What you will learn today
What you will learn today:

**Why** privacy can be so challenging in our projects

**How** we cause problems we didn’t intend to create

**What** we can do better, whatever role we play

**Where** to find resources to help us along the way
What you will do with what you learn
What you will do with what you learn

<table>
<thead>
<tr>
<th>Shift</th>
<th>Shift your thinking on what privacy is all about;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recognise</td>
<td>Recognise where privacy problems can begin – and end</td>
</tr>
<tr>
<td>Understand</td>
<td>Understand how to integrate best privacy practices into your projects;</td>
</tr>
<tr>
<td>Learn</td>
<td>Learn what resources, examples, and tools are available to you</td>
</tr>
</tbody>
</table>
Who am I?

- Tech policy and regulation specialist
- Currently working in tech politics
- Former web designer
- WordPress.org core-privacy team
- Cross-CMS privacy working group
- Mozilla Open Leaders programme
- **Not a lawyer!**
Have you ever asked yourself “how did we get here?”

(and I don’t mean 2 buses, 3 airports, 2 planes, 3 trains, and a rail replacement bus)
What everyone in this room thinks the web is about
What everyone outside this room* thinks the web is about

- Analytics and tracking
- Corporate surveillance
- Government surveillance
- iOT and domestic surveillance
- Social media abuse
- Electoral interference
- Trolling/harassment/abuse
- Racism/authoritarianism

*who holds political power
They think we’re the bad guys.
And privacy is at the heart of it.
Privacy is changing.
Are we keeping up?
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: early 2020**
- Replaces the ePrivacy Directive of 2002
- Data in transit: cookies, telemetry, advertising beacons, marketing
- Colloquially 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.
How GDPR changed how you develop

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

ABOUT THE AUTHOR
Heather Burns is a tech policy and regulation specialist from Glasgow, Scotland. She

QUICK SUMMA
about the sites and ways you collect a
<table>
<thead>
<tr>
<th>What you have</th>
<th>Awareness</th>
<th>Documentation</th>
<th>Privacy Notices</th>
<th>Children</th>
</tr>
</thead>
<tbody>
<tr>
<td>How you engage</td>
<td>Individual Rights</td>
<td>PbD and DPbD</td>
<td>Consent</td>
<td>Lawful Basis</td>
</tr>
<tr>
<td>How you work</td>
<td>Subject Access Requests</td>
<td>Data Breaches</td>
<td>DPOs</td>
<td>International</td>
</tr>
</tbody>
</table>
**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
The US is getting the hint about the need for privacy legislation

- “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 who meet the following criteria:
  - 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.
The web is made by the people who show up to make it.
And when it comes to privacy, we don’t have a clue about each other.
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 our projects 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 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 understand where we are starting 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?)
Where privacy matters

• Project management
• Development and coding
• Design and UX
Project management
First you need a framework.
Privacy by Design

How To Protect Your Users With The Privacy By Design Framework

QUICK SUMMARY ~ In these politically uncertain times, developers can help to defend their users' personal privacy by adopting the Privacy by Design (PbD) framework. These common...
What is Privacy by Design?

- Non-regulatory development framework devised in Canada in the 1990s
- Incorporated into GDPR as a requirement
- Make it a part of your development workflow from now on
The seven principles of Privacy by Design
Then you need to do some documentation.
Privacy Impact Assessments

• A living document which must be accessible to everyone involved in a project
• 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
• This document can be requisitioned by a data protection regulator
Privacy Impact Assessments

- Data collection and retention
- Subject access rights
- Human and technical security
- Legal compliance
- Risks
- Personnel, staff, and contributors
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?
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
Document it or it didn’t happen.
Checklist: Privacy in project management

- Privacy by Design
- Privacy Impact Assessments
- Data audits
- Data processing agreements
- Staff training and professional development
- Preparing for user rights
- Preparing for data breaches
- Document it or it didn’t happen
Development and coding
Coding standards

• Create a list of approved code libraries, tools, and frameworks
  • Programming languages, version control systems
  • Testing tools, infrastructure, monitoring tools, logging servers
  • Third party frameworks and APIs

• Disable unsafe/unnecessary modules

• Disable unnecessary data retention

• Code reviews should include data maps
System design

- Data minimisation, limitation, and deletion
- Encryption in transit and at rest
- Data sandboxing, separation, and aggregation
- Pseudonymisation, anonymisation
- Design reviews should view data flows through the eyes of an attacker
Testing and maintenance

- Dynamic testing for edge cases in the data
- Fuzz testing by intentionally triggering errors
- Penetration testing for data protection by design
- Security vulnerabilities and upgrades
- Incident logging and data breach preparation
Checklist: Privacy in development and coding

- Privacy by Design
- Privacy Impact Assessments
- Design requirements
- Coding standards
- Development guidelines
- Technical and security measures
- Consent and subject access mechanisms
- Testing and maintenance
Design and UX
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

• Dark Patterns (don’t do these!)
Checklist: Privacy in design and UX

- Designing to protect
- Designing for user rights
- Designing to inform
- Designing for consent
- Removing friction from good privacy options
- Introducing friction in front of negative privacy options
- Avoiding dark patterns and deceptive UX
...and one thing I don’t want you to do
Ethics washing

When ethics and codes of practice are used as a substitute for legal compliance

...or a means to cover up for the lack of it
What have you learned today?

• **Why** privacy can be so challenging in our projects
• **How** we cause problems we didn’t intend to create
• **What** we can do better, whatever role we play
• **Where** to find resources to help us along the way
Where to start?

- Talk about what you know – and what you don’t
- Review your data capture, sharing, flows, and retention
- Conduct a Privacy Impact Assessment
- Read up on GDPR, PBD, and the upcoming US privacy laws
- Take a look at your design and consent patterns
- Become privacy champions in your workplaces
- Contribute to privacy in open source projects
The Privacy Book
(ttitle TBD)
(help!)
You are people of enormous power and influence over privacy on the web.
The actions you take within your projects, however small, can protect the people in the data from those who would use that data to hurt them.
Let’s work to make the web a better place.
Now get started.

- @webdevlaw
- https://webdevlaw.uk/
- https://afterbrexit.tech
- https://www.smashingmagazine.com/2018/02/gdpr-for-web-developers/
- ...the book (late spring – early summer 2020)