



Ethics and Digital Technologies: Privacy by design

Karën Fort

karen.fort@sorbonne-universite.fr / <http://karenfort.org>

January 15th, 2019



Sources of inspiration

- ▶ edX MOOC from the University of Michigan (2016): *Data Science Ethics*
- ▶ *Ethical IT Innovation* (2016). S. Spiekermann. CRC Press.
- ▶ *Privacy by Design: the 7 Foundational Principles* (2011). Ann Cavoukian.
- ▶ *OWASP Top 10 Privacy Risks Project*
- ▶ *Engineering Privacy by Design* (2017). Carmela Troncoso.
- ▶ Wikipedia

Privacy by Design in Principles
The 7 Foundational Principles
The GDPR View

Engineering Privacy by Design

To finish

Privacy by Design in Principles
The 7 Foundational Principles
The GDPR View

Engineering Privacy by Design

To finish

1. Proactive, not Reactive; Preventative, not Remedial

- ▶ prevents privacy invasive events **before** they happen
- ▶ does **not** offer remedies for resolving privacy infractions once they have occurred

2. Privacy as the Default Setting

No action is required on the part of the individual to protect their privacy

it is built into the system, **by default**

3. Privacy Embedded into Design

Privacy is **not** an add-on

it is an **essential component** of the core functionality

4. Full Functionality - Positive-Sum, not Zero-Sum

accommodate **all** legitimate interests and objectives

No unnecessary trade-offs

5. End-to-End Security - Full Lifecycle Protection

Privacy throughout the **entire lifecycle** of the data involved

all data are **securely retained**, and then **securely destroyed** at the end of the process

6. Visibility and Transparency - Keep it Open

subject to **independent** verification

Its component parts and operations remain **visible** and **transparent**, to users and providers alike

7. Respect for User Privacy - Keep it User-Centric

keep the interests of the individual uppermost:

- ▶ strong privacy defaults
- ▶ appropriate notice
- ▶ user-friendly options

Privacy by Design in Principles

The 7 Foundational Principles

The GDPR View

Engineering Privacy by Design

To finish

The GDPR: <https://xkcd.com/1998/>

PRIVACY POLICY

WE'VE UPDATED OUR PRIVACY POLICY. THIS IS PURELY OUT OF THE GOODNESS OF OUR HEARTS, AND HAS NOTHING TO DO WITH ANY HYPOTHETICAL UNIONS ON ANY PARTICULAR CONTINENTS. PLEASE READ EVERY PART OF THIS POLICY CAREFULLY, AND DON'T JUST SKIP AHEAD LOOKING FOR SEX SCENES.

THIS POLICY GOVERNS YOUR INTERACTIONS WITH THIS WEBSITE, HEREIN REFERRED TO AS "THE SERVICE," "THE WEBSITE," "THE INTERNET," OR "FACEBOOK," AND WITH ALL OTHER WEBSITES AND ORGANIZATIONS OF ANY KIND. THE ENUMERATION IN THIS POLICY OF CERTAIN RIGHTS, SHALL NOT BE CONSTRUED TO DENY OR DISPARAGE OTHERS RETAINED BY THE USERS. BY USING THIS SERVICE, YOU OPT IN TO QUARTERING TROOPS IN YOUR HOME.

YOUR PERSONAL INFORMATION

PLEASE DON'T SEND US YOUR PERSONAL INFORMATION. WE DO NOT WANT YOUR PERSONAL INFORMATION. WE HAVE A HARD ENOUGH TIME KEEPING TRACK OF OUR OWN PERSONAL INFORMATION, LET ALONE YOURS.

IF YOU TELL US YOUR NAME OR ANY IDENTIFYING INFORMATION, WE WILL FORGET IT IMMEDIATELY. THE NEXT TIME WE SEE YOU, WE'LL STRUGGLE TO REMEMBER WHO YOU ARE, AND TRY DESPERATELY TO GET THROUGH THE CONVERSATION SO WE CAN GO ONLINE AND HOPEFULLY FIGURE IT OUT.

TRACKING PIXELS, COOKIES, AND BEACONS

THIS WEBSITE PLACES PIXELS ON YOUR SCREEN IN ORDER TO FORM TEXT AND IMAGES, SOME OF WHICH MAY REMAIN IN YOUR MEMORY AFTER YOU CLOSE THE PAGE. WE USE COOKIES TO ENHANCE YOUR PERFORMANCE. OUR WEBSITE MAY USE LOCAL STORAGE ON YOUR DEVICE IF WE RUN LOW ON SPACE ON OUR END. WE MAY USE BEACONS TO CALL ROHAN FOR AID.

3RD PARTY EXTENSIONS

THIS SERVICE MAY UTILIZE 3RD PARTY EXTENSIONS IN ORDER TO PLAY THE SONG *CAN U FEEL IT* FROM THEIR DEBUT ALBUM *ALIVE*.

PERMISSION

FOR USERS WHO ARE CITIZENS OF THE EUROPEAN UNION, WE WILL NOW BE REQUESTING PERMISSION BEFORE INITIATING ORGAN HARVESTING.

SCOPE AND LIMITATIONS

THIS POLICY SUPERSEDES ANY APPLICABLE FEDERAL, STATE, AND LOCAL LAWS, REGULATIONS AND ORDINANCES, INTERNATIONAL TREATIES, AND LEGAL AGREEMENTS THAT WOULD OTHERWISE APPLY. IF ANY PROVISION OF THIS POLICY IS FOUND BY A COURT TO BE UNENFORCEABLE, IT NEVERTHELESS REMAINS IN FORCE.

THIS ORGANIZATION IS NOT LIABLE AND THIS AGREEMENT SHALL NOT BE CONSTRUED. THESE STATEMENTS HAVE NOT BEEN EVALUATED BY THE FDA. THIS WEBSITE IS INTENDED TO TREAT, CURE, AND PREVENT ANY DISEASE.

IF YOU KNOW ANYONE IN EUROPE, PLEASE TELL THEM WE'RE COOL.

Art. 25 GDPR: Data protection by design and by default

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.
2. ¹ The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. ² That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. ³ In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.



Privacy by Design in Principles

Engineering Privacy by Design

Web Applications

Minimization

Anonymity

To finish

Privacy by Design in Principles

Engineering Privacy by Design

Web Applications

Minimization

Anonymity

To finish

Top 10 Privacy Risks in Web Applications (OWASP)

- P1 Web Application Vulnerabilities
- P2 Operator-sided Data Leakage
- P3 Insufficient Data Breach Response
- P4 Insufficient Deletion of personal data
- P5 Non-transparent Policies, Terms and Conditions
- P6 Collection of data not required for the primary purpose
- P7 Sharing of data with third party
- P8 Outdated personal data
- P9 Missing or Insufficient Session Expiration
- P10 Insecure Data Transfer

Details here: https://www.owasp.org/images/0/0a/OWASP_Top_10_Privacy_Countermeasures_v1.0.pdf

OWASP's Grid: strengths

How to check?	Countermeasures
<p data-bbox="175 456 363 477">General questions:</p> <ul data-bbox="216 487 644 542" style="list-style-type: none"><li data-bbox="216 487 644 542">• Is an incident response plan for privacy incidents in place?	<p data-bbox="706 456 1022 477">Countermeasures (in advance):</p> <ul data-bbox="747 487 1173 542" style="list-style-type: none"><li data-bbox="747 487 1173 542">• Create and maintain incident response plan.

→ a precise and **pragmatic** (immediately applicable) grid of analysis

Privacy by Design in Principles

Engineering Privacy by Design

Web Applications

Minimization

Anonymity

To finish

Privacy as an Exercise of Control

Data minimization is a "necessary and foundational first step" [Gurses et al., 2011]

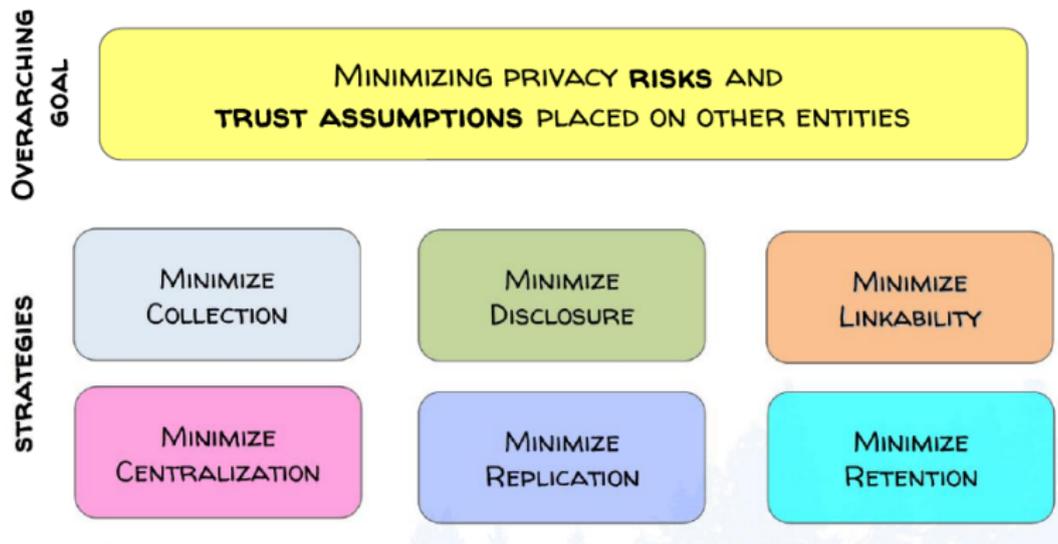
BUT, it's not "data" that is minimized (in the system as a *whole*)

- kept in user devices
- sent encrypted to a server (only client has the key)
- distributed over multiple servers: only the user, or colluding servers, can recover the data

"DATA MINIMIZATION" IS A BAD METAPHOR!!!

Seda Gurses, Carmela Troncoso, Claudia Diaz. Engineering Privacy by Design. Computers, Privacy & Data Protection. 2011

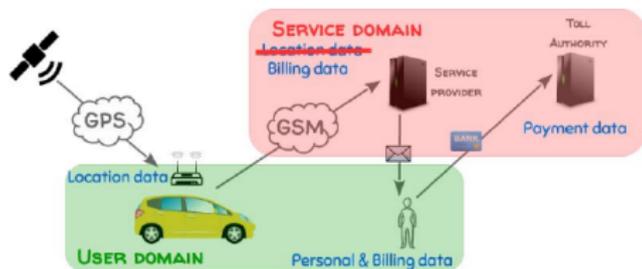
Data Minimization Strategies



[Gurses et al., 2011]

Example

CASE STUDY: ELECTRONIC TOLL PRICING



Location is not needed,
only the amount to bill!

[Gurses et al., 2011]

Privacy by Design in Principles

Engineering Privacy by Design

Web Applications

Minimization

Anonymity

To finish

De-identification has limited value

Zip code, birth date and sex are not considered as **personally identifying information**

However, **87%** of social security numbers can be determined uniquely from the zip code, birth date and sex... (edX MOOC)

De-identification can be easily defeated:

- ▶ identifying data in retained fields
- ▶ combination of multiple partial identification
- ▶ using external data sets

Beyond Grids

Grids are attractive:

- ▶ simple
- ▶ illusion of exhaustiveness

But they are far from enough:

" Neither the risk analysis informed by engineering practice, nor the socially informed engineering practice can be replaced by the other." [Gurses et al., 2011]

Privacy by Design in Principles

Engineering Privacy by Design

To finish

WYHTR: What You Have To Remember



- ▶ Principles
- ▶ Minimization
- ▶ References



Gurses, S., Troncoso, C., and Diaz, C. (2011).
Engineering privacy by design.
In Computers, Privacy & Data Protection.