

DESIGNING FOR PRIVACY IN AN INCREASINGLY PUBLIC WORLD



" Privacy is not about secrecy. It's all about control."

—Dr. Ann Cavoukian, privacy by design leader, former Information and Privacy Commissioner for Ontario

What's the big deal with privacy? I've got nothing to hide!

Privacy isn't about being secretive.

It's about maintaining control of your own information.

Sometimes we don't understand the need for privacy until it affect us, personally.

As a result of the COVID-19 pandemic, for example, identity theft doubled from 2019 to 2020, making privacy and security issues more relevant than ever.

Even if we're not concerned with privacy issues, we're not designing for ourselves. If we're designing with empathy, we'll consider the needs of people not like ourselves — people with different backgrounds and experiences.

As designers, we're uniquely positioned to take the lead with this issue.

"Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say."

—Edward Snowden



5 Pillars for Privacy by Design

CULTURE

Cultivate a privacy by design culture

Many organizations devote little time to developing a culture of privacy by design.

Inclusive design plays a significant role here: If you're thinking inclusively, you'll be thinking about privacy. Accessibility and privacy are intertwined too.

DATA

87% of the U.S. population can be uniquely identified by just their date of birth, gender, ZIP code. Those items aren't even considered PII.

PERSONALLY IDENTIFIABLE INFORMATION

PII: INFORMATION WHICH CAN BE USED TO IDENTIFY A SINGLE SPECIFIC INDIVIDUAL



Only collect the data you need

Companies tend to want to Hoover up whatever data they can. Don't be afraid to ask, "Why do we need that?"

Be transparent

Be transparent—not only with what data is used and why, but with who it's given to. People may not realize a single site shares their data with 100s of third parties. PII can be misused for identity theft, so your customers need to feel safe handing it over.

PATTERNS

Avoid deceptive patterns

Deceptive patterns trick people into doing things they didn't mean to do—like share their contacts or other personal information.

Read up on deceptive patterns and don't allow them into your designs. Harry Brignull's work is a great place to start.

LANGUAGE

Use language with care

Language can be used to obscure privacy issues and to confuse users. Use clear language with marketing copy, as well as legal and privacy policies.

Write to the average reading level

The average reading level in the United States is at about the 8th grade level. If you're not writing to that level, you may be making it difficult for your users to understand important content.

TOOLS

Provide tools for protecting data

Give users options to control their personal information. You could advocate for a Privacy microsite or tool box to highlight these features.

Ensure privacy features are discoverable

Make these features easy to find and offer them contextually. Privacy information can be highlighted during onboarding and via "just in time" alerts, which appear when you're using an experience in a new way.

California's Opt-Out Icon draws attention to features, which allow consumers to opt out of sharing their personal information with third parties.



Remind users of privacy features

Reminding users to review their privacy settings can instill trust with them that a company has their best interests at heart.

Offer these reminders proactively, regularly.

Never change privacy settings without warning users

Alert users in advance whenever changes need to be made to privacy settings. Avoid making changes, which may endanger users (people!) within at-risk groups.

AI & PRIVACY

- What if AI-designed patterns "work" but undermine privacy?
- How is AI using the data entered with a prompt?
- Are you explaining to users how data is used and shared? Clearly and prominently? Consider patterns for disclosure.
- How might data accidentally be exposed?
- Should you be anonymizing data? Can you truly anonymize data?

WHY SHOULD OUR CLIENTS CARE?

Discussing privacy issues with clients can be sticky. But ignoring them for short-term benefits can lead to long-term costs.

To remind your clients that respecting the privacy of their customers is important, focus on the following themes ...

- **Civic responsibility** - Encourage your clients to exercise leadership in respecting users' privacy.
- **Reputation management** - Remind clients their brand can be tarnished if they fail to respect people's privacy.
- **Site abandonment** - Users may leave their site for another if they perceive their privacy is being undermined in the moment.
- **Loss of user base** - If the experience is bad enough, customers may abandon their business altogether.
- **Financial impact** - Increasingly, legislation and regulations mean fines for companies, which ignore users' privacy.



WEBSITE



ARTICLE

technique

A Technique artifact
Prepared by Robert Stribley
Contact us for more information about privacy by design—or how to craft better digital experiences
www.thisistechneque.com