



FRONTEND UNITED

KEYNOTE

Privacy, data protection, and open
source development

Heather Burns

UTRECHT
31 May - 2 June 2018

Today we're going to talk about

The different ways we view online privacy



Why this matters for us in open source



How to bridge these divides in our work

Who am I?

(possibly a bad question for 9 AM on a Saturday morning)

- Glasgow, Scotland
- Designed my first web site in 1997
- Professional web designer from 2007-2015
- Now work exclusively in digital law and tech policy
- Exhaustive/exhausting work on GDPR in the two year leadup
- Not a lawyer!

The background of the image is a repeating pattern of blue floral and geometric motifs on a white background. The pattern consists of stylized flowers, leaves, and geometric shapes arranged in a grid-like fashion. A solid black horizontal bar is positioned across the middle of the image, serving as a background for the text.

**Privacy is changing,
and so are we.**

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

America is waking up

Balancing the Rights Of Web Surfers Equally and Responsibly (BROWSER) Act of 2017

Social Media Privacy and Consumer Rights Act of 2018

Secure and Protect Americans' Data Act (SPADA) of 2017

Customer Online Notification for Stopping Edge-provider Network Transgressions (CONSENT) Act of 2018

Internet Bill of Rights of 2018

The image features a repeating blue floral pattern on a white background, which is partially obscured by a solid black horizontal band. The pattern consists of intricate, symmetrical designs with floral and geometric motifs. The black band is positioned in the center of the image, creating a stark contrast with the white background.

Why does that matter?

The background of the slide is a repeating pattern of blue floral and geometric motifs on a white background. The pattern consists of stylized flowers, leaves, and geometric shapes arranged in a grid-like fashion. A solid black horizontal bar is positioned behind the text.

Because 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 owner
- Opt-out culture
- Culture of adversarial courtroom litigation
- People fear governments and trust businesses

The background of the slide features a repeating blue floral pattern on a white background. The pattern consists of intricate, symmetrical designs with floral and geometric motifs. A solid black horizontal bar is positioned across the middle of the slide, serving as a background for the text.

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

The background of the image is a repeating pattern of blue floral and geometric motifs on a white background. The pattern consists of stylized flowers, leaves, and geometric shapes arranged in a grid-like fashion. A solid black horizontal bar is positioned across the middle of the image, containing the text.

**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

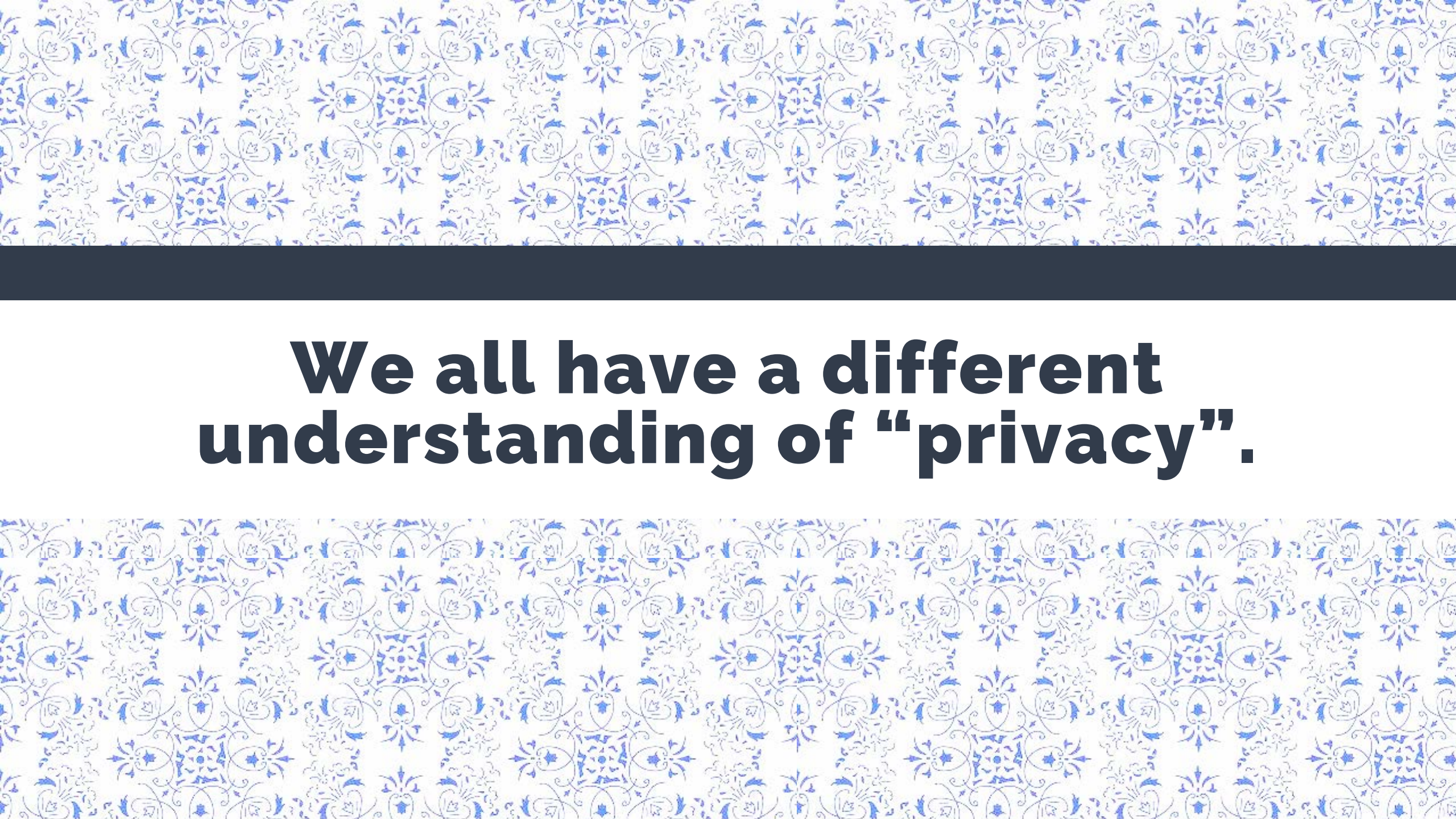
“Jack-booted thugs”

“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”

The background of the slide is a repeating pattern of blue floral and geometric motifs on a white background. The pattern consists of stylized flowers, leaves, and geometric shapes arranged in a grid-like fashion. A solid dark blue horizontal bar is positioned behind the text.

We all have a different understanding of “privacy”.



...and who are we?



**We make the software that
runs the open web.**

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

The image features a repeating blue floral pattern on a white background, which is partially obscured by a solid black horizontal band. The pattern consists of intricate, symmetrical designs with floral and geometric motifs. The black band is positioned in the center of the image, creating a stark contrast with the white background and the blue pattern.

**And we've never acknowledged
our differences.**

What happens when our differences meet?

We structure our projects 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 enough protect the people in the data

We don't learn from our mistakes.

The image features a repeating blue floral pattern on a white background, which is partially obscured by a solid black horizontal band. The pattern consists of intricate, symmetrical designs with floral and geometric motifs. The black band is positioned in the center of the image, creating a stark contrast with the white background and the blue pattern.

That changes today.

**Today we start the journey
to an open source
best practice standard
for privacy.**

The image features a repeating blue floral pattern on a white background, which is partially obscured by a solid black horizontal band. The pattern consists of intricate, symmetrical designs with floral and geometric motifs. The black band is positioned in the middle of the image, creating a central white space where the text is located.

But how do we do that?

What you need to have

Definitions and principles

Documentation and resources

Leadership

Community

The background of the slide is a repeating pattern of blue floral and geometric motifs on a white background. The pattern consists of stylized flowers, leaves, and geometric shapes arranged in a grid-like fashion.

Definitions and principles

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

Two kinds of privacy rules

Hard law and regulation

- GDPR
- the ePrivacy Directive
- COPPA / HIPPA
- Autoriteit Persoonsgegevens

Soft law and regulation

- Industry codes of conduct
- ISO standards
- International conventions
- Frameworks (PbD)

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

The background of the slide is a repeating pattern of blue floral and geometric motifs on a white background. The pattern consists of stylized flowers, leaves, and geometric shapes arranged in a grid-like fashion.

Definitions and principles

**Let's use soft law to identify
common privacy values.**

International privacy frameworks

1. OECD Privacy Principles (1980)
2. Council of Europe Convention for the Protection of Individuals with Regard to the Processing of Personal Data (1980/two weeks ago 2018)
3. ISO/IEC 2001 International Standard on Information Technology / Security Techniques / Privacy Framework (2011)
4. APEC Privacy Framework (2005)
5. 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		

The background of the slide is a repeating blue floral pattern on a white background. The pattern consists of intricate, symmetrical designs with floral and geometric motifs. A solid dark grey horizontal bar is positioned across the middle of the slide, containing the text "Standards and definitions".

Standards and definitions

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

Data integrity

Purpose
minimisation

Lifecycle
limitation

Human and
technical
security

Transparency
and notice

User
participation
and rights

Accountability,
enforcement,
and redress

Choice, control,
and consent

Special
categories of
data

Legal
compliance

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

The background of the slide features a repeating pattern of intricate blue floral and geometric designs on a white background. The pattern consists of stylized flowers, leaves, and geometric shapes arranged in a grid-like fashion.

Documentation and resources

Map your privacy principles to your development workflows

Documentation and resources

- Define how each privacy principle fits into your project
- Amend your project guidelines on how work is *structured*
- Amend your 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

Example of principle identification: data minimisation

Data
minimisation

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

Example of project guidelines planning : Food for thought for WordPress plugins

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

- Does the plugin use error logging? Does it avoid logging personal data if possible? Could you use things like `wp_privacy_anonymize_data` to minimize the personal data logged? How long are log entries kept? Who has access to them?
- In wp-admin, what role/capabilities are required to access/see personal data? Are they sufficient?
- How does your plugin handle personal data? Use `wp_add_privacy_policy_content` (link) to disclose to your users any of the following...

Example of development guidelines: WordPress privacy notice tool

Code Example

i 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.

```
1 function my_example_plugin_add_privacy_policy_content() {
2     if ( ! function_exists( 'wp_add_privacy_policy_content' ) ) {
3         return;
4     }
5
6     $content = sprintf(
7         __( 'When you leave a comment on this site, we send your name, email
8         address, IP address and comment text to example.com. Example.com does
9         not retain your personal data.'
10
11         The example.com privacy policy is <a href="%s" target="_blank">here</a>.',
12         'my_plugin_textdomain' ),
13         'https://example.com/privacv-policv'
```

[Expand full source code](#)

The background of the slide is a repeating pattern of blue floral and geometric motifs on a white background. The pattern consists of stylized flowers, leaves, and geometric shapes arranged in a grid-like fashion. A solid dark grey horizontal bar is positioned across the middle of the slide, containing the word "Leadership" in white text.

Leadership

Privacy is everyone's job

Leadership

- Identify privacy champions within your project
- Involve a variety of roles and backgrounds – development, UX, marketing, policy, and yes, legal...
- But do not view privacy as a legal obligation
- Don't leave it with lawyers – and don't expect them to know anything either
- Support and educate, don't lecture and preach ... and don't “privacy shame”
- Respect differing views and find a compromise
- Provide the project with the resources it needs

“Data protection is important, but so is a decentralized, social web. These conversations, and the innovation that hopefully results from it, are important.

If we fail to make the Open Web compliant with data regulations, we could empower walled gardens and stifle innovation towards a more decentralized web.”

<https://dri.es/the-data-protection-challenges-of-a-decentralized-social-web>

The background of the slide is a repeating pattern of blue floral and geometric motifs on a white background. The pattern consists of stylized flowers, leaves, and geometric shapes arranged in a grid-like fashion. A solid dark grey horizontal bar is positioned across the middle of the slide, containing the word "Community" in white text.

Community

Support, empower, and inspire

Community

- Make privacy (*not* legal compliance) the focus
- Communicate, clarify, and create
- Encourage privacy talks at conferences, and work on contributor days
- Qualify your participants
- Be clear on the project goals
- Be clear on the project constraints
- Be clear on the scope of work – it's OK to tell people to hold ideas for a future release

The background of the slide is a repeating pattern of blue floral and geometric motifs on a white background. The pattern consists of stylized flowers, leaves, and geometric shapes arranged in a grid-like fashion.

Community

Case study: the WordPress GDPR project

Identify your goals

“We cannot make WordPress sites compliant, but we can provide site administrators and users with the tools they need to help them bring their sites into healthy compliance.

This project works towards the 25 May 2018 deadline, and the constraints and expectations, of GDPR.

It does, however, take a wider view of online privacy in general, and considers privacy and data protection issues outside GDPR's explicit scope, for future work.”

Identify your 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 best practice journey

Identify your scope of work (v1)

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 the scope of GDPR

Identify your scope of work (v1)

What we didn't do:

1. Scaremonger or threaten
2. Discuss penalties, fines, or enforcement – at all
3. Make a plugin (module)
4. Leave the work with legal
5. Try to save the world in one go
6. Get the version numbering right

GDPR ≠ privacy

- The GDPR Compliance group now continues work as a permanent privacy core group at <https://make.wordpress.org/core/components/privacy>
<https://developer.wordpress.org/plugins/privacy/>
- Roadmaps for V2, V3 in progress
- I'm running a workshop at WordCamp Europe on developing for privacy and data protection which will bring it all together

The image features a repeating blue floral pattern on a white background, which is visible at the top and bottom edges. A solid black horizontal bar spans the width of the image, serving as a background for the text.

That was the easy part.

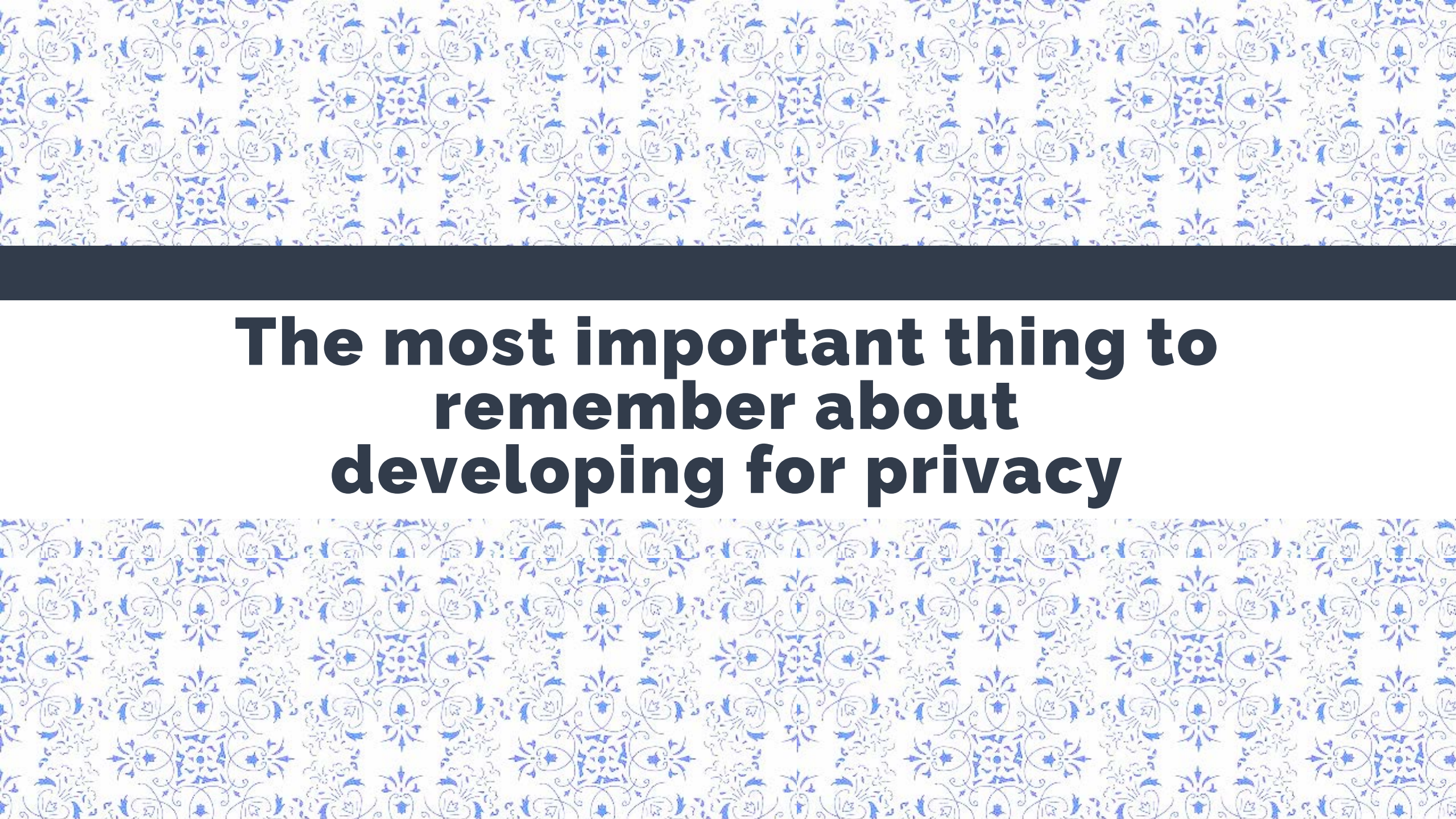
What you've learned

How to define privacy as a principle

How to provide support and resources

How to provide leadership across the project

How to involve the community

The background of the slide is a repeating pattern of blue floral and geometric motifs on a white background. The pattern consists of stylized flowers, leaves, and geometric shapes arranged in a grid-like fashion. A solid black horizontal bar is positioned behind the text, providing a high-contrast background for the white text.

**The most important thing to
remember about
developing for privacy**

**Thank you, and
let's get to work.**

@webdevlaw

<https://webdevlaw.uk>