GDPR & FOSS

Marc Jones
CIPP/US, CISSP
Compliance Engineer &
In-House Counsel
marc.jones@civicactions.com

CivicActions

- ➔ Obligatory IANYL* TINLA**
- ➔ Currently Compliance Engineer & In-House Counsel at CivicActions
- ➔ But these are my own views

* I am not your lawyer
** This is not legal advice

Overview

- ➔ GDPR is the new EU privacy law
- ➔ Generally no specific requirements for software developers
- ➔ Presents an oppertunity for FOSS

Why listen to this presentation?

Why Listen to this presentation

1. Why is free software important to you?
   a. Concerned with control
      i. of their own computer
      ii. with other people having control of their computers
      iii. It’s not really about the computer, it is about the data
2. Obsessed with encrypting things
      i. Generally strong supporters of “privacy”

Key documents of FOSS

→ The Free Software Definition

→ Debian Social Contract

→ Open Source Definition

Why listen to this presentation | FOSS developers as civil libertarians

‘To understand the concept, you should think of “free” as in “free speech,” not as in “free beer”.’

“The Free Software Definition,” Free Software Foundation

http://www.gnu.org/philosophy/free-sw.html

Why listen to this presentation | FOSS developers as civil libertarians

0. The freedom to run the program as you wish, for any purpose (freedom 0).

1. The freedom to study how the program works, and change it so it does your computing as you wish (freedom 1). Access to the source code is a precondition for this.

2. The freedom to redistribute copies so you can help your neighbor (freedom 2).

3. The freedom to distribute copies of your modified versions to others (freedom 3). By doing this you can give the whole community a chance to benefit from your changes. Access to the source code is a precondition for this.

“The Free Software Definition,” Free Software Foundation
http://www.gnu.org/philosophy/free-sw.html

Why listen to this presentation | FOSS developers as civil libertarians

0. The freedom to run the program as you wish, for any purpose (freedom 0).

1. The freedom to study how the program works, and change it so it does your computing as you wish (freedom 1). Access to the source code is a precondition for this.

2. The freedom to redistribute copies so you can help your neighbor (freedom 2).

3. The freedom to distribute copies of your modified versions to others (freedom 3). By doing this you can give the whole community a chance to benefit from your changes. Access to the source code is a precondition for this.

"The Free Software Definition," Free Software Foundation
http://www.gnu.org/philosophy/free-sw.html

Why listen to this presentation | FOSS developers as civil libertarians

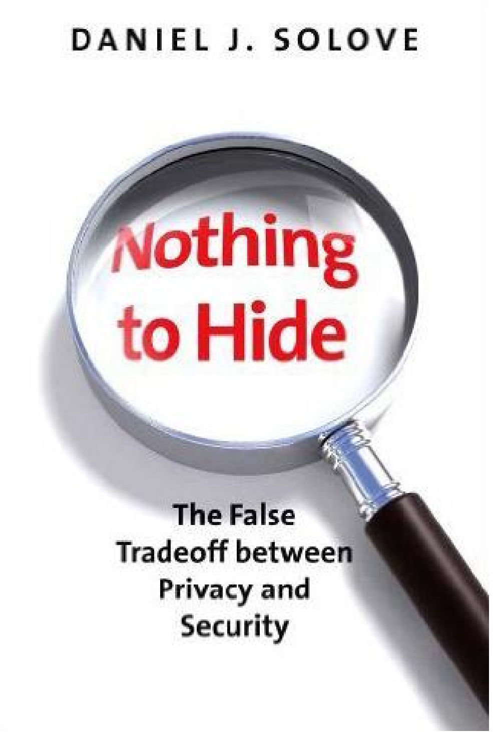
Privacy is more than encryption

➔ Privacy isn't just "[some]*thing To Hide*" argument

➔ It's "*the right to be let alone*"

Why listen to this presentation | FOSS developers as civil libertarians

- Privacy is often viewed just as about hiding wrongs
- Violations of privacy are not just “Orwellien but Kafkaesque.”
- “Violations of privacy affect the power relationships between people and the institutions of the modern state”



DANIEL J. SOLOVE

Nothing to Hide

The False Tradeoff between Privacy and Security

Why listen to this presentation | FOSS developers as civil libertarians

Privacy is more than encryption

➔ Privacy isn’t just “[some*]thing To Hide*” argument

➔ **It’s “*the right to be let alone*”**

Overview of the General Data Protection Regulation (GDPR)?

CivicActions

Overview of the GDPR

1. **What is it?**
2. What does it protect?
3. Who has to follow the rules?
4. Basic rules

Overview of the GDPR | What is it?

- ➔ General Data Protection Regulation
- ➔ Replaces Data Protection Directive (95/46/EC)
- ➔ Effective May 2018
- ➔ Technology Neutral, Risk based approach

Overview of the GDPR | What is it?

- ➔ “lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.” Art. 1 § 1
- ➔ “protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.” Art. 1 § 2

Overview of the GDPR

1. What is it?
2. **What does it protect?**
3. Who has to follow the rules?
4. Basic rules

Overview of the GDPR | What does it protect?

➔ “applies to the processing of personal data wholly or partly by automated means, and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system”

Art.2 § 1

Overview of the GDPR | What does it protect?

Exceptions

- ➔ “by natural persons in the course of a purely personal or household activity” Art 2(2)(c)
- ➔ National security
- ➔ Many parts of law enforcement
- ➔ Matters outside the scope of EU law

Who does it apply to?

➔ Any controller/processor established in the EU

➔ Any controller offering goods or services in the EU

➔ Anyone that EU law applies too

Summary:

➔ GDPR Basically everyone who is processing data on a EU citizen

➔ Unless it is for personal reasons

Overview of the GDPR | Who does it apply to?

Definitions

- ➔ “Controller” - the guy who wanted the data
- ➔ “Processor” - the guy actually holding or manipulating the data
- ➔ “Processing” - doing anything to the data
- ➔ “Data subject” - you (or any other natural person)
- ➔ “Personal data” - any information about a identifiable data subject

Overview of the GDPR | Who does it apply to?

TLDR/Definitions For Lawyers

“'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;”

“'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;”

Overview of the GDPR

1. What is it?
2. What does it protect?
3. Who does it apply to?
4. **Basic rules**

Purposes of the GDPR

- ➔ “Transparency” - processed in a “transparent manner”
- ➔ “Purpose limitation” - collected for a specified legitimate purpose
- ➔ “Data minimization” - adequate, relevant and limited to what is necessary
- ➔ “Accuracy” - keep data up to date; delete or update inaccurate information
- ➔ “Storage limitation”* - retain data only as long as it is necessary to fulfill the original purpose
- ➔ “Integrity and confidentiality” - use “appropriate technical or organizational measures” to protect data

GDPR Art. 5(1)

* Some exceptions for research

Overview of the GDPR | Basics

“Appropriate”

➔ Used at least 80 times in the implementing rules

➔ over 110 times in the entire text

“Reasonable”

➔ Used at least 10 times in the implementing rules

➔ over 23 times in the entire text

Overview of the GDPR | Basics

➔ **Lawyers view of “reasonable” or appropriate**

“Since there are occasions when every vessel will break from her moorings, and since, if she does, she becomes a menace to those about her; the owner’s duty, as in other similar situations, to provide against resulting injuries is a function of three variables: (1) The probability that she will break away; (2) the gravity of the resulting injury, if she does; (3) the burden of adequate precautions. Possibly it serves to bring this notion into relief to state it in algebraic terms: if the probability be called P; the injury, L; and the burden, B; liability depends upon whether B is less than L multiplied by P: i.e., whether B < PL.”

Judge Learned Hand*, United States v. Carroll Towing Co. 159 F.2d 169 (2d. Cir. 1947)

*Coolest name for a judge ever

Overview of the GDPR | Basics

Appropriate measures sometimes include:

➔ **Pseudonymization and encryption of personal data**

➔ **Ensure confidentiality, integrity, and availability**

➔ **Ability to restore access to personal data in a timely manner**

➔ **Process for regularly testing and evaluating the effectiveness of controls for ensuring security**

Art. 32

“The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').” Art 5(2)

Lawfulness of processing must be based on at least 1 of 6 justifications. Art. 6

Two key justifications:

- ➔ Data subject has given consent
- ➔ Performance of a contract data subject is party to

Why we should care?

Overview of the GDPR

1. **Self promotion**
2. Strengthen privacy rights
3. Take advantage of new opportunities

Overview of the GDPR | Basics

- ➔ Data protection/Privacy by design
- ➔ Consent must be affirmative
- ➔ Appropriate technical measures to ensure appropriate security
- ➔ Use encryption when possible
- ➔ Use data pseudonymization when possible
- ➔ Anonymize data when possible
- ➔ Data subjects will be provided with processing steps
- ➔ Data subjects have right to access/review processing of data at any time
- ➔ Combining disparate data could be considered personal data or profiling
- ➔ Data portability
- ➔ Data subjects have right to export data in a commonly used format
- ➔ Data subjects have right to update incorrect data for free
- ➔ Data subjects have a right to data erasure without delay
- ➔ Controllers must notify other data holders of request for erasure
- ➔ Data subjects have a right to object or withdraw consent from processing
- ➔ Data can only be stored for a limited period of time
- ➔ Must be able to identify, track, and assess impact of breaches

Overview of the GDPR | Why We should care about the GDPR?

Self Promotion

- ➔ Many of our users will be subject to the GDPR
- ➔ Our users need to demonstrate compliance with the GDPR
- ➔ Does your project make it hard/easier for them to demonstrate compliance
- ➔ Help companies save money!

Overview of the GDPR

1. Self promotion
2. **Strengthen privacy rights**
3. Take advantage of new opportunities

Overview of the GDPR | Strengthen Privacy Rights

- ➔ **Define "appropriate"**
- ➔ **Raise the bar on what computers can do to protect privacy**
  - ◆ Give users software that respects privacy out of the box
  - ◆ Demonstrate to courts/regulators what is feasible if you are not motivated solely by profit
- ➔ **Create expectations for users that they should have control**

Overview of the GDPR | Strengthen Privacy Rights

➔ Data protection/Privacy by design
➔ Consent must be affirmative
➔ Appropriate technical measures to ensure appropriate security
➔ Use of data must be limited to the purpose for which it is collected
➔ Use encryption when possible
➔ Use data pseudonymization when possible
➔ Anonymize data when possible
➔ Data subjects will be provided with processing steps
➔ Data subjects have right to access/review processing of data at any time
➔ Combining disparate data could be considered personal data or profiling
➔ Data portability
➔ Data subjects have right to export data in a commonly used format
➔ Data subjects have right to update incorrect data for free
➔ Data subjects have a right to data erasure without delay
➔ Controllers must notify other data holders of request for erasure
➔ Data subjects have a right to object or withdraw consent from processing
➔ Data can only be stored for a limited period of time
➔ Must be able to identify, track, and assess impact of breaches

Overview of the GDPR | Strengthen Privacy Rights

➔ Data protection/Privacy by design
➔ Consent must be affirmative
➔ Appropriate technical measures to ensure appropriate security
➔ Use of data must be limited to the purpose for which it is collected
➔ Use encryption when possible
➔ Use data pseudonymization when possible
➔ Anonymize data when possible
➔ Data subjects will be provided with processing steps
➔ Data subjects have right to access/review processing of data at any time
➔ Combining disparate data could be considered personal data or profiling
➔ Data portability
➔ Data subjects have right to export data in a commonly used format
➔ Data subjects have right to update incorrect data for free
➔ Data subjects have a right to data erasure without delay
➔ Controllers must notify other data holders of request for erasure
➔ Data subjects have a right to object or withdraw consent from processing
➔ Data can only be stored for a limited period of time
➔ Must be able to identify, track, and assess impact of breaches

Consent must be affirmative

- ➔ **Mostly applies to user interfaces**
- ➔ **Affirmative consent requires that the data subject take some active step**
  - ◆ Type “I agree” or type <my name> or <my initials>
  - ◆ Checking a box
  - ◆ Clicking a button
- ➔ **Consent must be opting into process**
  - ◆ Do not ask if the person wants to opt out of processing, assume they do
- ➔ **Let users change their mind later and revoke their consent**
- ➔ **Make it obvious when people are consenting, don’t hide it in your default user interface**

Use data pseudonymization/minimization when possible

- ➔ Don’t collect data you don’t actually need
- ➔ Can you allow users to use your software without logging in?
- ➔ Can you allow them use your software without collecting an identifier?
- ➔ Do you need the IP address in your logs?
- ➔ Can you record personal information like IP address in a separate log with a shorter retention period?
- ➔ Can you store account or access control information in a segregated location?

Right to access/review processing of data at any time

- ➔ Track when your data processes personal data
- ➔ Make that log available to users
- ➔ Give users a complete overview of what the software did with their data
- ➔ When was the email sent?
- ➔ Who ran a report that included their personal data?
- ➔ Build in a portal to allow individuals to access their own records in systems that they don’t normally access

Overview of the GDPR | Strengthen Privacy Rights

1. Right to update incorrect data for free
2. Right to data erasure without delay
3. Right to have data stored for a limited period of time

- ➔ Make it easy to update all personal information in your software
- ➔ Don’t make a username or realname a key field for database relationships
- ➔ Test what happens when personal data is deleted?
- ➔ Let users self delete an account!
- ➔ If you need the ability to track account abuse for security, keep the minimum amount of information necessary to record that in a separate location
- ➔ Decide how much data are you going to delete

Overview of the GDPR

1. Self promotion
2. Strengthen privacy rights
3. **Take advantage of new opportunities**

Right to Data portability & Data export to common format

- ➔ Must be able to export personal data into a “commonly used and machine-readable format” Art. 20 (1)
- ➔ Must allow data subjects to move data to other controllers
- ➔ Controllers encouraged to allow the data to be moved *directly* between controllers

➔ Imagine

- Exporting your facebook profile to a Google Buzz
- Exporting your facebook profile to a private Drupal instance
- Exporting your Drupal data to a common format to load into a WordPress instance
- Facebook helping you to create an process to move your data from Facebook to your Diaspora

Thank you.