Developing for privacy and data protection

Heather Burns // WordCamp Europe // 16 June 2018

What you will learn today

What you will learn today

Theory

- An overview of the changing data protection and privacy landscape
- The different cultural and legal views of privacy within the WordPress project
- How we can create a healthy privacy standard outside legal requirements

Practice

- GDPR: Tools, resources, guidance, code, and a really good test run
- Beyond GDPR: how the WordPress project is working to improve privacy for 31% of the open web
- How you can contribute to privacy in WordPress and in your own work

What you will do with that knowledge

What you will do with that knowledge

- **Shift your thinking** to respect privacy as a positive cultural value, not resent it as a negative legal obligation;
- **Integrate** best privacy practices into your development workflow;
- **Review** your existing work for privacy improvements;
- **Contribute** to WordPress's growing privacy work.

Please welcome my teaching assistants:

Kåre Mulvad Steffensen

Stefan Kremer

Xenos Konstantinos

Rian Kinney

Leo Postovoit

Thanks for the warm-up:

DDD Scotland

PHP Yorkshire

Newcastle WP User Group

Manchester WP User Group

FrontEnd United Utrecht

This workshop was made possible by the

yoast

Yoast Diversity Fund

Theory

An overview of the changing data protection and privacy landscape

Europe's privacy overhaul

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 Directive: TBD (autumn/winter?)
  - Replaces the ePrivacy Directive of 2002
  - Data in transit: cookies, telemetry, advertising beacons, marketing
  - Colloquially and somewhat inaccurately known as the "Cookie Law"

GDPR essentials

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. WordPress 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 identification number (e.g., Social Security number)
- Passport number
- Vehicle registration 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

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

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: Individual rights

- The right to be **informed** about what you are doing with data (privacy notices);
- The right of users to **access** a copy of the data you hold on them;
- The right to **correct** any data that you hold;
- The right to **erasure**, meaning the *right to request* deletion of certain kinds of data you hold (erasure tool);
- The right to **restrict processing**, or the right to ask you to stop using data in certain ways;
- The right to **data portability**, or the right to take the data you hold about them to another service provider (export tool);
- The right to **object** to your uses of their data; and
- Their rights in relation to **automated decision making and profiling**, including data you use or share for advertising, marketing, and behavioural analysis.

GDPR: Consent and legal basis

- In most circumstances, the data collection and processing you perform must be done with the **consent** of the people that data is about.
- If consent is not the basis, your use of data must be grounded in a **legal basis**.
- The consent mechanisms and legal bases you use to collect and process data must be clear, documented, and verifiable.

GDPR: Consent must be

- **Active**: consent is freely given, specific, and unambiguous;
- Active consent is also **positive**, meaning you have not presumed consent from a pre-ticked box, inactivity, or *not* selecting any option;
- Privacy must be presented as **granular** multiple choices, and not a zero-sum in-or-out game.
- **Unbundled:** users cannot be forced to grant consent for one thing in order to receive another;
- **Named:** the user must be made aware of all specific third parties who will be receiving their data and why they will be receiving it;
- **No imbalance in the relationship:** consent must not create an unfair relationship between the user and the data processor;
- **Verifiable and documented:** you must be able to prove who gave their consent, how consent was given, what information they were given, what they agreed to, when they consented, and whether or not the user has withdrawn their consent.

GDPR: Lawful bases for processing data

- Necessary for the **performance of a contract**;
- Necessary to **comply with a legal obligation**;
- Necessary to **protect the person's vital interests** (for example, homelessness help)
- Necessary for **the performance of a task in the public interest** or in the exercise of official authority;
- Necessary for the purposes of the "**legitimate interests**" pursued by the controller or third party.

GDPR: stop abusing legitimate interest

Legitimate interest **is not:**

- Your first option – it should be the last resort
- A "catch all" for things you've decided you want to do without consent but don't know how
- A way to claim consent for data you already collected – **it cannot be applied retrospectively to existing data.**

Who is subject to GDPR and ePD?

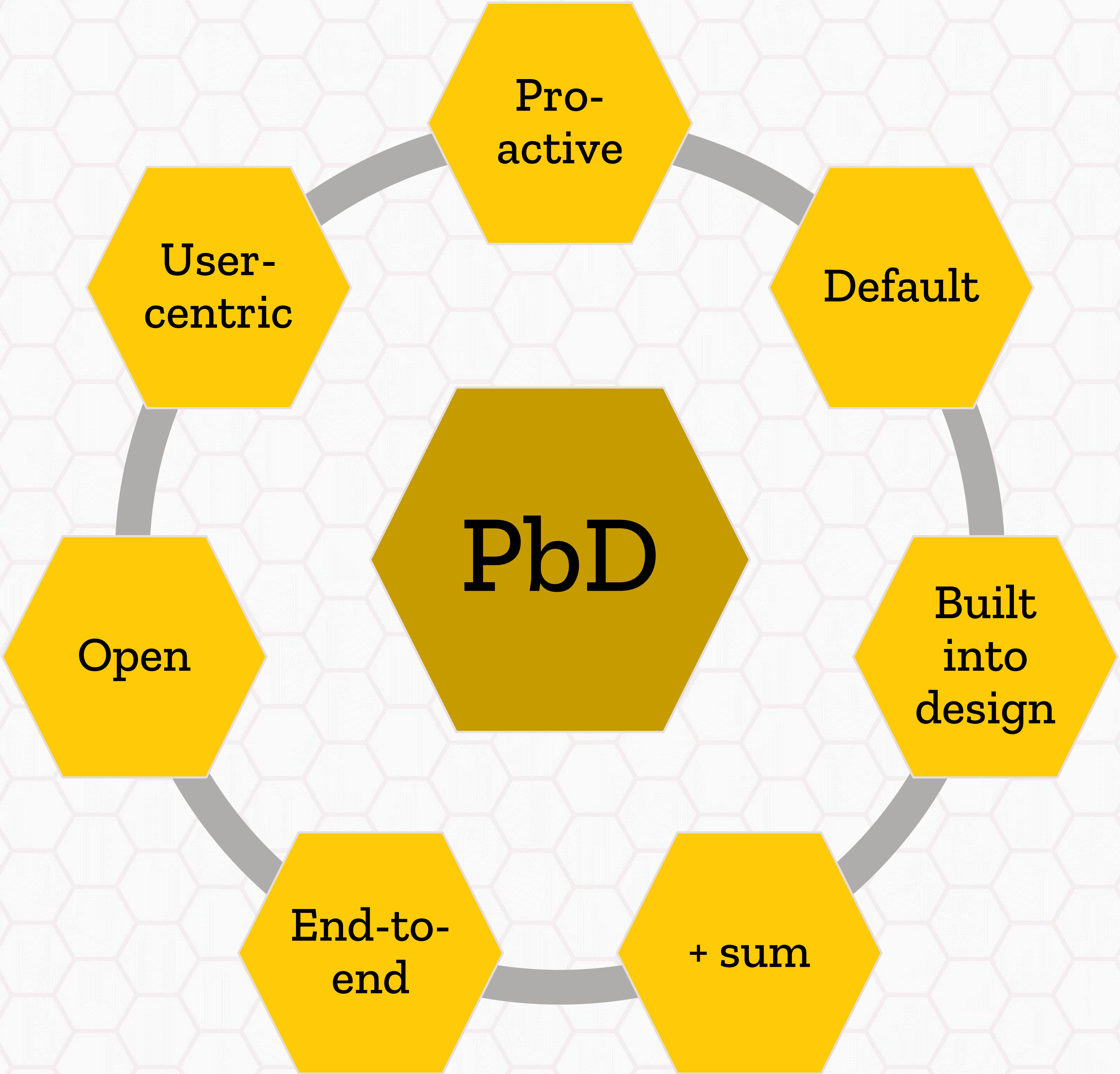
- All data collected, processed, and retained about persons within the European Union
- Extraterritorial: applies to non-EU collection and processing
- All capturing and/or processing of personal data: no minimum size or turnover
- All situations: public sector, private sector, academia, startup, side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

Privacy by Design

What is Privacy by Design?

- Non-regulatory development framework devised in Canada in the 1990s
- Incorporated into GDPR as a requirement
- Review 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 the 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.*

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

Data collection and retention

Subject Access Rights

Legal

Human and technical security

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?

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

America is ready to legislate privacy

- Balancing the Rights Of Web Surfers Equally and Responsibly (BROWSER) Act of 2017
- Secure and Protect Americans' Data Act (SPADA) of 2017
- Internet Bill of Rights of 2018
- FTC Privacy Act changes
- Social Media Privacy and Consumer Rights Act of 2018
- Customer Online Notification for Stopping Edge-provider Network Transgressions (CONSENT) Act of 2018
- Resolution on applying GDPR protections to U.S. citizens

Why does that matter?

Theory

The different cultural and legal views of privacy within the WordPress project

WordPress 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

We also have very different legal approaches to privacy.

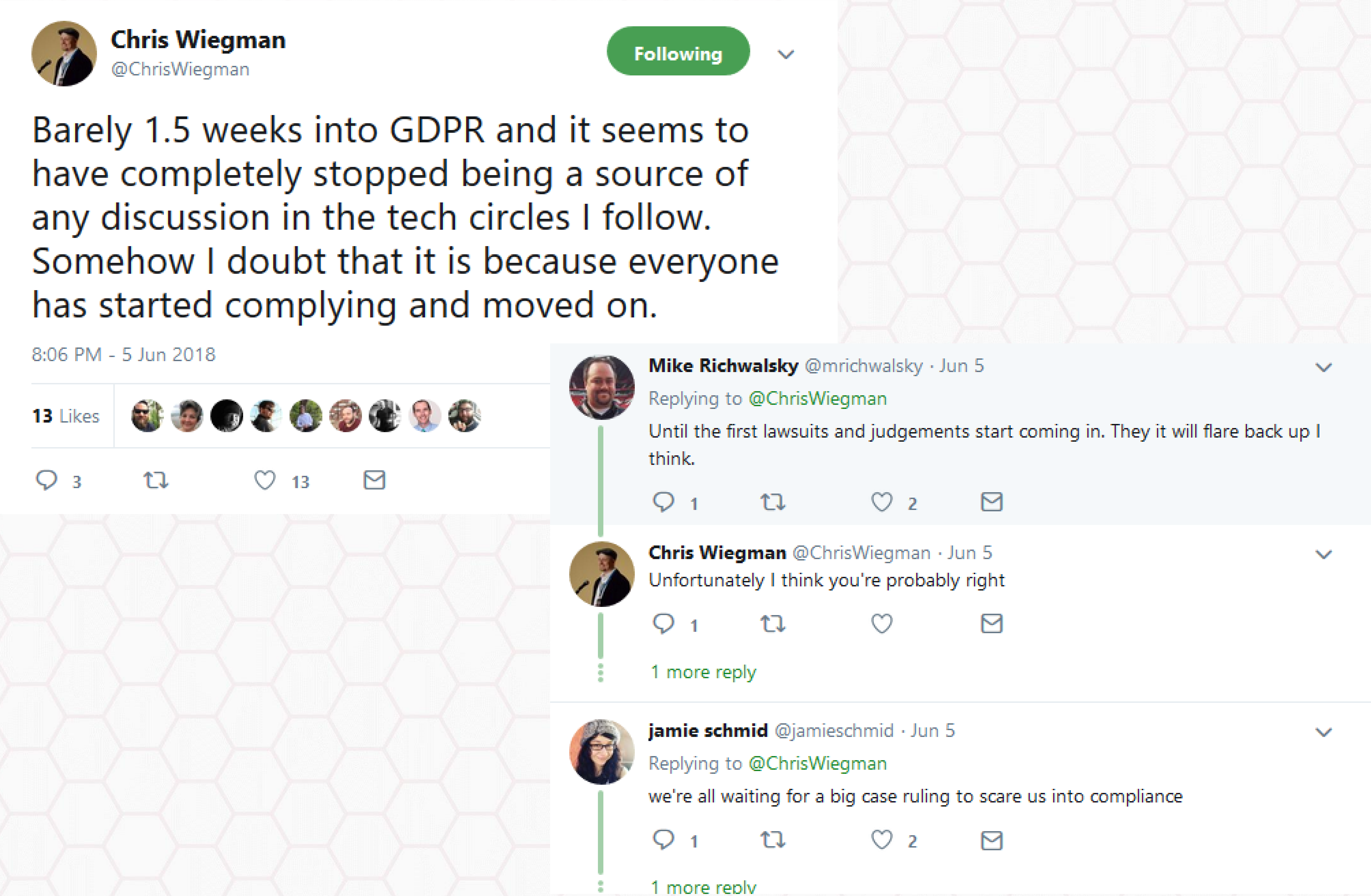
European legal approach to privacy

- 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

Those differences shape our approach to compliance.



Chris Wiegman @ChrisWiegman

Barely 1.5 weeks into GDPR and it seems to have completely stopped being a source of any discussion in the tech circles I follow. Somehow I doubt that it is because everyone has started complying and moved on.

8:06 PM - 5 Jun 2018

Mike Richwalsky @mrichwalsky · Jun 5

Replying to @ChrisWiegman

Until the first lawsuits and judgements start coming in. They it will flare back up I think.

Chris Wiegman @ChrisWiegman · Jun 5

Unfortunately I think you're probably right

1 more reply

jamie schmid @jamieschmid · Jun 5

Replying to @ChrisWiegman

we're all waiting for a big case ruling to scare us into compliance

1 more reply

"Under the GDPR's new tools, we'll be able to use enforcement notices to require companies to delete algorithms or stop processing.

I think orders to stop processing are going to be as powerful, if not more powerful than administrative fines."

-Elizabeth Denham, the UK Information Commissioner,
to the Civil Liberties Committee of the European Union, 4 June 2018

And when it comes to privacy,
we don’t agree to disagree.

Things Europeans say about the American approach to privacy…

"Wild West"

"Even before GDPR starts, they are violating the rules"

"Their tone is still far from acknowledging the serious concerns people have"

"A lack of progress may challenge the effectiveness of self-regulation in this area and may increase the pressure to legislate."

"We thank you for appearing to testify before our committee today"

…and things Americans say about the European approach to privacy

“Jack-booted thugs”

“It could significantly interrupt transatlantic commerce and create unnecessary barriers to trade”

“The European approach runs the risk of being insensitive to context”

“There should be no government involvement”

“I don't understand how we've reached a point where we, in the United States, are reliant on a foreign regulation to protect our data”

We all have a different understanding of "privacy".

...but who are we?

We make the software that runs 31% of the open web.

We are people of enormous power and influence over privacy on the internet.

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

What happens when our differences meet?

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.

The actions we take within the ecosystem, however small, can protect the people in the data from those who would use that data to hurt them.

So we need to shift our thinking.

We need to stop thinking of privacy as a legal problem to run away from, and instead, think of it as a cultural opportunity to embrace.

Theory

How we can create a healthy privacy standard outside legal requirements

What is “privacy” about, as a principle and not as a law?

Two kinds of privacy rules

Hard law and regulation

- GDPR
- CJEU judgements
- COPPA / HIPPA
- ICO / CNIL / FTC / etc

Soft law and regulation

- Industry codes of conduct
- ISO standards
- International conventions
- Frameworks (Privacy by Design)

Hard laws build their foundations
on the standards defined in soft laws.
This is certainly the case for online privacy.

Let's use soft law to define common privacy values.

International privacy frameworks

- OECD Privacy Principles (1980)
- Council of Europe Convention for the Protection of Individuals with Regard to the Processing of Personal Data (1980/two weeks ago 2018)
- ISO/IEC 2001 International Standard on Information Technology / Security Techniques / Privacy Framework (2011)
- APEC Privacy Framework (2005)
- FTC Fair Information Practice Principles (2000)

OECD	COE	ISO	APEC	FIPP
Collection Limitation Principle	Legitimacy of data processing and quality of data	Consent and choice	Preventing harm	Notice/Awareness
Data Quality Principle	Special categories of data	Purpose legitimacy and specification	Notice	Choice/Consent
Purpose Specification Principle	Data security	Collection limitation	Collection limitation	Problems with Choice/Consent
Use Limitation Principle	Transparency of processing	Data minimization	Uses of personal information	Access/Participation
Security Safeguards Principle	Rights of the data subject	Use, retention and disclosure limitation	Choice	Integrity/Security
Openness Principle		Accuracy and quality	Integrity of personal information	Enforcement/Redress
Individual Participation Principle		Openness, transparency and notice	Security safeguards	
Accountability Principle		Individual participation and access	Access and correction	
		Accountability	Accountability	
		Information security		
		Privacy compliance		

OECD	COE	ISO	APEC	FIPP
Collection Limitation Principle	Legitimacy of data processing and quality of data	Consent and choice	Preventing harm	Notice/Awareness
Data Quality Principle	Special categories of data	Purpose legitimacy and specification	Notice	Choice/Consent
Purpose Specification Principle	Data security	Collection limitation	Collection limitation	Problems with Choice/Consent
Use Limitation Principle	Transparency of processing	Data minimization	Uses of personal information	Access/Participation
Security Safeguards Principle	Rights of the data subject	Use, retention and disclosure limitation	Choice	Integrity/Security
Openness Principle		Accuracy and quality	Integrity of personal information	Enforcement/Redress
Individual Participation Principle		Openness, transparency and notice	Security safeguards	
Accountability Principle		Individual participation and access	Access and correction	
		Accountability	Accountability	
		Information security		
		Privacy compliance		

What are common privacy values?

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

- Data minimisation
- User participation and rights
- Data integrity
- Accountability, enforcement, and redress
- Purpose minimisation
- Choice, control, and consent
- Lifecycle limitation
- Special categories of data
- Human and technical security
- Legal compliance
- Transparency and notice

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

Creating and following "soft regulation" principles for user privacy lessens the chances of "hard regulation" being imposed onto your project.

How might we integrate common privacy values into the WordPress project?

Example of principle integration

Transparency and notice

- What is the status of transparency and notice in core?
- Does it need to change?
- What do the development guidelines say about project design and transparency and notice?
- What do the development guidelines say about code and transparency and notice?
- What do we want to achieve?
- When do we want to ship that?
- How do we build in the functionality for transparency and notice?
- What about plugins and themes?
- Who else needs to be involved?

Example of planning and documentation

Transparency and notice

https://developer.wordpress.org/plugins/privacy/

- How does your plugin handle personal data? Use wp_add_privacy_policy_content to disclose to your users any of the following:
- Does the plugin share personal data with third parties (e.g. to outside APIs/servers). If so, what data does it share with which third parties and do they have a published privacy policy you can provide a link to?
- Does the plugin collect personal data? If so, what data and where is it stored? Think about places like user data/meta, options, post meta, custom tables, files, etc.

Example of planning and documentation

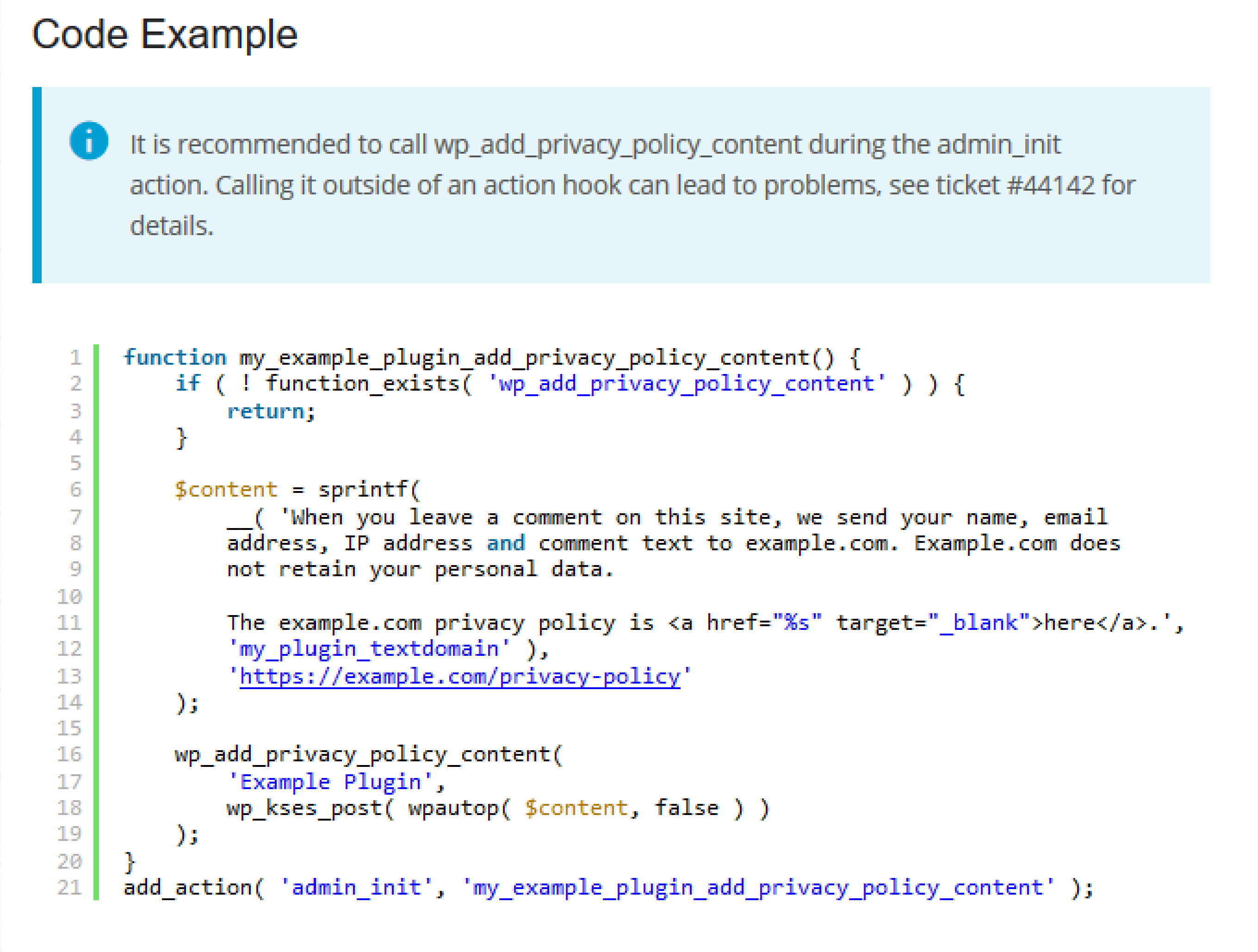
https://developer.wordpress.org/plugins/privacy/

Transparency and notice

- Does the plugin use personal data collected by others? If so, what data? Does the plugin pass personal data to a SDK? What does that SDK do with the data?
- Does the plugin collect telemetry data, directly or indirectly? Loading an image from a third-party source on every install, for example, could indirectly log and track the usage data of all of your plugin installs.
- Does the plugin enqueue Javascript, tracking pixels or embed iframes from a third party (third party JS, tracking pixels and iframes can collect visitor's data/actions, leave cookies, etc.)?
- Does the plugin store things in the browser? If so, where and what? Think about things like cookies, local storage, etc

Example of development guidelines and code sample

Transparency and notice



Code Example

It is recommended to call wp_add_privacy_policy_content during the admin_init action. Calling it outside of an action hook can lead to problems, see ticket #44142 for details.

```
function my_example_plugin_add_privacy_policy_content() {
    if ( ! function_exists( 'wp_add_privacy_policy_content' ) ) {
        return;
    }

    $content = sprintf(
        __( 'When you leave a comment on this site, we send your name, email
        address, IP address and comment text to example.com. Example.com does
        not retain your personal data.

        The example.com privacy policy is <a href="%s" target="_blank">here</a>.',
        'my_plugin_textdomain' ),
        'https://example.com/privacy-policy'
    );

    wp_add_privacy_policy_content(
        'Example Plugin',
        wp_kses_post( wpautop( $content, false ) )
    );
}
add_action( 'admin_init', 'my_example_plugin_add_privacy_policy_content' );
```

Not legal advice

3 down, 8 to go…

11 universal privacy principles

Data minimisation

User participation and rights

Data integrity

Accountability, enforcement, and redress

Purpose minimisation

Choice, control, and consent

Lifecycle limitation

Special categories of data

Human and technical security

Legal compliance

Transparency and notice

Integrating privacy principles

- Define how each privacy principle needs to be adopted
- Amend project guidelines on how work is *structured*
- Amend development guidelines on how work is *coded*
- Provide resources for developers to understand how to use any new functionality
- Provide resources for site administrators to understand why these things matter and what they need to do

Practice

GDPR: tools, resources, guidance, code, and a really good test run

Phase 1

The GDPR compliance project

GDPR core compliance roadmap

- 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

Project constraints

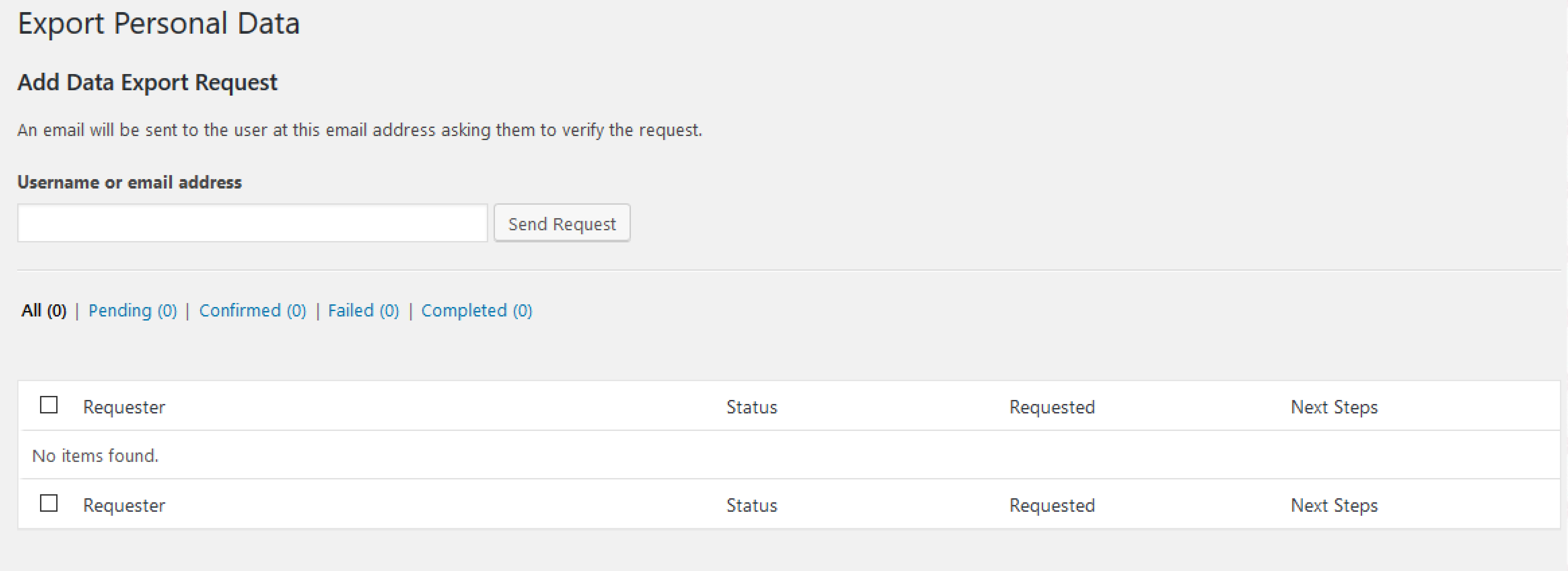
- We cannot make WordPress sites compliant
- No tool achieves compliance in and of itself
- No tool removes the user's responsibility for compliance
- There is no such thing as "compliance", only a journey
- The WordPress project is allergic to anything "legal" – and privacy was seen as a legal (and European) thing
- No open source CMS gave GDPR or privacy proper resourcing

What we did do

1. Add tools to core to allow users to create a privacy notice, export data, and erase data
2. Create plugin functionality and hooks to feed data into those tools
3. Add documentation/help for admins, users, and devs
4. Remove "legal compliance" from plugin guidelines
5. Identify areas for future work outside GDPR

Tools shipped in 4.9.6

GDPR-specific enhancements



Export Personal Data

Add Data Export Request

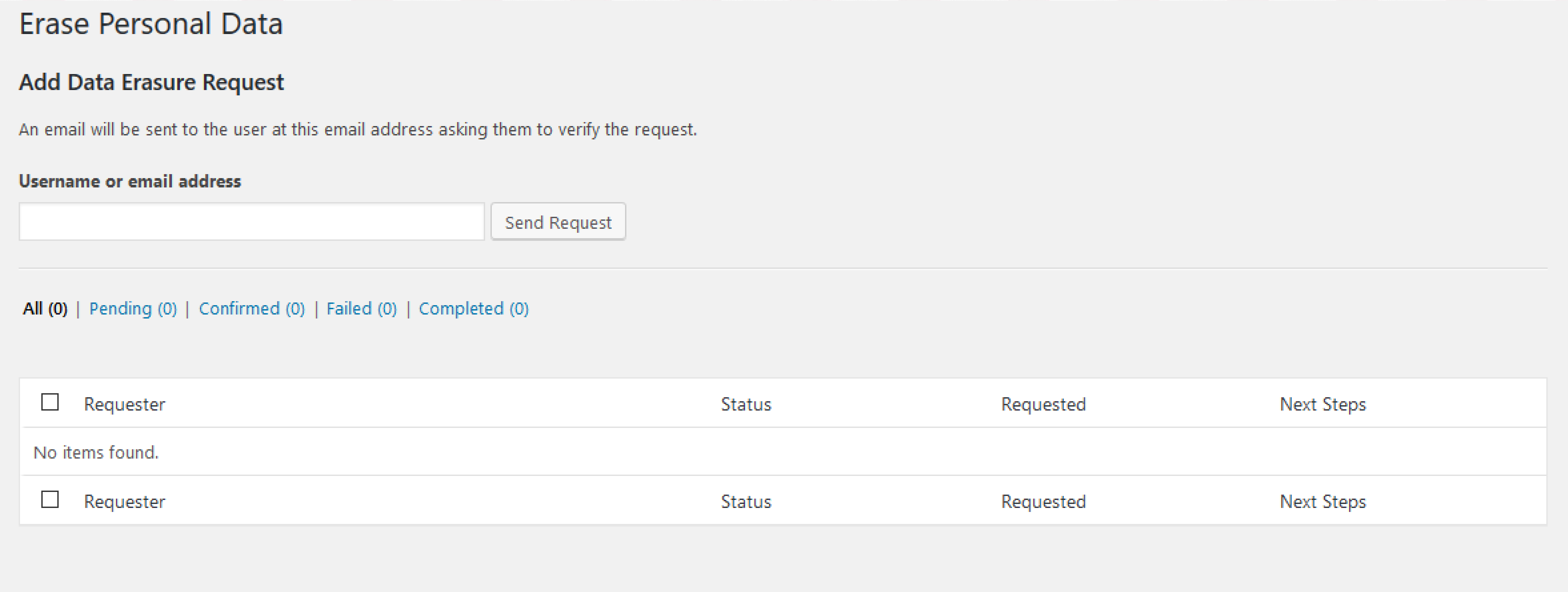
An email will be sent to the user at this email address asking them to verify the request.

Username or email address

Send Request

All (0) | Pending (0) | Confirmed (0) | Failed (0) | Completed (0)

□	Requester	Status	Requested	Next Steps
No items found.				
□	Requester	Status	Requested	Next Steps



Erase Personal Data

Add Data Erasure Request

An email will be sent to the user at this email address asking them to verify the request.

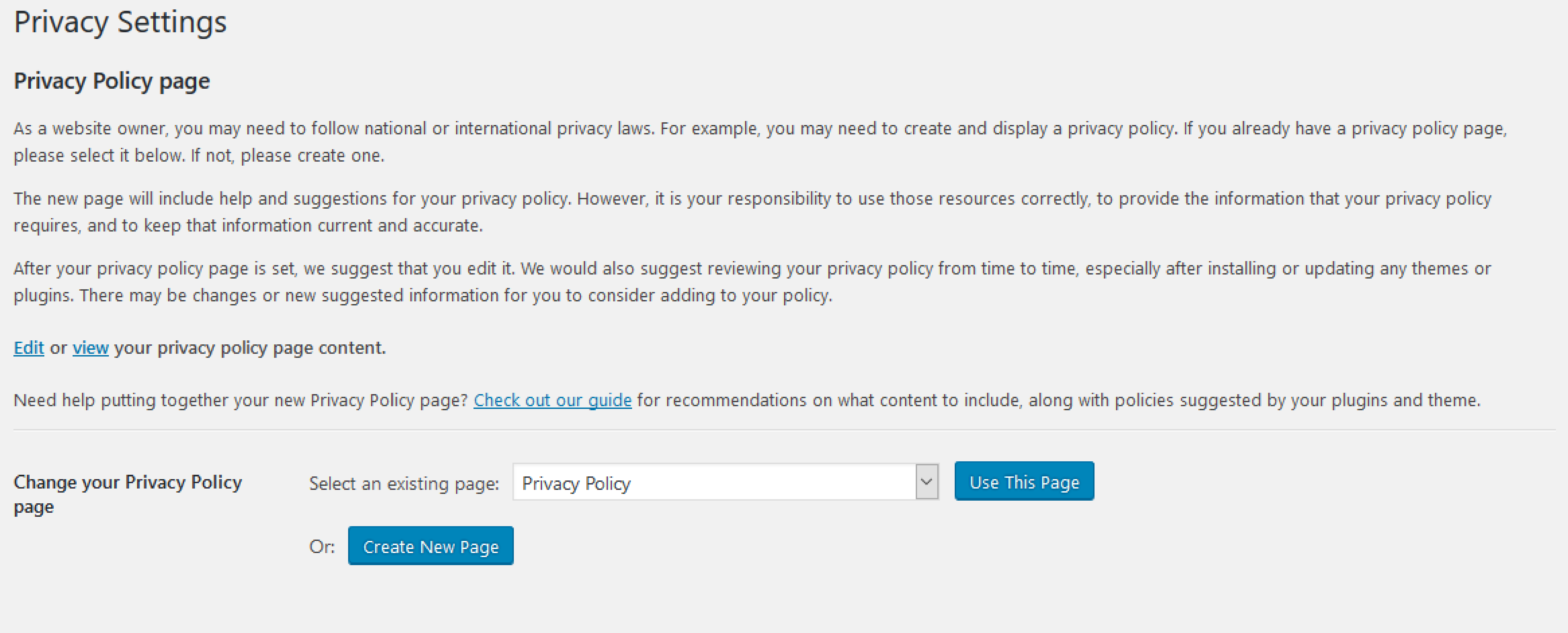
Username or email address

All (0) | Pending (0) | Confirmed (0) | Failed (0) | Completed (0)

□	Requester	Status	Requested	Next Steps
No items found.				
□	Requester	Status	Requested	Next Steps

Privacy notice tool

- Starter for a GDPR-ready privacy notice
- Not a template – headers and prompts are just that
- Functionality to feed info in from plugins and themes
- Admin is responsible for publishing



Privacy Settings

Privacy Policy page

As a website owner, you may need to follow national or international privacy laws. For example, you may need to create and display a privacy policy. If you already have a privacy policy page, please select it below. If not, please create one.

The new page will include help and suggestions for your privacy policy. However, it is your responsibility to use those resources correctly, to provide the information that your privacy policy requires, and to keep that information current and accurate.

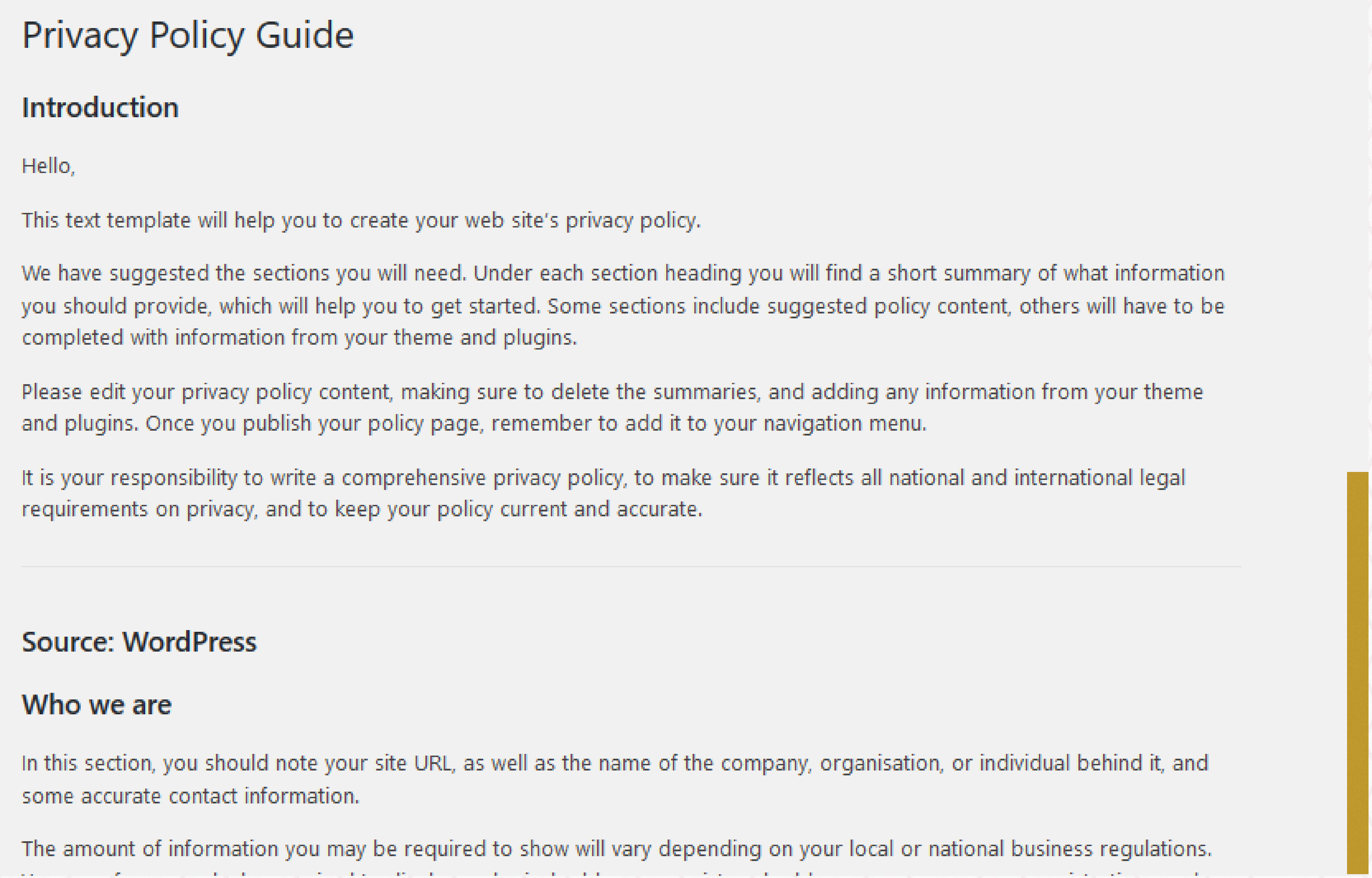
After your privacy policy page is set, we suggest that you edit it. We would also suggest reviewing your privacy policy from time to time, especially after installing or updating any themes or plugins. There may be changes or new suggested information for you to consider adding to your policy.

Edit or view your privacy policy page content.

Need help putting together your new Privacy Policy page? Check out our guide for recommendations on what content to include, along with policies suggested by your plugins and theme.

Change your Privacy Policy page

Select an existing page: Privacy Policy



Privacy Policy Guide

Introduction

Hello,

This text template will help you to create your web site's privacy policy.

We have suggested the sections you will need. Under each section heading you will find a short summary of what information you should provide, which will help you to get started. Some sections include suggested policy content, others will have to be completed with information from your theme and plugins.

Please edit your privacy policy content, making sure to delete the summaries, and adding any information from your theme and plugins. Once you publish your policy page, remember to add it to your navigation menu.

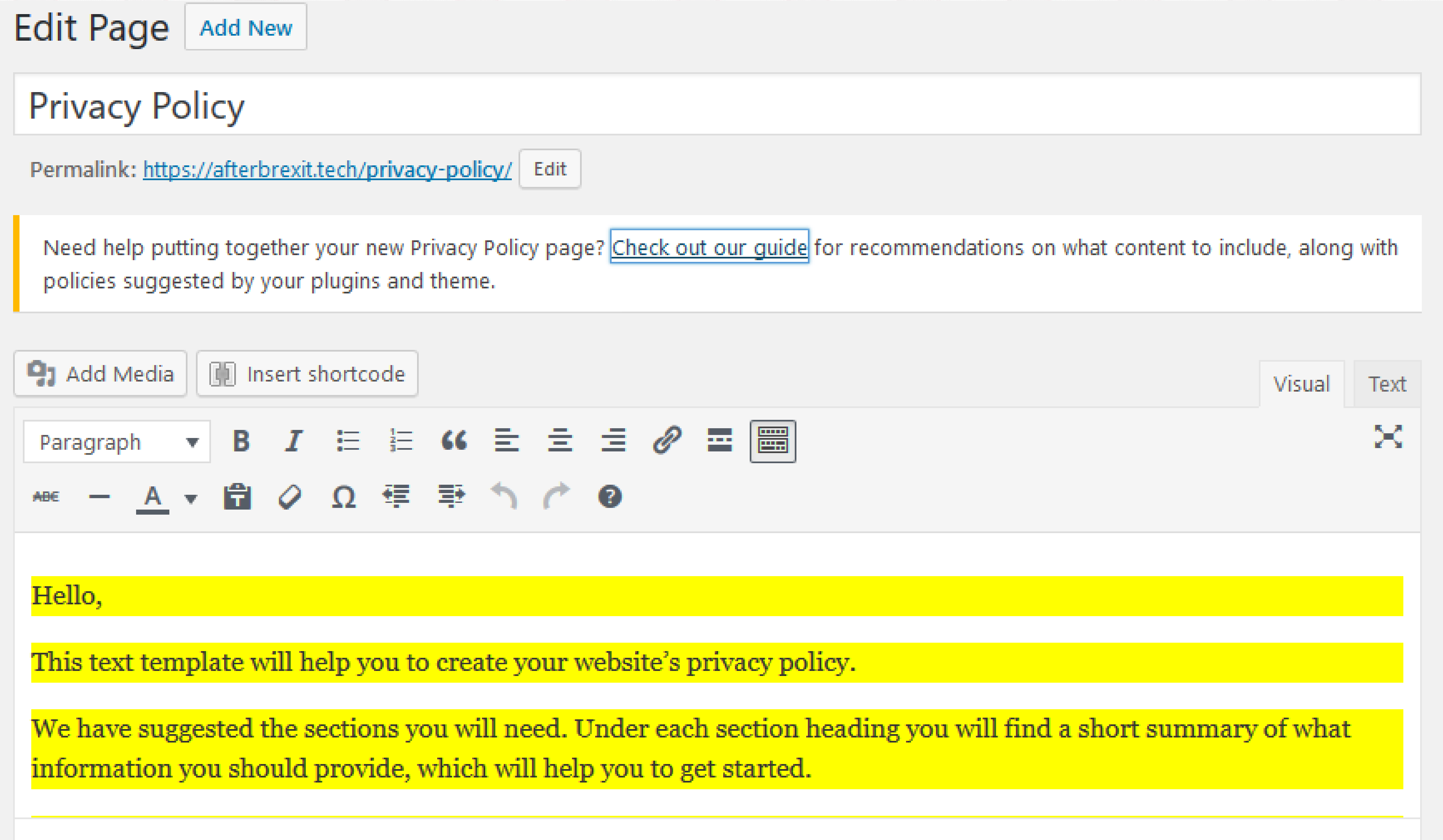
It is your responsibility to write a comprehensive privacy policy, to make sure it reflects all national and international legal requirements on privacy, and to keep your policy current and accurate.

Source: WordPress

Who we are

In this section, you should note your site URL, as well as the name of the company, organisation, or individual behind it, and some accurate contact information.

The amount of information you may be required to show will vary depending on your local or national business regulations.



Privacy Policy

Permalink: https://afterbrexit.tech/privacy-policy/ Edit

Need help putting together your new Privacy Policy page? Check out our guide for recommendations on what content to include, along with policies suggested by your plugins and theme.

Hello,

This text template will help you to create your website's privacy policy.

We have suggested the sections you will need. Under each section heading you will find a short summary of what information you should provide, which will help you to get started.

Functionality and documentation

Developer guidelines

https://developer.wordpress.org/plugins/privacy/

Theory

- What is privacy?
- Privacy by Design
- Food for thought for your plugin

Practice

- Suggesting text for the site privacy policy
- Adding the Personal Data Exporter to Your Plugin
- Adding the Personal Data Eraser to Your Plugin
- Privacy Related Options, Hooks, Filters, and Capabilities

We removed “legal compliance“ from plugin guidelines

...at last

Detailed Plugin Guidelines

https://developer.wordpress.org/plugins/wordpress-org/detailed-plugin-guidelines/

Guideline 9 (*Developers and their plugins must not do anything illegal, dishonest, or morally offensive.*) has been amended to include the following new prohibition:

implying that a plugin can create, provide, automate, or guarantee legal compliance

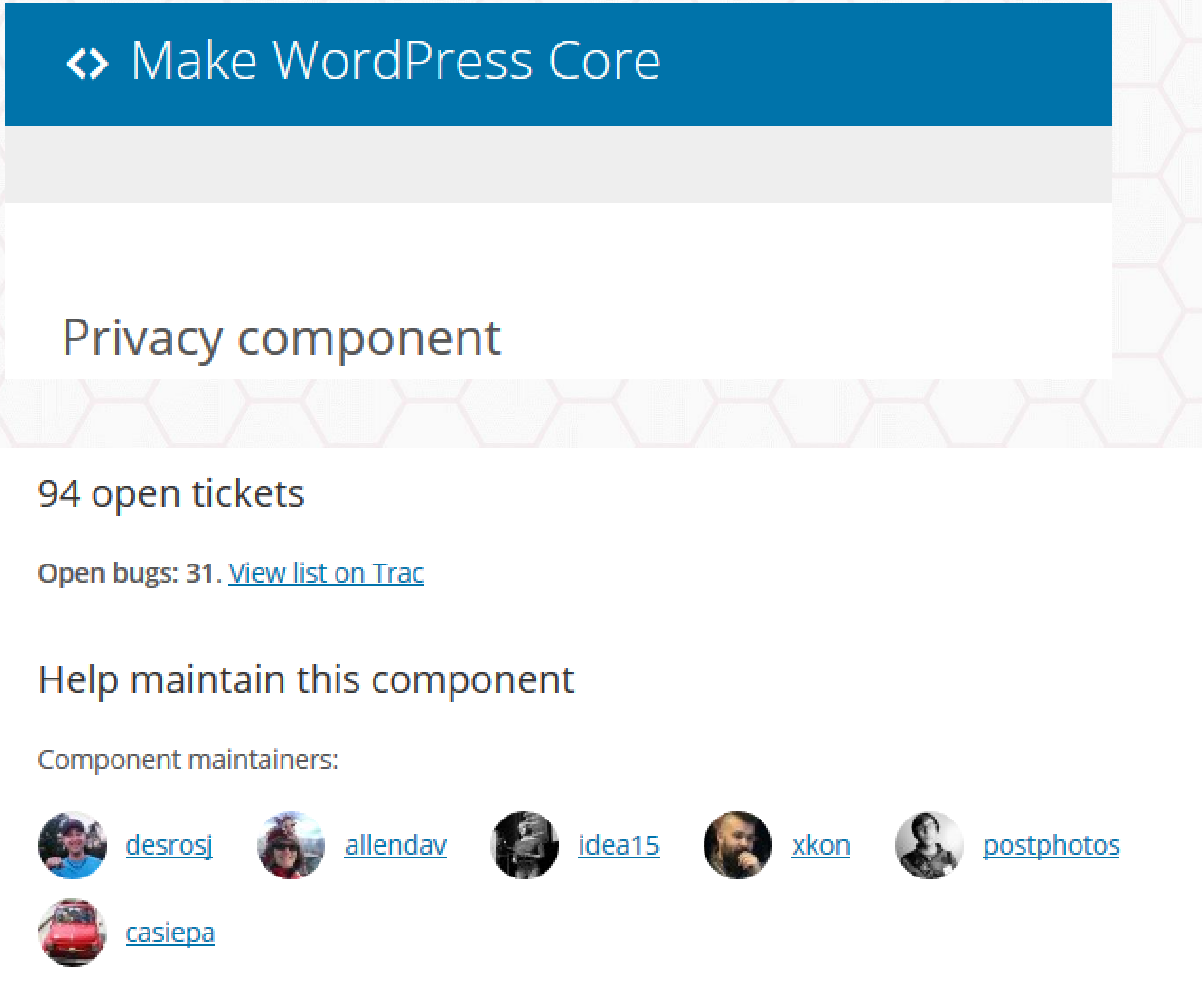
What we didn't do is as important as what we did do.

What we didn’t do

- Scaremonger or threaten
- Discuss penalties, fines, or enforcement – at all
- Make a plugin rather than applying the work to core
- Leave the work with legal
- Try to save the world in one go
- Get the version numbering right

With the test run being over…

We got Privacy established as a permanent core component.



<> Make WordPress Core

Privacy component

94 open tickets

Open bugs: 31. View list on Trac

Help maintain this component

Component maintainers:

desrosj allendav idea15 xkon postphotos casiepa

Practice

Beyond GDPR: how the WordPress project is working to improve privacy for 31% of the open web

Phase 2 roadmap

Core-privacy

1. Core features

Gravatar Improvements

Goal: Give site owners and users greater control over the integration with Gravatar.

Related tickets: #44067, #14682

Embed Controls

Goal: Give site owners control over which embeds are enabled on their site (and thereby allowing site owners the means to limit the cookies and personal data collection embeds sometimes employ.)

Related tickets: #43713, #44001

2. Plugin privacy

Administrators

Should be able to easily determine which plugins
1) do or do not integrate with WordPress privacy tools,
2) provide the level of data privacy control that their site requires or
3) have no privacy impacts on their site at all;

Developers

Would benefit from clearer guidance as they begin to understand what data usage is critical for the functioning of a site or plugin (e.g. authentication) and what data usage the user can and should have control over (e.g. sharing location data);

Users

Should be able to understand the ways a plugin's functionality impacts their privacy during their experience on a site, and, in many cases, to have control, choice, and consent over that data usage. This is key to the work on consent and logging.

3. Consent and logging
(major project)

Goal:

Attempt to come up with a standard way for WordPress and plugins to obtain consent from users and allow users to edit their consent - e.g. through front-side resources;

for WordPress and plugins to store and query consent in a consistent manner;

and for administrators to be able to review a user's consent history and status to help them with compliance inquiries.

(oh, is that all?)

3. Consent and logging
(the big one)

- "Done correctly, a thoughtfully deployed solution for consent across the WordPress ecosystem - drawing as many choices as possible into one central dashboard or settings panel, rather than being scattered across countless places - could greatly enhance user choice over privacy whilst avoiding the "consent fatigue" associated with the first iteration of the ePrivacy Directive.
- Work on consent and logging could involve UX developing a universal pattern library of designs for consent and choice, based on existing pattern libraries developed for IAAP and by IF London."

4, 5, and 6 minor fixes: Erasure and export, i13n, privacy page

- Improve and polish the erasure and export tools added originally in WordPress 4.9.6
  Related trac tickets: 44135, 44265, 44133, 43438, 43437, 44013
- Deploy simple but critical fixes to ensure that privacy-related emails are received in the user's native language
  Related trac tickets: 43985, 44084
- Create Minor UX changes to the privacy notice page within the admin dashboard
  Related trac tickets: 44100, 44131

7. Multisite support

Goal: Extend the tools added originally in WordPress 4.9.6 in a thoughtful manner to a wide variety of multisite/network setups, taking careful consideration of the various needs of the different purposes and sizes of networks out there.

- *Related trac tickets: 43738, 43821, 43822*

Practice

How you can contribute to privacy in WordPress and in your own work

#core-privacy: where and when

- Office hours are 1500 UTC on Wednesdays in Making WordPress Slack
- Bug scrubs are Mondays at 1500 UTC
- https://github.com/wordpress-privacy/
- https://make.wordpress.org/core/components/privacy/
- https://make.wordpress.org/core/roadmap/privacy
- https://developer.wordpress.org/plugins/privacy/
- https://core.trac.wordpress.org/query?status=!closed&component=Privacy

#core-privacy: what and how

Roadmap areas of work:

1. Core features
2. Plugin privacy
3. **Consent and logging**
4. Erasure and export
5. Internationalisation
6. Privacy page
7. Multisite support

- 4.9.7
- 4.9.8 ...?
- 4.9.9 ...?
- Consent and logging will be a major focus

Where to start?

- Review your data capture, sharing, flows, and retention
- Conduct a Privacy Impact Assessment
- Read up on GDPR, PBD, and the open source standard idea
- Explore the 4.9.6 privacy tools, and help us create new ones
- Become privacy champions in your workplaces
- **Demonstrate leadership in privacy within the ecosystem**

What have you learned today?

By now I hope you know how to

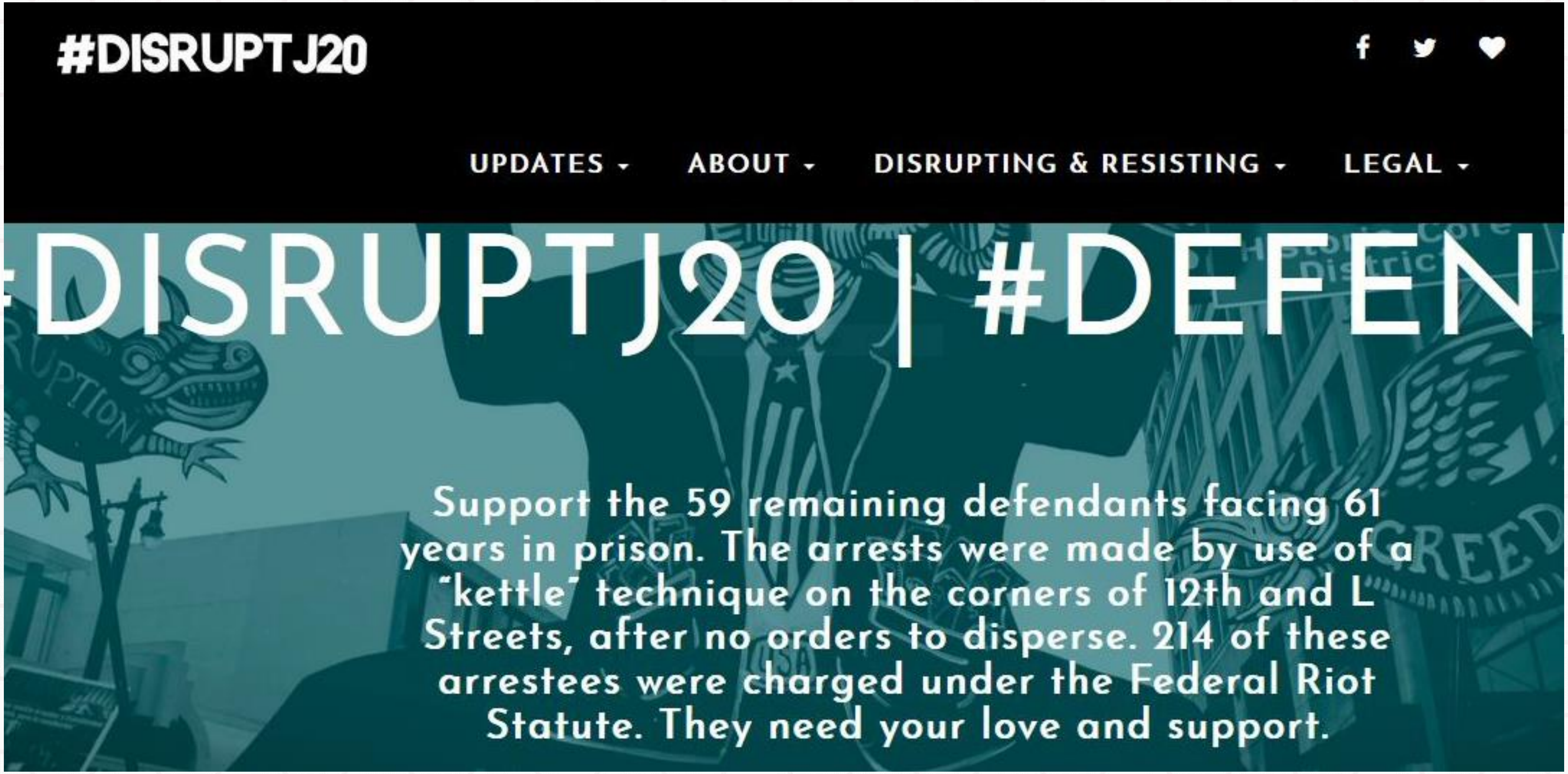
- **respect** privacy as a positive cultural value, rather than resent it as a negative legal obligation;
- **integrate** best privacy practice into your development workflow;
- make a plan to **review** your existing work for privacy improvements;
- **contribute** to WordPress's privacy work.

The most important thing to remember about developing for privacy and data protection

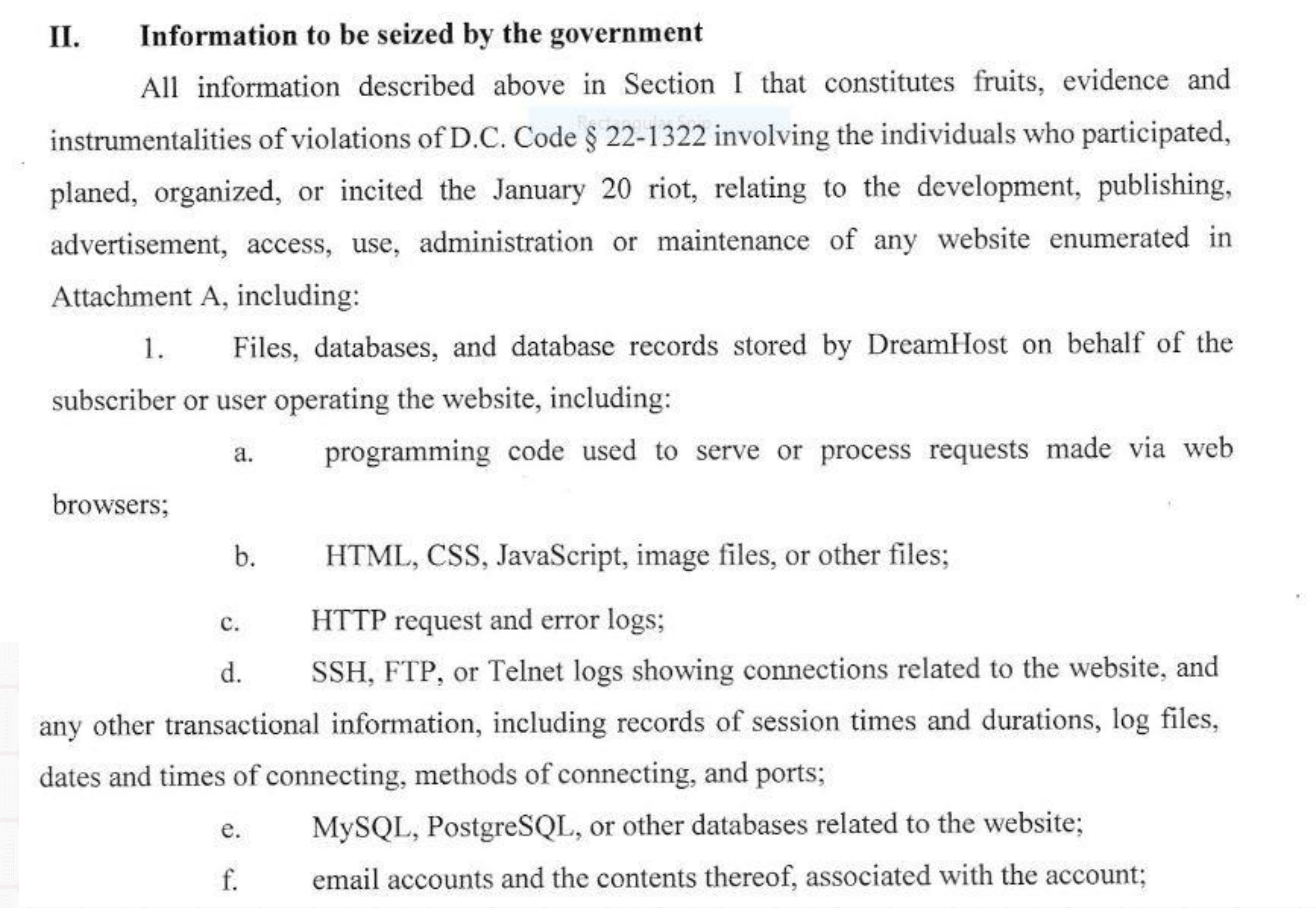
What do these cities have in common?

- Belgrade
- Paris
- Vienna
- Seville
- Sofia
- Leiden

Every WordCamp Europe host city has experienced civil war, fascism, totalitarianism, or the genocide within the last century.



Support the 59 remaining defendants facing 61 years in prison. The arrests were made by use of a "kettle" technique on the corners of 12th and L Streets, after no orders to disperse. 214 of these arrestees were charged under the Federal Riot Statute. They need your love and support.



II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of D.C. Code § 22-1322 involving the individuals who participated, planed, organized, or incited the January 20 riot, relating to the development, publishing, advertisement, access, use, administration or maintenance of any website enumerated in Attachment A, including:

1. Files, databases, and database records stored by DreamHost on behalf of the subscriber or user operating the website, including:

a. programming code used to serve or process requests made via web browsers;

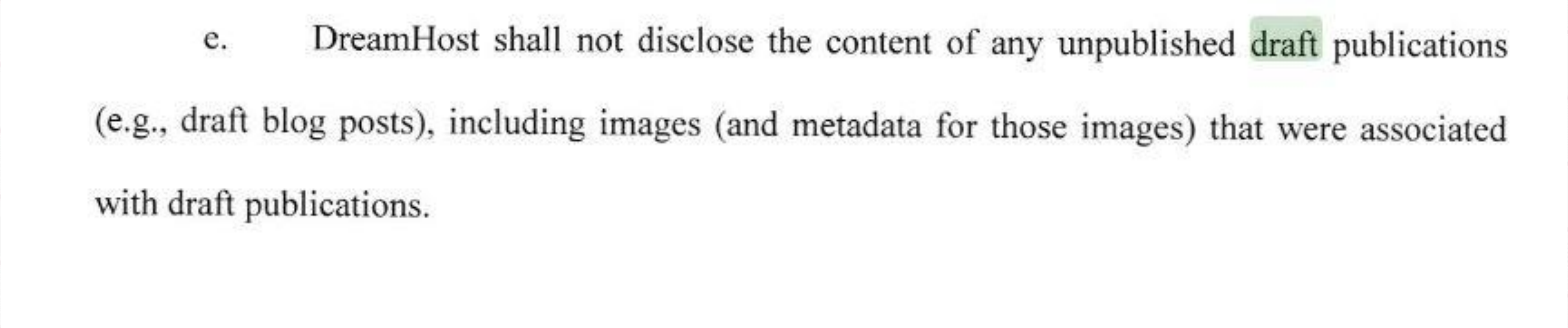
b. HTML, CSS, JavaScript, image files, or other files;

c. HTTP request and error logs;

d. SSH, FTP, or Telnet logs showing connections related to the website, and any other transactional information, including records of session times and durations, log files, dates and times of connecting, methods of connecting, and ports;

e. MySQL, PostgreSQL, or other databases related to the website;

f. email accounts and the contents thereof, associated with the account;



e. DreamHost shall not disclose the content of any unpublished draft publications (e.g., draft blog posts), including images (and metadata for those images) that were associated with draft publications.

We make the software that runs 31% of the open web.

We are people of enormous power and influence over privacy on the internet.

The actions we take within the ecosystem, however small, can protect the people in the data from those who would use that data to hurt them.

Let's make WordPress the most privacy-conscious open-source project in the world.

Thank you for coming today.
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/