Getting your privacy notices ready for GDPR

Heather Burns // WordCamp London // 15 April 2018

WORDCAMP LONDON 2018

Hi, I'm Heather, and I've not been having a very good time lately.

https://flic.kr/p/WgHB31

But I’m having a better time than this guy.

"...long privacy policies are very confusing. And if you make it long and spell out all the detail, then you're probably going to reduce the percent of people who read it and make it accessible to them.

So, one of the things that -- that we've struggled with over time is to make something that is as simple as possible so people can understand it, as well as giving them controls in line in the product in the context of when they're trying to actually use them, taking into account that we don't expect that most people will want to go through and read a full legal document."

- Mark "Sherlock Holmes" Zuckerberg, 10 April 2018

What is changing, and why

Fundamentals don't change

- "The right to be informed"
- Data Protection Directive of 1995 (UK: Data Protection Act of 1998)
- GDPR becomes enforceable on 25 May

Old school


EFF Live Tweets
@EFFLive
Follow
Senator Kennedy tells #Zuckerberg, “Your user agreement sucks. The purpose of the user agreement is to cover Facebook’s rear end, not to inform Facebook’s users of their rights.”
11:30 PM - 10 Apr 2018
130 Retweets 232 Likes
9
130
232

Old school

- US domination of tech meant privacy was seen as a contractual matter, not a cultural one
- This led to privacy policies that were contractual gibberish
- The focus was indeed the company's rear end

GDPR

- GDPR **refreshes, redefines, and reshapes** privacy notices
- The focus is now the data subject, the uses of their data, and their rights over their data – **not** the company's rear end

Who needs a GDPR-ready privacy notice?

You do!

- All sites, apps, businesses, organisations, and services collecting and/or processing personal data in Europe
- All sites, apps, businesses, organisations, and services collecting and/or processing personal data about Europeans
- **We are staying in GDPR** after that thing we're not going to talk about

Where can I get a template?

NO YOU CAN'T GET A TEMPLATE

You actually have to think about this stuff now

- Approach it as a positive exercise
- Refresh, renew, recommit
- Think ethically

Drafting your GDPR-ready privacy notice

How should you approach your privacy notices?

- What you say (content)
- How you say it (voice)
- How you display it (UX)

What information should you include?

Content // Voice // UX

Essential Facts

- Who you are
- What personal data you collect
- What categories (including sensitive)
- The consent or legal basis you collect it by
- Who it is shared with, including third parties
- How long you retain it
- What consent and user access rights people have over their data
- How they can contact you

As you grow

- What Privacy Impact Assessments you have carried out
- How you protect data with technical and security measures
- How you protect international data transfers
- What data breach procedures are in place
- What third parties you receive data *from*
- What automated decision making and/or profiling you do with user data
- Any industry regulatory disclosure requirements

What language should you use?

Content // Voice // UX

Voice

Do use

- Plain English
- Short paragraphs
- Clear sections
- User-centred language
- Language for children
- Language for vulnerable people
- Choices and options

Don’t use

- Hokey language
- Sarcasm or attitude
- Legalese
- Internal jargon
- Company-centred language
- Threatening contract terms
- Take it or leave it

How should you format your notices?

Content // Voice // UX

UX and design

- Layered notices
- “Just-in-time” notices
- Icons and symbols
- Mobile and responsive
- Choices and options
- Unbundled granularity

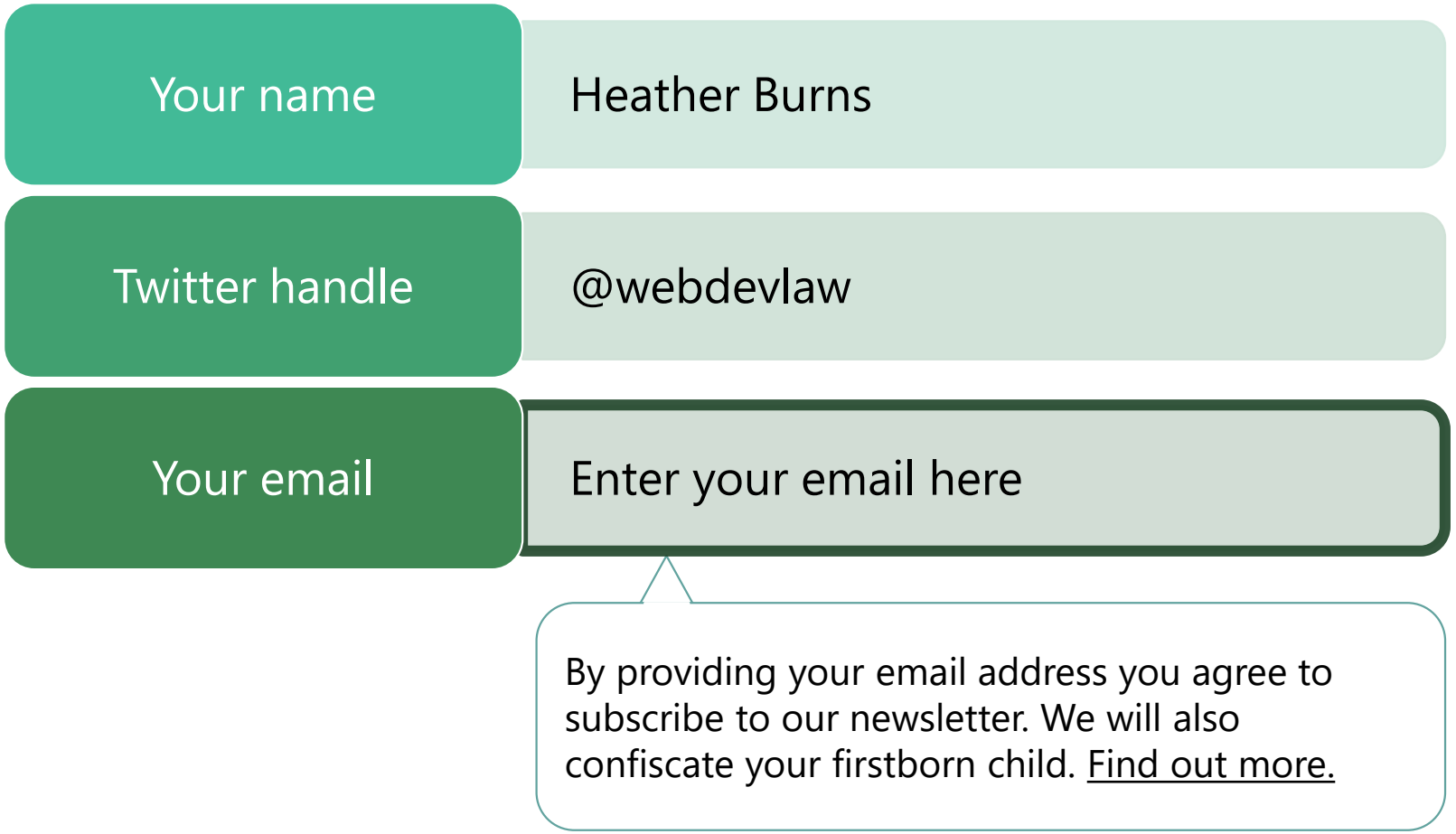
UX and design

Layered notices

- Who are we?
- What information do we collect?
- Why do we collect it?

UX and design

“Just-in-time” notices (tooltips, etc)



UX and design

Icons and symbols


Account details

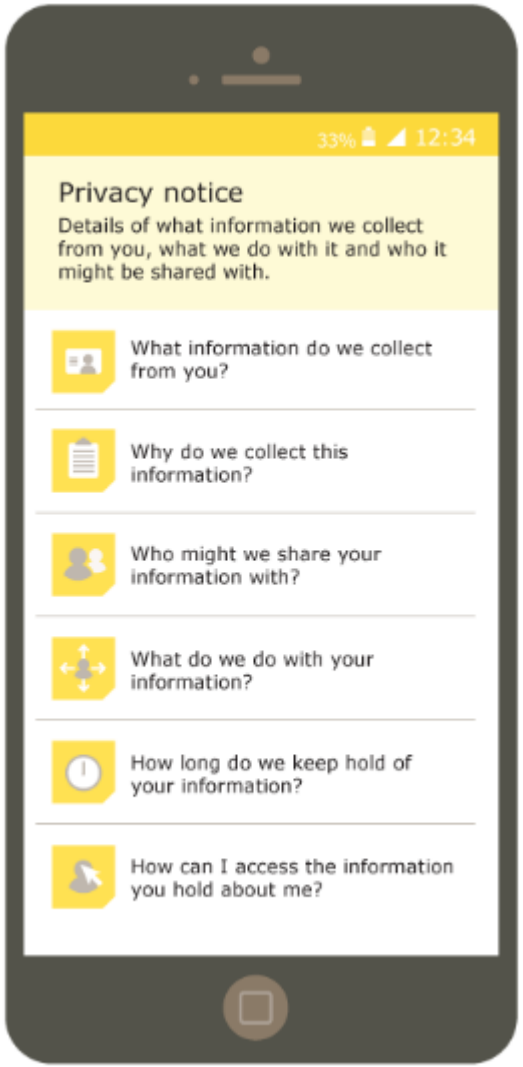

Ad preferences

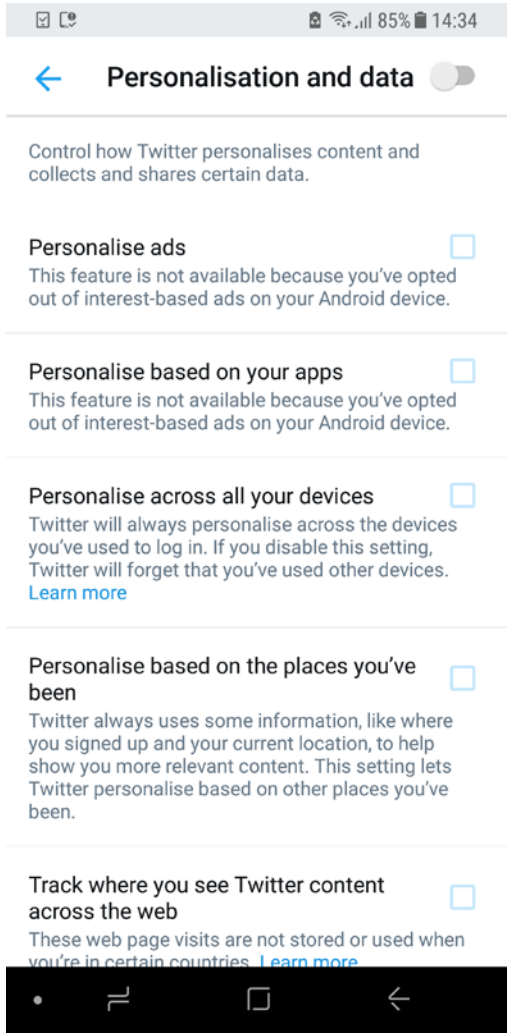

Privacy preferences


Download my data

UX and design

Mobile and responsive

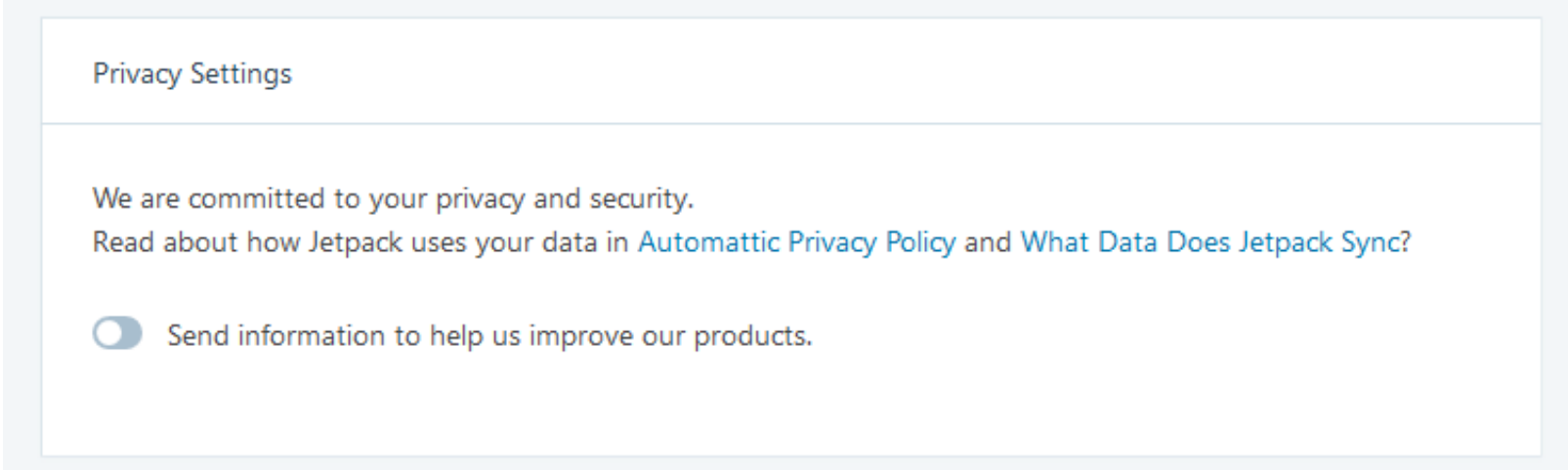




UX and design

Choices and options

Unbundled granularity



*Remember that under GDPR these privacy options must be **off by default**. The user must actively **opt-in**.

What if I don’t include one?

What if I don't include one?

- Lack of trust at best –
  a perception of dishonesty at worst
- Contractual issues with suppliers
- European users can raise a case with their data protection authority (ICO, etc)

What is WordPress doing to help me?

GDPR core compliance project

- Enhancing privacy standards in core
- Examining the plugin developer guidelines with privacy in mind
- Creating documentation focused on best practices in online privacy
- **Adding tools which will allow site administrators to create user-friendly privacy notices**

Trac tickets

- 43389 - Add a privacy policy page setting to options-reading.php
- 43435 - Add settings screen for creating a privacy policy
- 43473 - Add default text for a privacy policy
- **43481 - Privacy policy tools - Admin page UI**
- 43491 - Automatically create a Privacy Policy page when installing WordPress
- 43549 - Add a privacy policy page setting/selector to the customizer
- 43620 - Privacy Policy page design
- 43715 - Popup notification for Privacy Policy page

Building a privacy notice tool

For developers

- Clearer plugin guidelines about privacy for better development practices
- The ability to add privacy information within the plugin repo
- As time goes on, the normalisation of privacy standards disclosure regardless of legal framework

For users

- Built-in functionality to generate a privacy notice page (like About)
- The ability to pull information about data and privacy automatically from plugins
- The ability to generate, review, manually complete, and publish a privacy notice

Questions you need to think about if you develop plugins

- What personal data does this plugin collect?
  (Cookies, telemetry, form entries…)
- Why is that data collected?
  (Consent and legal basis)
- Is data passed to third parties?
  (Social media logins are third parties, and are evil)
- What personal data is stored on the database and remotely?
- What consent mechanisms are provided for users?
- What privacy settings does the plugin administrator have?
- What privacy settings does the user have?
- What data does the plugin transfer outside the EU?

Any advice?

Practical tips

- Privacy notices are living documents. Review and refresh them regularly
- Separate them from Terms and Conditions
- Get your management's buy-in
- Get real people to test your notices
- Privacy notices should supplement user settings, options, and dashboards
- Your online notice is a reflection of your offline business, and privacy notices are just one part of GDPR

Where can I learn more?

- WordPress's privacy resource blog is coming soon
- When in doubt, go with what ICO says (https://ico.org.uk and @iconews)
- CNIL (France) and the Data Protection Commissioner (ROI) also have good advice
- Come to my **three hour** (hooray!) GDPR and privacy workshop at WordCamp Europe

This might just be the healthiest thing you can do for your business this year.

https://webdevlaw.uk
@webdevlaw

WORDCAMP LONDON 2018