Developing for privacy

Heather Burns // Dutch PHP Conference // 7 June 2019

What you will learn today

What you will learn today

- How to define a healthy approach to user privacy
- How to integrate the Privacy by Design framework into your workflow
- What's the status of current and upcoming privacy legislation
- Where to find tools and resources to help you along the way

What you will do with what you learn

What you will do with what you learn

- Understand how to respect privacy as a positive cultural value, not resent it as a negative legal obligation;
- Learn how to integrate best privacy practices into your workflow;
- Prepare to review your existing work for improvements;
- Use the resources, examples, and tools to encourage healthy privacy practices within your projects.

Who am I?

@webdevlaw

- Tech policy and regulation specialist
- Currently a Policy Fellow
- Former web designer
- WordPress.org core-privacy team
- Cross-CMS privacy working group
- Mozilla Open Leaders programme
- Accessibility matters too
- Brexit's impact on tech policy
- **Not a lawyer!**

An overview of the changing data protection and privacy landscape

Europe's privacy overhaul

- GDPR: 25 May 2018
  - Replaced the Data Protection Directive of 1995
  - Maintains original principles, expands and modernises
  - Data at rest: collection, usage, retention
- ePrivacy Regulation: TBD (autumn 2019-ish)
  - Replaces the ePrivacy Directive of 2002
  - Data in transit: cookies, telemetry, advertising beacons, marketing
  - Colloquially and somewhat inaccurately known as the "Cookie Law"

Who is subject to GDPR and ePD?

- All data collected, processed, and retained about persons within the European Union
- Extraterritorial: applies to non-EU collection and processing
- All capturing and/or processing of personal data: no minimum size or turnover
- All situations: public sector, private sector, academia, startup, side project, or hobby

GDPR essentials

https://www.smashingmagazine.com/2018/02/gdpr-for-web-developers/

What you have	Awareness	Documentation	Privacy Notices	Children
How you engage	Individual Rights	PbD and DPbD	Consent	Lawful Basis
How you work	Subject Access Requests	Data Breaches	DPOs	International

GDPR: what is personal data?

- **Personal data:** any information relating to an identified or identifiable natural person. This can be one piece of information or multiple data points combined in a record
- **Sensitive personal data:** information about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health data, sex life or sexual orientation, past or spent criminal convictions
- **New definitions:** genetic data, biometric data, location data, and online identifiers (e.g. database identifiers)

How is that different from PII?

PII = Americanism

- Full name (if not common)
- Face (sometimes)
- Home address
- Email address (if private from an association/club membership, etc.)
- National ID number (e.g., SSN)
- Passport number
- License plate number
- Driver's license number
- Face, fingerprints, or handwriting
- Credit card numbers
- Digital identity
- Date of birth
- Birthplace
- Genetic information
- Telephone number
- Login name, screen name, nickname, or handle

What *might* be PII?

- First or last name, if common
- Country, state, postcode or city of residence
- Age, especially if non-specific
- Gender or race
- Name of the school they attend or workplace
- Grades, salary, or job position
- Criminal record
- Cookies

America is legislating privacy

"US GDPR" NTIA standards	BROWSER Act	SPADA	Internet Bill of Rights
FTC Privacy Act changes	Social Media Privacy and Consumer Rights Act	CONSENT Act	Resolution on applying GDPR protections to U.S. citizens

California Consumer Privacy Act (CCPA)

- Takes effect 01/01/20, and becomes enforceable 1 July 2020
- Applies to any business with California users or customers:
  - Applies to for-profit businesses with gross revenues in excess of $25 million OR alone or in combination, holds data on >50,000 households, consumers, or devices, OR derives >50% of revenues from selling consumer PII
  - Does not apply to nonprofits
- If you prepared well for GDPR, you're about 75% of the way there already

Why does that matter?

It matters because of the different cultural, historical, and legal views of privacy across the Atlantic.

Open source software is made by the people who show up.

We have very different cultural approaches to privacy.

European cultural approach to privacy

- Privacy is a fundamental human right
- Data belongs to the subject
- Opt-in culture
- Culture of constructive work through regulators, with fines or court action a rare last resort
- People trust governments and fear businesses

American cultural approach to privacy

- Free speech is a fundamental human right
- Data belongs to the site/service owner
- Opt-out culture
- Culture of adversarial courtroom litigation
- People fear governments and trust businesses

These cultural differences were born from very different historical experiences.

European historical approach to privacy

- Collective/social approach
- Human > individual rights
- Legacy of holocausts, genocides, state totalitarianism
- European privacy approach is a form of atonement

American historical approach to privacy

- Individual approach
- Individual > human rights
- East coast “Puritan” legacy: private life should be public
- West coast “Frontier” legacy: freedom to do what you want without consent

These historical experiences led to very different legal approaches to privacy.

European legal approach to privacy

- Privacy is regulated through hard law
- One overarching law for all member states and sectors
- Data protection regulators
- Not tied to citizenship or nationality
- Privacy is its own law
- Litigation is the last resort

American legal approach to privacy

- Privacy is governed through soft law
- No overarching DP law; piecemeal approach across sectors and states
- No data protection regulator
- Tied to citizenship and nationality
- Privacy is a subcategory of contract, tort, or property law
- Litigation is the first resort

We all come to the table with a different understanding of what privacy is and how it works.

and we've never understood our differences, much less acknowledged them.

What's the result of that?

- We *structure* our work with different cultural approaches to privacy
- We *write* our code with different legal approaches to privacy
- We *assume* everyone we code with works and thinks like we do
- We *create* the open web with no common standard for privacy
- We *fail* to do everything we could do to protect the people in the data
- We *don't* learn from our mistakes.

We have to do better.

And the first step to doing better is to understanding where we are coming from before we can know where we're going.

(uh, so where are we going?)

We’re going to shift our thinking.

We’re going to stop thinking of privacy as a complicated and scary legal problem to run away from…

…and we’re going to start thinking of it as an easy and positive development mindset to embrace.

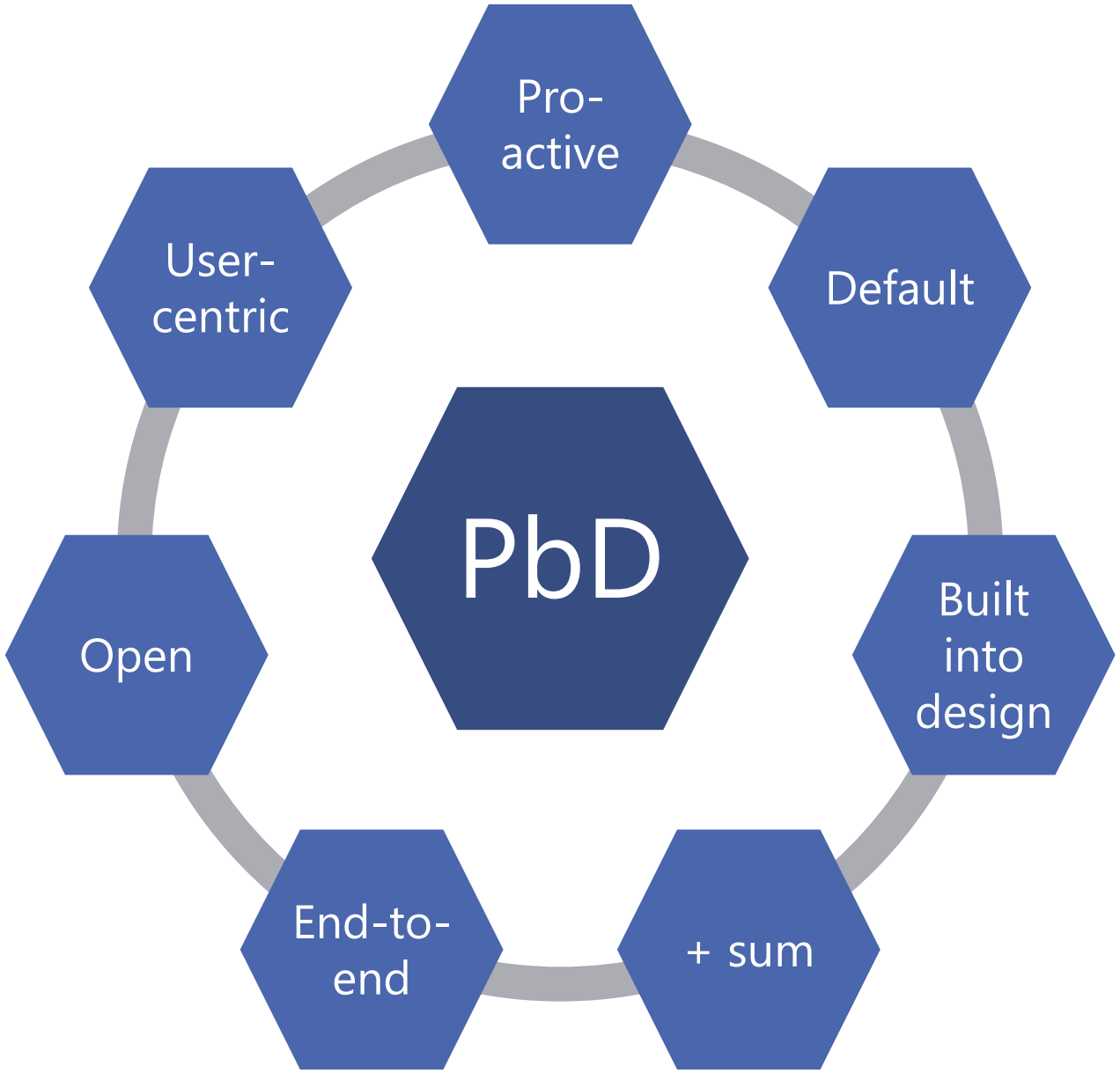
(ok, that's brilliant Heather,
now how do we do that?)

Privacy by Design

https://www.smashingmagazine.com/2017/07/privacy-by-design-framework/

What is Privacy by Design?

- Non-regulatory development framework devised in Canada in the 1990s
- Incorporated into GDPR as a requirement
- Review your existing projects for PbD compliance, and make it a part of your development workflow from now on
- https://www.smashingmagazine.com/2017/07/privacy-by-design-framework/



The seven principles of Privacy by Design

Checking your project on PBD

Questions from the UK ICO

- ❑ *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*
- ❑ *We anticipate risks and privacy-invasive events before they occur, and take steps to prevent harm to individuals*

Checking your project on PBD

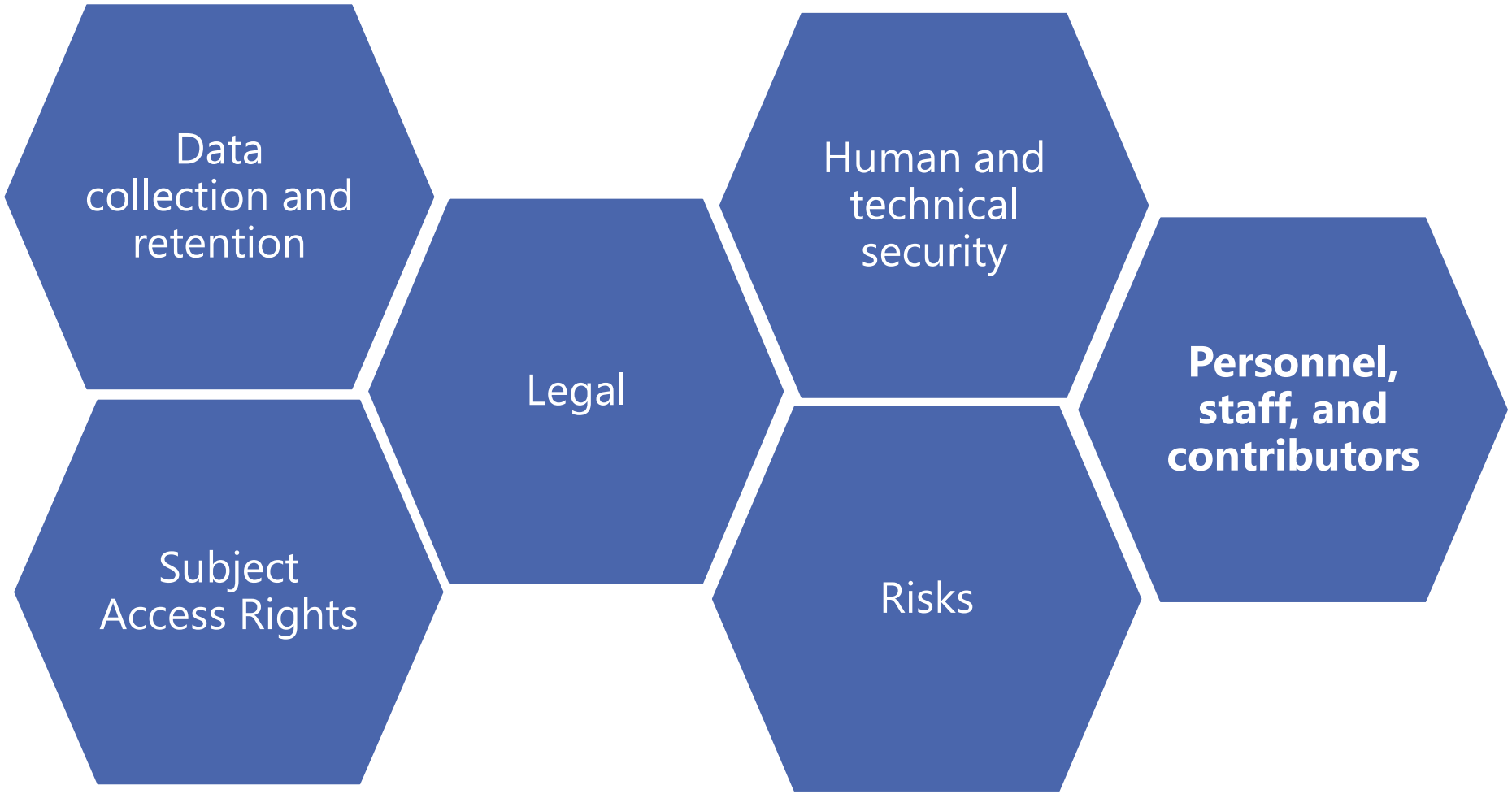
Questions from the UK ICO

- *We ensure that personal data is automatically protected in any system, service, product, and/or business practice, so that individuals should not have to take any specific action to protect their privacy*
- *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 into account.*

PBD: Privacy Impact Assessments

- A living document which must be accessible to all
- Document what you are doing and why (consent/legal basis)
- Document the risks
    - To the data subjects
    - To the organisation
    - To technical and systems
- Document your risk mitigation

PBD: Privacy Impact Assessments



PIA questions:
Personnel, staff, and contributors

- Who has access to the data?
- What data protection training have those individuals received?
- What security measures do those individuals work with?
- What data breach notification and alert procedures are in place?
- What procedures are in place for government requests?

PIA questions:
Personnel, staff, and contributors

- What data protection training have those individuals received?
  - European data protection and privacy framework
  - Industry or sector regulations (health, finance, etc)
  - Development frameworks and methodologies
  - Documentation of training in HR records
  - Inductions and refreshers

What if you don’t have a privacy law to use to structure your work?

Remember, privacy isn't just about law – it's about values and practices.

What are common privacy values?

Derived from several international standards, frameworks, and agreements

Data minimisation

Collect only the data you need and no more

Data integrity

Ensure that the data is true, authentic, and up to date

Purpose minimisation

Use the data only for the purpose you collected it for and nothing else

Lifecycle limitation

Do not use the data for other purposes, keep it longer than you need, or share it with others without reason

Human and technical security

Take adequate technical and human measures to protect the data from misuse and its subjects from harm

Transparency and notice

Make public what data you hold, why you hold it, and what you do with it

User participation and rights

Give people rights to access their data, correct mistakes, and the ability to ask you to stop using their data

Accountability, enforcement, and redress

Fix problems when things go wrong, make it right when people are hurt, and face the consequences for misuse.

Choice, control, and consent

Give people choices, options, and rights over how you use their data at any time

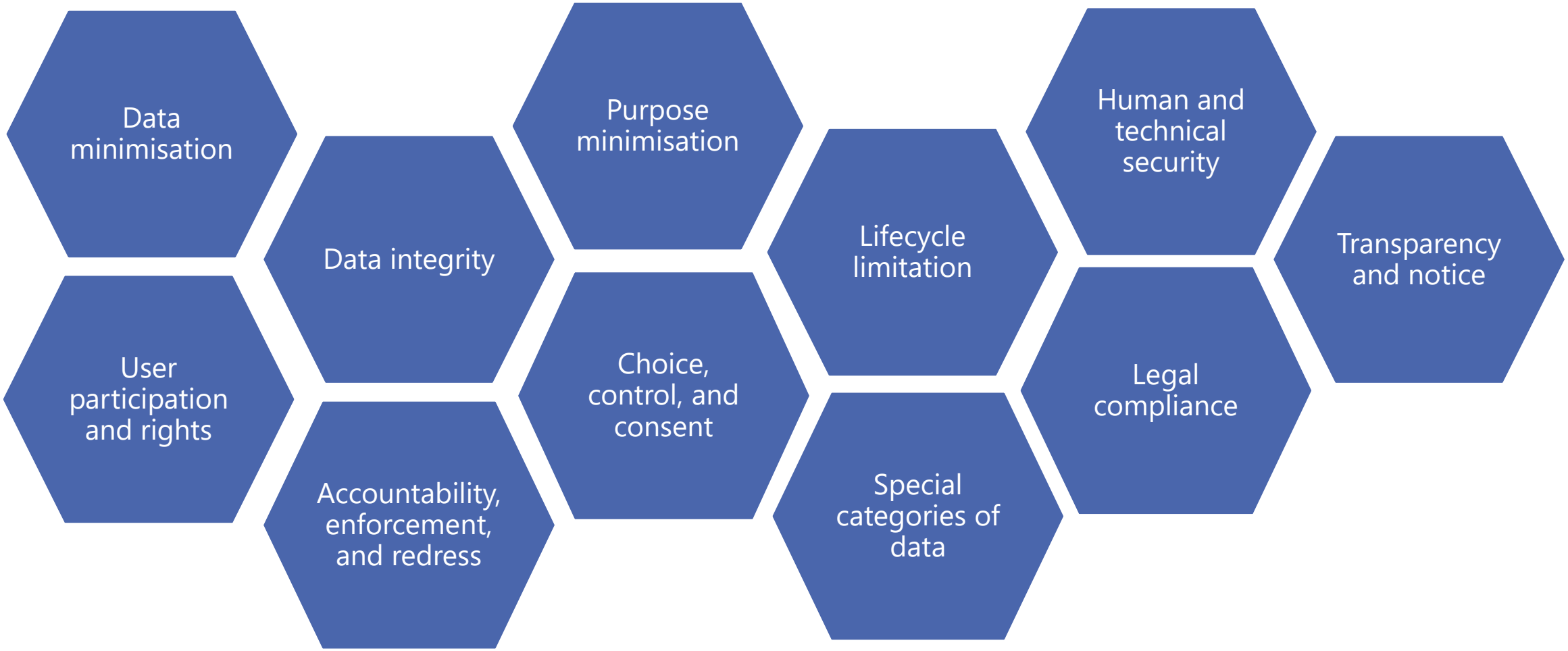
Special categories of data

Take care with sensitive data which could result in the people it is about being hurt

Legal compliance

Work cooperatively and productively with regulations, laws, and supervisory bodies

11 universal privacy principles



https://github.com/webdevlaw/open-source-privacy-standards

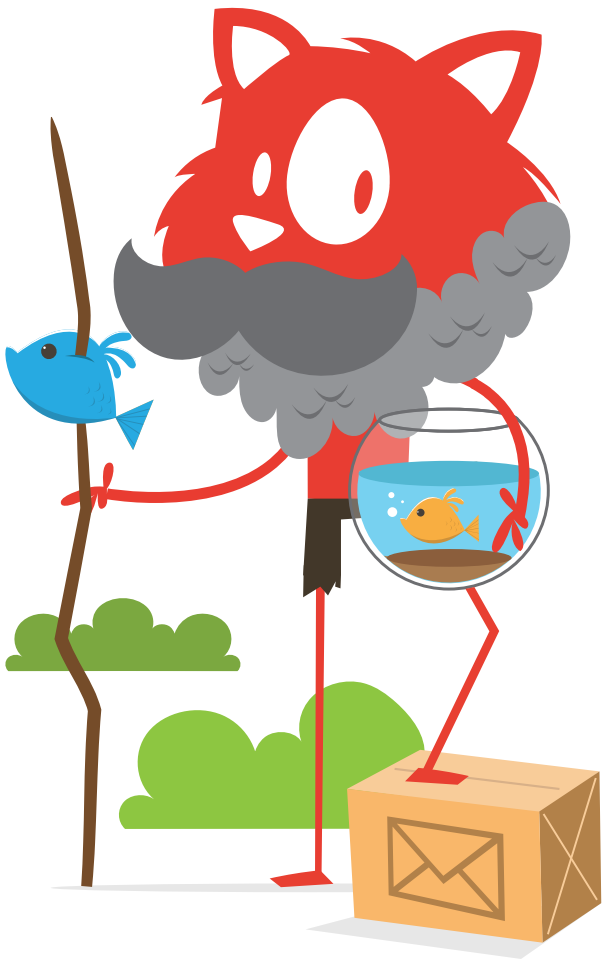
Design Resources @ Smashing

Part 1: Privacy Concerns And Privacy In Web Forms

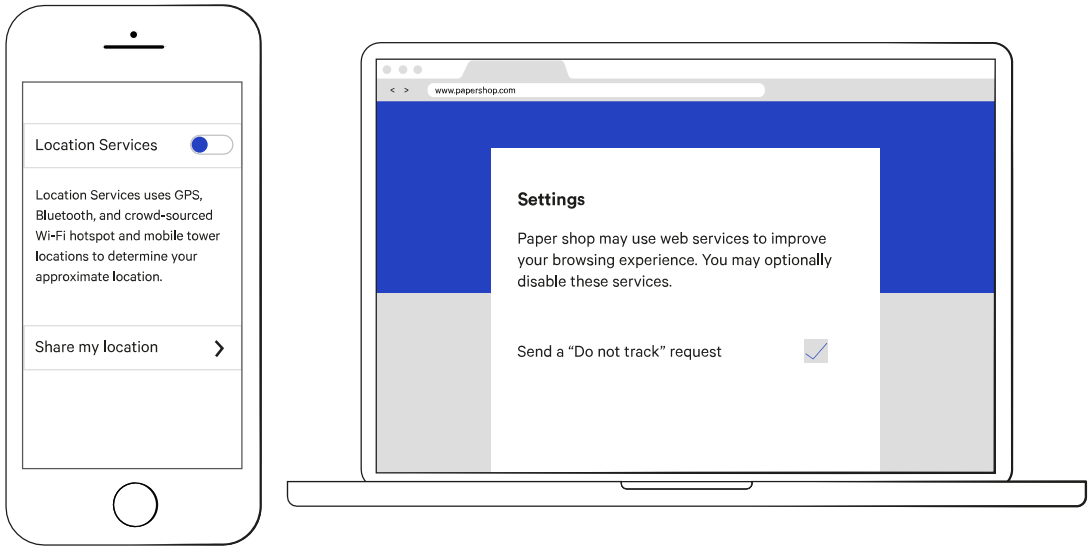
Part 2: Better Cookie Consent Experiences

Part 3: Better Notifications UX And Permission Requests

Part 4: Privacy-aware Design Framework



More design libraries and guides



- Data permissions catalogue for designing for consent (Projects by IF)
- Design for privacy - how will the ePrivacy revamp affect UX/design
- IAPP UX guide to getting consent
- Bridging privacy policy with product design
- Shaping Choices in the Digital World

Where to start?

- ❑ Review your data capture, sharing, flows, and retention
- ❑ Conduct a Privacy Impact Assessment
- ❑ Document your knowledge and gaps
- ❑ Read up on GDPR, PBD, the upcoming US privacy laws, and best practice privacy standards
- ❑ Become privacy champions in your workplaces
- ❑ Demonstrate leadership in privacy within your project contributions

What have you learned today?

By now I hope you know how to

- respect privacy as a positive cultural value, rather than resent it as a negative legal obligation;
- integrate best privacy practice into your development workflow;
- make a plan to review your existing work for privacy improvements;
- access the tools, resources, and articles available to help you.

Now show me what you can do!

- @webdevlaw
- https://webdevlaw.uk/data-protection-gdpr
- https://github.com/webdevlaw/open-source-privacy-standards
- https://www.smashingmagazine.com/2018/02/gdpr-for-web-developers/
- https://www.smashingmagazine.com/2017/07/privacy-by-design-framework/