INF226 – Software Security

Håkon Robbestad Gylterud

2019–10–28

Privacy – a human right?

Article 12 of the Universal Declaration of Human Rights (1948)

*No one shall be subjected to arbitrary interference with his **privacy**, family, home or correspondence, nor to attacks upon his honor and reputation.*

Article 8 of the European Convention on Human Rights (1953)

Right to respect for private and family life:

1. Everyone has the right to **respect for his private and family life**, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Article 8 of the Charter of Fundamental Rights of the European Union (2009)

1. Everyone has the **right to the protection of personal data concerning him or her**.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

Definition

Information privacy refers to the ability of the individual to control their personal information.

Personal information is any information attachable to a specific (physical) person and includes:

- Name and ID number
- Birtdate and gender
- Residence and location
- Healthcare records
- Political information
- Criminal records
- ...

What constitutes threats to privacy

- Collection of information
- Aggregation of information
- Dissemination of information

Collection of information

Many events in our daily lives are recorded in various computer systems:

- Health-care and other public services (Example: NAV)
- School records
- Credit-card usage
- Traveling
- Surveilance cameras
- Internet browsing

Who has access to this information? How de we know these systems are secure?

Aggregation of information

Aggregation means to combine existing data to infer new information:

- Combining different data bases (Example: Credit rating)
- De-anonymisation
- Security breaches
- Using data for a different purpose

Pan-opticlick

Electronic Frontier Foundation has a website to make people aware how unique their browser's fingerprint is:

`https://panopticlick.eff.org/`

Note: A low score (few bits) does not mean that you cannot be tracked: tracking companies have access to more data (writing style, typing speed, click movement and timing, CSS tricks$\cdots$).

Dissemination of information

Spreading personal information:

- Selling personal data to advertisers / credit lenders / employers.
- Exposing emotionally important or taboo information about a subject (life exprience, nudity, private relationships $\cdots$)
- Exposing someone's personal information to encourage harrassment (doxing)

. . . or threatening to do so (blackmail).

Who poses a threat?

- Other individuals
- Companies
- Non-governmental organisations
- Government organisations
- Criminals

The individual

Question

What can the individual do to protect their information privacy?

The privacy paradox

The privacy paradox: Many users say that they value their privacy, but they act in ways which endanger their privacy.

(For instance by sharing a lot of information on Facebook)

The privacy paradox

The privacy paradox: Many users say that they value their privacy, but they act in ways which endanger their privacy.

(For instance by sharing a lot of information on Facebook)

Question

To what extent do you think the following factors contribute to this paradox:

- The users are not aware of the privacy implications of their actions. For instance, because of lack of technical understanding.
- Social pressure to share (impression management).

Software developers & privacy

Question

Think of two examples where software can pose a threat to the privacy of its users.

- What can the software developers do to protect the privacy of their users?

Software developers & privacy

Question

Think of two examples where software can pose a threat to the privacy of its users.

- What can the software developers do to protect the privacy of their users?

Question

Are the developers ethically or legally obliged to implement these protections?

Legal protection

Current law

The currently applicable laws on privacy in Norway/EEA

- EU directive:
  - General Data Protection Regulation (GDPR)
- Norwegian law:
  - Personopplysningsloven av 2018 incorporates GDPR into Norwegian law.
  - Datatilsynet is the Norwegian supervisory authority on privacy issues.

GDPR

General Data Protection Regulation (**GDPR**), is an EU directive which came into effect 25th of May 2018.

Specifies:

- the **rights** of individuals and
- the **obligations** of data processors.

More specific than the 1995 directive it replaces.

Where to find information?

- The GDPR law: while the GDPR is a law text, its language is quite clear.
- Datatilsynet has both explainations of the law, and examples of how this is implemented in specific cases.

Fundamental principles

The fundamental principles for data processing according to GDPR:

- Lawfulness
- Fairness
- Transparency

Terms used: “data subject”, “controller” and “processor”.

Article 6: Lawfulness

Processing shall be lawful only if and to the extent that at least one of the following applies:

1. (· · ·)data subject has given **consent**(· · ·) for specific purposes.
2. processing is **necessary (· · ·) for a contract** to which the **data subject is party** (· · ·)
3. processing is **necessary (· · ·) legal obligation** (· · ·)
4. processing is **necessary (· · ·) to protect (· · ·) vital interests** (· · ·)
5. processing is **necessary (· · ·) for (· · ·) public interest** (· · ·)
6. processing is **necessary (· · ·) for the purpose of legitimate interests** (· · ·) except when overridden by fundamental rights(· · ·)

Article 9: Special categories of data

1. **Processing of personal data** revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation **shall be prohibited**.

2. Is a list of exceptions of this rule (Including when consent is given, medical nescessity and public interests.)

Separating necessary from optional

When processing data, one should separate between:

- Data collected based on optional consent
- Data necessary to provide the given service

Minimise data collection

As developers of software:

- Do not collect data you do not need.
- Keep the data only as log as you need:
  - Example: Delete shipping data once package is shipped.

What constitutes consent?

- Must be demonstratable
- Formulated:
  - in an intelligible and easily accessible form,
  - using clear and plain language.

What constitutes consent?

- Must be demonstratable
- Formulated:
  - in an intelligible and easily accessible form,
  - using clear and plain language.

- Must be specific to each kind of data
- Must be possible to withdraw

What constitutes consent?

- Must be demonstratable
- Formulated:
  - in an intelligible and easily accessible form,
  - using clear and plain language.
- Must be specific to each kind of data
- Must be possible to withdraw
- Not sufficient: Prefilled checkboxes
- Not sufficient: ☐ I agree to the terms.

What constitutes consent?

- Must be demonstratable
- Formulated:
  - in an intelligible and easily accessible form,
  - using clear and plain language.
- Must be specific to each kind of data
- Must be possible to withdraw
- Not sufficient: Prefilled checkboxes
- Not sufficient: ☐ I agree to the terms.

One technical solution: keep separate fields in database, for each consent.

Aquiring consent

As developers of software: Define clearly what kind of data the service collects/aggregates/disseminates.

- Divide into categories.
- Ask for consent for each category upon registration of a user.
- Store the separate consent as fields in database.
- Make an interface for changing consent settings.
- No prefilled checkboxes.

Not enough to have "I accept these terms"...

Fairness

The data processing should not exceed what the data subject can reasonably expect.

- Controllers are obliged to protect the fundamental rights of the data subject.
- Automated decisions should be predictable.

Transparency

Information about what is collected must be clearly stated where the data is collected.

GDPR: Rights of the individual

Rights of the individual

According to GDPR the following are the rights of the data subject:

- Right of access
- Right to rectification
- Right to erasure
- Right to data restriction
- Right to data portability
- Right to object

Right of access (article 15)

The data subject has the right to obtain from the controller:

- Wether data is processed
- The purpose of the processing

Right of access (article 15)

The data subject has the right to obtain from the controller:

- Wether data is processed
- The purpose of the processing

- What kinds of data is collected
- Recipients of data
- Duration of the data collection

Right of access (article 15)

The data subject has the right to obtain from the controller:

- Wether data is processed
- The purpose of the processing

- What kinds of data is collected
- Recipients of data
- Duration of the data collection

- To which extent data can be deleted, rectified or minimised
- To which extent objections can be made'

Right of access (article 15)

The data subject has the right to obtain from the controller:

- Wether data is processed
- The purpose of the processing

- What kinds of data is collected
- Recipients of data
- Duration of the data collection

- To which extent data can be deleted, rectified or minimised
- To which extent objections can be made'

- Logic behind automated decisions

Right to rectification (article 16)

The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her.

Allow editing of profile

As software developers: To provide rectification, allow the users to edit their profile.

- Minimal requirement: Allow user to
  - see the data in their profile.
  - request manual rectification.
- More useful to have a fully automated process.

Example: Deindexing from search engines

Search engines are now obliged to consider requests from individuals to deindex search results on their name.

- Also covers search suggestions (`John Doe criminal`)
- Restricted to search results deemed either:
  - incorrect or
  - irrelevant or
  - burdensome

45% of the requests leads to deindexing (source: Google transparency report).

Right to erasure (article 17)

The data subject can in some circumstances request data to be deleted by the data controller:

- Consent has been withdrawn
- The data is no longer necessary
- Data was collected unlawfully
- Deletion is required by (EU or national) law
- Data subject was a minor and using a social website

“Forget me”

As software developers:

The service should have a method which **takes a UserID and deletes personal data** attached to it.

"Forget me"

As software developers:

The service should have a method which **takes a UserID and deletes personal data** attached to it.

- Easy enough to delete a record in a DB
- More difficult with *foreign keys* to this object.
- Even more difficult with hash-chain/tamper-evident data structures.
- How about restoration from backup?
- Notify third parties of erasure.

Right to data portability (article 20)

- If data was collected based on consent or contract,
- the data subject has the right to receive the information in a:
  - structured,
  - commonly used and
  - machine-readable format
- and have the right to transmit those data to another controller

Export data

As software developers: There should be a button "Export data" which gives the user all the data associated with them.

- Use a standard format: JSON, XML, CSV,$\cdots$

Does not have to be automatic.

See data collected

Similar to export, but is part of the interface displaying the data in a **human readable** way.

Implement pseudonymisation

As software developers:

If you want to do statistical analysis on your users data, consider hashing+salting, or better use a **KDF, on UserID** to **pseudonymise the data** before processing.

- Important if using third-party service for analysis.
- Reversable if you keep the salt.
- Non-reversable if salt is deleted.

Be careful about third part access to data

As software developers:

If third parties get access to data:

- Make sure they comply with GDPR
- Log access (e.g. through APIs)
- Do not give more access than needed
- Coordinate data erasure / processing restriction

Muddiest point

Answer on `mitt.uib.no`.