Authentication and Authorization in PHP

THE IMPACT OF PRIVACY LEGISLATION

Matthew Setter
PHP SECURITY ENGINEER

@settermjd matthewsetter.com

Module Overview

- Introduction to privacy legislation
- Impact on data stored in applications
- Introduction to:
  - The General Data Protection Regulation
  - The California Consumer Privacy Act
  - The Australian Privacy Act

Why Cover Privacy Legislation?

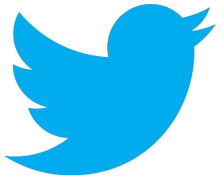
Module Overview

- What they cover
- What you must be aware of
- What the implications are
- Reconsider your attitude to data collection

Where Has Online Privacy Legislation Come From?

The Data Economy

Big Tech



“Google services on Android devices and iPhones store your location data even—if you use a privacy setting preventing Google from doing so”

Associated Press

“Facebook still collects data on you —even when you’re logged out”

David Baser, Facebook Product Management Director

“Twitter also uses cookies dropped on your system to keep an eye on where you go on the web. As long as there's a *"tweet this"* or *"follow me"* button on the site, Twitter harvests information on where you are.”

LifeHacker

Modern Privacy Legislation

Modern Privacy Legislation

The General Data Protection Regulation

The California Consumer Privacy Act

The Australian Privacy Act

The General Data Protection Regulation

“The GDPR is a regulation in EU law on data protection and privacy in the European Union (EU) and the European Economic Area (EEA).”

Wikipedia - The General Data Protection Regulation (GDPR)

“It also addresses the transfer of personal data outside the EU and EEA areas. The GDPR's primary aim is to **give control** to individuals over **their personal data** and to **simplify** the regulatory environment for international business by **unifying** the regulation within the EU.”

Wikipedia - The General Data Protection Regulation (GDPR)

GDPR Quick Facts

- Originates in the European Convention on Human Rights (1950)

“Everyone has the right to respect for his private and family life, his home and his correspondence.”

Article 8 of the European Convention on Human Rights

GDPR Quick Facts

- Originates in the European Convention on Human Rights (1950)
- The European Data Protection Directive (1995)
- Established minimum EU data privacy and security standards
- GDPR passed into law in 2016
- GDPR enforced from May 25, 2018

If you process the personal data of EU citizens or residents, or you offer goods or services to such people, then the GDPR applies to you — **even if you're not in the EU.**

GDPR Financial Penalties

- The larger of €20 million or 4% of global revenue

GDPR Financial Penalties

- The larger of €20 million or 4% of global revenue **- whichever is higher**

GDPR Financial Penalties

- The larger of €20 million or 4% of global revenue **- whichever is higher**
- People have the right to seek compensation for damages

The California Consumer Privacy Act

“The CCPA is a state statute intended to enhance privacy rights and consumer protection for residents of California, United States.”

Wikipedia - The California Consumer Privacy Act

CCPA Quick Facts

People can:

- Know what personal data is being collected about them
- Know whether their personal data is sold or disclosed and to whom
- Say no to the sale of their personal data

CCPA Quick Facts

People can:

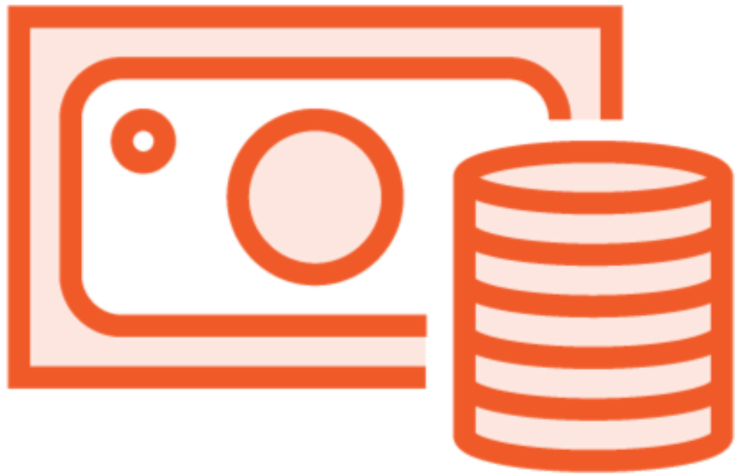
- Access their personal data
- Request a business to delete any personal information
- Not be discriminated against for exercising their privacy rights

CCPA Applies to For-profit Entities

That:

- Collect consumer personal data
- Does business in California

CCPA Applies to for-profit Entities



That satisfy one of:

1. Annual gross revenue > $25 million
2. Buys, receives, or sells personal information of >= 50,000 consumers or households
3. Earns more than half of annual revenue from selling consumers' personal information

The Australian Privacy Act 1998

The Australian Privacy Act 1998

- Established in 1988
- Protects privacy rights of Australian citizens
- Regulates org. use of personal information

Australian Privacy Act 1998

- Gives citizens more control over their data
- Citizens can correct, access, and request personal information
- Applies to:
  - Government agencies
  - Some private organisations
  - Some small businesses

The Australian Privacy Principles

Include guidelines covering:

- Openness and transparency
- Anonymity
- Dealing with solicited and unsolicited personal information

Australian Privacy Principles

- Data collection and disclosure
- Cross-border data disclosure
- Data quality, security, and accessibility
- Correcting personal data

Legislation Summary

- Helps individuals protect their privacy
- Gives users greater control

Legislation Summary

Users must:

- Be informed
- Know what they are consenting to
- Be able to revoke consent

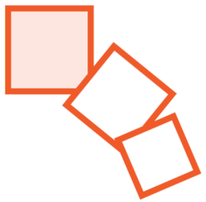
Service cannot be conditional upon consent

What Does It Mean For Developers?

Data Collection Questions

What information was collected when that profile was created?

Why did it ask for these particular pieces of personal information?



Is the data necessary?

Will that information ever be used in your application?

```
[Thu Mar 13 19:04:13 2020] [error] [user: settermjd] Login failed
```

Is Collected Data Personally Identifiable?

Would they be able to identify one or more of your users?

Would they be able to learn something about your users that they didn't know before?

Is there anything incriminating about your users?

What might happen if there was a breach?

Which External Services Do You Use?

Email Service

Database Service

Logging Service

External Services

- What data do they collect?
- Where is your data physically stored?
- Can you access that data when required?
- What are the external privacy policies?
- What are the provider’s privacy policies?
- Is the data outside of your jurisdiction?

What is the Opportunity Cost?

What does it cost:

- To request, validate, and store user data?
- On a daily, weekly, monthly, yearly basis?
- To archive, retrieve and update the data?
- If there is a data breach?

Less Can Be More

Less data can mean:

- Reduced storage and computing costs
- Less code to be written and maintained
- Fewer places where things can go wrong
- Less potential for a data breach

What Should You Do?

Ask yourself:

- What data is being collected?
- Why?
- How will it be used
- Where is it stored?
- How will you respond to a data breach?
- Why do users have their level of access?

How Do You Communicate?

- Do you have a privacy policy?

How Do You Communicate?

- Do you have a privacy policy?
- Who maintains it?
- How do you communicate changes to it?

Communicating Privacy Policy Changes

Hello,

We've made some changes to our Terms of Service and Privacy Policy. The changes will go into effect March 7, 2016. Here's a summary of them:

Mainly, we've simplified some of the language, clarified some points in response to questions from users, and removed some parts that were unnecessary or redundant. The bedrock relationship between you and Medium won't change. You own your content. We won't sell it or your personal information to third parties. We respect Do Not Track. And we make it simple for you to delete your content for good if you want.

Posting content: We've clarified the section about your rights to content you post. If you create something and post it to Medium, you own the rights, as you always have. We might use that content to promote Medium, and we might use it in connection with advertising on Medium. None of this is new. But we've worked to make it clearer.

Deleting content: When you delete a post, or your whole account, it is gone after 14 days (it used to be 30).

Don't break Medium: We've added a section listing some things you can't do with Medium, such as spamming or scraping, manipulating our recommend system, and other ways of interfering with Medium that make the user experience worse.

Communicating Privacy Policy Changes

Ahoy!
Twilio's Terms of Service, Acceptable Use Policy, and Privacy Notice will be updated effective February 1, 2016. You can review updated language here.
Please contact help@twilio.com with any questions.

Quick Recap

- Broad overview of privacy legislation
- What they cover
- What you must be aware of
- What the implications are
- Asked a number of key questions

Privacy Legislation
is **Serious!**