it's time to consider a chief privacy officer —Acxiom has one.

BUILD PRIVACY INTO YOUR PRODUCT'S DNA

You probably can't compete on privacy alone, but combining usability with privacy—like Heartbeat does—can be an advantage. Or, build third-party products that encourage privacy, such as the rating system for apps (PDF) that would let consumers know how private and secure they are that a group of computer scientists proposed. I talked with Columbia professor Henning Schulzrinne, who recommended an Energy Star-like privacy rating system, and futurist Marcel Bullinga, who told me about an idea for a universal dashboard that would allow users to control their privacy across the internet. The Electronic Frontier Foundation's Privacy Badger blocks advertisers and trackers that collect data, while Lightbeam, a browser add-on for Firefox, shows you who's accessing data on every site you visit.

RECONSIDER THE ADS YOU RUN

Les Orchard and Doc Searls, among others, have written about how ad-tracking software can delay site load speeds, degrading the user's experience.

CULTIVATE YOUR PRIVACY SKILLS

Take a course on data analytics. Hold a lunch-and-learn at your office about US privacy laws. Share the W3C's guidelines on browser fingerprinting and privacy, the FTC's guidelines for privacy and security for the internet of things and its older report on protecting consumer privacy (PDF), Microsoft's adherence to the ISO's guidelines, or the foundational principles of "Privacy by Design."

It's tough to keep up, but there are resources to help, like the Electronic Privacy Information Center and writers like David Meyer and Kashmir Hill. Write more articles

like this one and come up with other ideas for "privacy by design." Maybe you've built privacy into your process in a cool way. I know I'd love to hear about it.

Be realistic about the hurdles

Bringing privacy into your process is still challenging. First off, usage patterns are one of the basic underpinnings of UX. The vast troves of online data being generated aren't evil in themselves. On the contrary, they hold possibilities for wonderful insights and improvements to life. But there's a fine line between that and invasive—possibly even abusive—behavior. (One pretty unambiguous example is Mattel's Hello Barbie, which records children's voices and transfers them to an online server to process and respond to them.)

Then, there are the users themselves, who seem to sort of care about privacy, but sort of don't. A 2014 report from Pew found that while 80 percent of Americans are concerned about third parties accessing data about them on social networking sites, 55 percent "agree" or "strongly agree" with this statement: "I am willing to share some information about myself with companies in order to use online services for free." Essentially, we've grown accustomed to the commerce of personal information online in exchange for free services. There's the old saw, "If you're not paying for the service, then you're the product." User data is quite the lucrative product, too. There's arguably a *disadvantage* to throttling its flow. (See: Google's market cap of $360 billion.) Many companies have never even considered that there may be alternatives to the current user-data-for-service model of so much of the internet.

Then there's this notion of "Minimum Viable Product Disease," where products are rushed out the door before privacy is taken into account. That's no big surprise—adopting privacy as a foundational principle is time-consuming and expensive, as ad company 4info found.

Try anyway

The fact that it's hard doesn't mean we're off the hook. Just as we have a responsibility to design accessible products, even when it'd be easier not to, we have a responsibility to consider privacy. We all have a role in shaping the way products are delivered, ensuring they serve users' interests in an era when the notion of private life has been thoroughly compromised. So let's do it mindfully, not limiting our considerations to features that users see. Instead, let's look underneath and above, reach further into the future, and think bigger about what user experience is.

Further reading about

User Experience

How to Sell UX Research with Two Simple Questions

It's one reason why so many UX designers are frustrated in their job and why many projects fail. And it's also why we often can't sell research: every decision-maker is confident in their own mental picture. In this article, Sophia Prater shows you how to collaboratively expose misalignment and gaps in your team's shared understanding by bringing the team together around two simple questions. What are the objects? How do they relate?

Design for Safety, An Excerpt

None of us want to build products that put our users' safety at risk, but how do you reduce the risk that our products will be weaponized by abusers? In this excerpt from Design for Safety, Eva PenzeyMoog offers a clear strategy for building inclusive safety in our products.

About the Author

Alex Schmidt

Alex Schmidt is a UX strategist and researcher. As an award-winning journalist, her work has been published on/in NPR, Marketplace, The Los Angeles Times, and NewYorker.com, among other outlets. She is based currently in New York City, but is originally (and in the future) of Los Angeles.

9 Reader Comments

1

Tigt

September 22, 2015 at 11:45 am

It would be sweet of you guys to replace the “(here, here, here, here, here, and here)” set of links in the 3rd paragraph with domain names or something, for screen-readers and mobile users.

As far as privacy goes, is there any data on how people feel about the “green lock” for HTTPS? Yellow or broken ones?

2

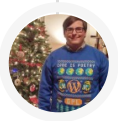
Alex Schmidt

September 22, 2015 at 3:09 pm

Hey Tigt — I’ll leave your first point to the ALA editors.

On the second, that’s a great question and my answer is: not sure. A guess, based on the Pew research report I referenced, is that people don’t know a much about HTTP vis-a-vis HTTPS, or the colors associated. That’s one reason that something as simple as “privacy icons” could go a long way. We could be doing a heckuva lot better at communicating.

3



Luke Pettway

September 23, 2015 at 8:36 am

I'm in total agreement with this. There should be a workflow designated for handling sensitive data that is overseen by someone who is qualified to handle this data and understands the risks. For example this could be the HIPAA ambassador who makes sure that are requirements are met using a checklist. All data used in testing should be fake, and in a separate database, and only people who need to see any real data should ever have access to see it.

To sum it all up:

Least Privileged Access
Proper Workflows that follow PCI/HIPAA compliance
Separate data for testing vs real use cases
Proper Auditing Process for validating security (Be Proactive)

4

Alex Schmidt

September 24, 2015 at 9:35 am

Hey Luke – These are awesome ideas. Making it someone's job, integrating into the workflow more clearly…cosign 100%.

5

Andi Galpern

October 1, 2015 at 4:40 am

Alex, thank you for writing this article. There is so much good information in here.

6

Alex Schmidt

October 1, 2015 at 10:07 am

I'm so glad you found it useful, Andi!

7

Policia

October 2, 2015 at 11:30 am

Thank for this article, great!

8

Brit Tammeorg

October 28, 2015 at 9:33 am

Great article. I actually read it several times, which is for me pretty rare thing to do these days. I wanted to also say that I have mentioned you at my latest blog post (https://goo.gl/4KxjEa). I hope you appreciate it.

Thanks and keep up the good work!

9

topbagsus

January 12, 2016 at 8:25 am

I noticed myself with the same issues many times. I've personally started using Men

GOT SOMETHING TO SAY?

We have turned off comments, but you can see what folks had to say before we did so.

More from ALA

Breaking Out of the Box

by **Patrick Brosset**

What can we do with thirty pixels? Windows Controls Overlay frees us from 40 years of history telling us how apps should look.

Code · December 09, 2021

How to Sell UX Research with Two Simple Questions

by **Sophia V. Prater**

Seriously, do not ever design screens again without first answering these questions: what are the objects and how do they relate?

User Experience · October 21, 2021

A Content Model Is Not a Design System

by **Mike Wills**

Why do so many content models still look more like design systems rather than reflecting structured data? Mike Wills takes us on a personal journey as he examines his own past experiences and invites us to conceive content models that articulate meaning and group related content together for use on any channel.

Content · September 23, 2021

Design for Safety, An Excerpt

by **Eva PenzeyMoog**

In this excerpt from Design for Safety, Eva PenzeyMoog discusses concrete ways you can incorporate safety awareness into your design processes.

Process · August 26, 2021

Sustainable Web Design, An Excerpt

by **Tom Greenwood**

In this excerpt from Sustainable Web Design, Tom Greenwood provides clear guidance on how to track and address the carbon footprint of our websites.

Design · August 05, 2021

ISSN 1534-0295 · Copyright © 1998–2022 A List Apart & Our Authors

Proudly powered by WordPress · Hosted by Pressable