and you may ask yourself, how did I get here?

Heather Burns // CodeMobile // 4 April 2019

Who am I?

@webdevlaw, for one

- Tech policy and regulation specialist
- Former web designer
- WordPress.org core-privacy team
- Cross-CMS privacy working group
- Mozilla Open Leaders programme
- Accessibility too
- Brexit's impact on tech policy

- Hire me 👍

things don’t always work out the way we planned.

0

days since a privacy scandal

Diplomats gonna diplomacy

(Spoiler: they don’t say very nice things about you.)

(but I think you’re pretty awesome.)

You are people of enormous power and influence over privacy on the web.

How can you help put things right?

1. Understand each other

Software is made
by those of us
who show up.

Thing is,
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 approaches.

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.

You have to understand where your team has come from before you can know where you're going.

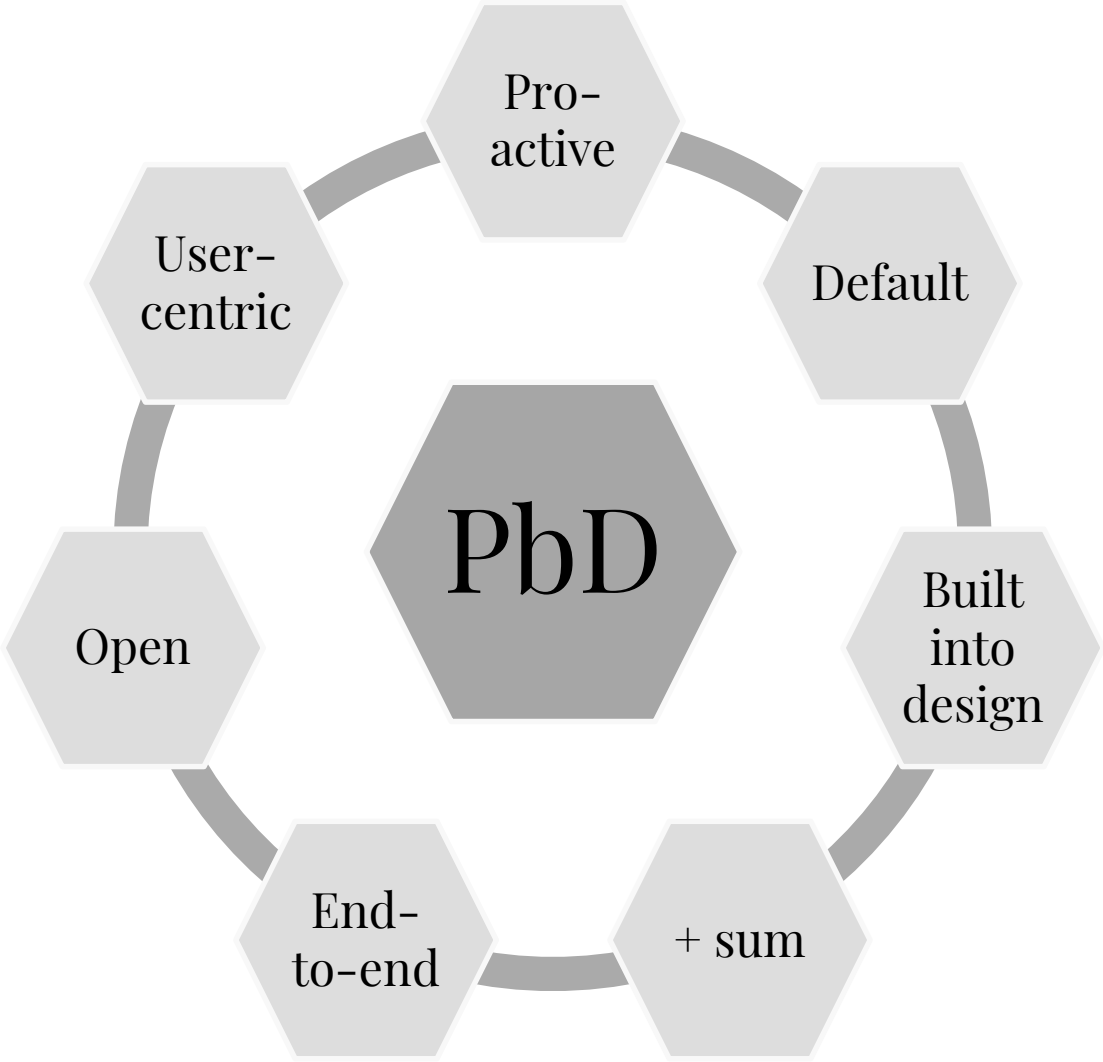
2. Hold yourself accountable

“the era of move fast and break things is over”

Hemant Tajena, writing in the Harvard Business Review

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 retrofit as required
- 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 the project on PBD

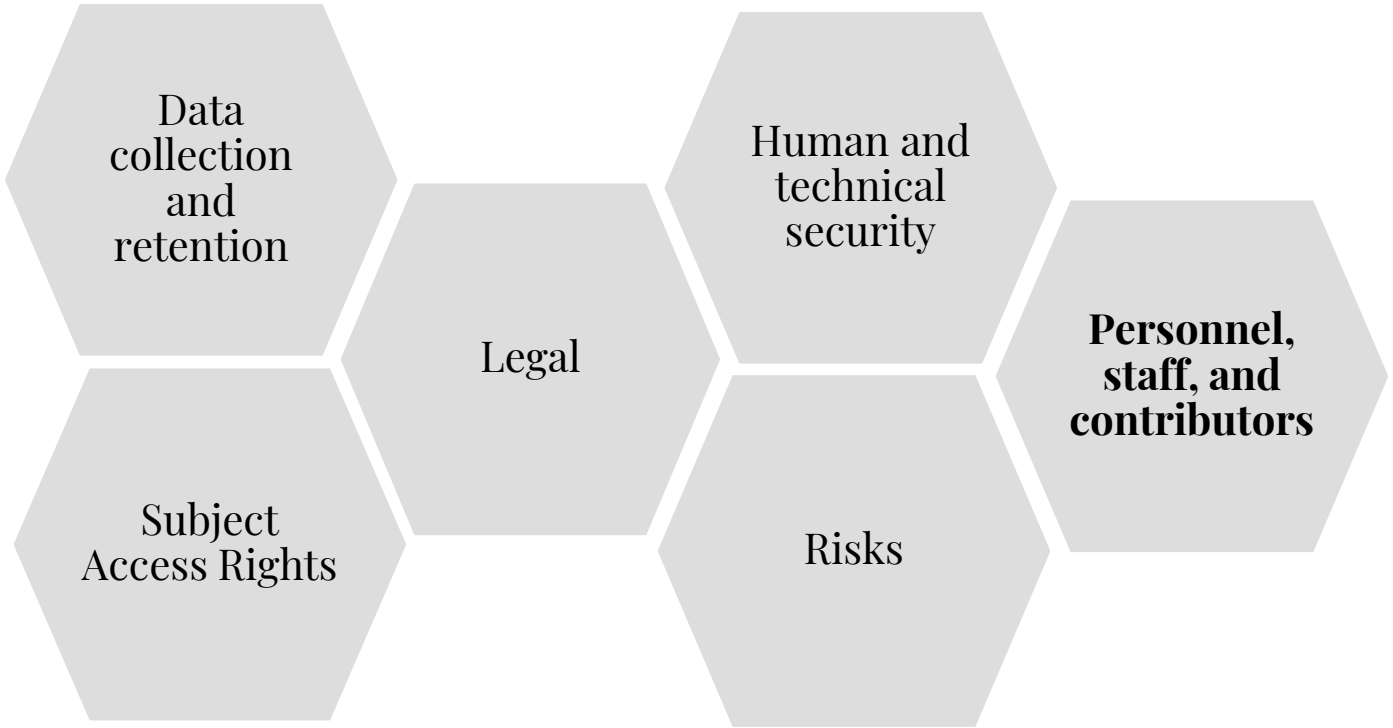
Questions from the UK ICO

- 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.

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 data subjects, your organisation, and your 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

Review what you do, why
you do it, who does it,
and what they know.

Document it.
Document all of it.
Document it all the time.

3. Ethics aren’t enough

“the era of move fast and break things is over”

Hemant Tajena, writing in the Harvard Business Review

“the era of move fast and break things is over…

It is intellectually inconsistent to preach about a disruptive, billion-dollar vision and imagine it as being free from regulatory considerations. It fascinates me how often entrepreneurs lack a basic grounding in the regulatory hurdles they may face.”

Hemant Tajena, writing in the Harvard Business Review

“Ethics give us the tools to take a critical look at how we make decisions, and to determine whether they grant users agency, rights, protections, and the opportunity to flourish.

Yet ethics do not stand alone. They merely lay the foundation for larger frameworks of social contracts encompassing policy, governance, law, and human rights.”

Ethics washing

Is when ethics projects are devised and adopted *in lieu of* a healthy approach to privacy laws and regulations.

These codes are rarely deployed to *complement* privacy laws and the rights they grant users; instead, they are often used to *circumvent* them.

Why is ethics washing bad?

- It is the *opposite* of good ethical process
- It *increases* governance risks
- It allows villains to play the hero
- It signals a belief that projects are above the law
- It signals a belief that projects can “mark their own homework”
- It shifts the moral responsibility for safeguarding privacy from the project to the user

Six tests to guard against ethics washing

1. There must be early and regular engagement with external stakeholders.
2. There must be a means of external, but not necessarily public, independent oversight.
3. There must be transparent procedures on why choices were made.
4. There must be a stable framework of non-arbitrary standards which can be used to reference the selection of certain values, ethics, and rights over other ones.
5. There must be a clear indication that the selected ethics do not substitute for fundamental human or citizen rights.
6. There must be a clear statement on the relationship between the principles declared and any existing legal or regulatory frameworks, including an explanation of what will happen if the principles and the law are in conflict.

-Ben Wagner, Vienna University

“We owe it ourselves and our users to use ethics *the right way* to help shape the privacy rules and regulations which govern our craft, to differentiate between best practices and the rule of law, and to ensure the paths we carve for our users lead to human flourishing.

And we owe it to ourselves to understand the important role ethics can play, and learn to use them to build better futures, rather than exploit the trend to use them as a loophole around the law and the rights it grants our users.”

https://wordpress.tv/2018/07/06/morten-rand-hendriksen-the-ethics-of-web-design/

Reclaim your craft

(take back control)

1. Understand each other

2. Hold yourself accountable

3. Ethics aren’t enough

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 together to reclaim our craft.

Thank you!

@webdevlaw

https://webdevlaw.uk
https://afterbrexit.tech