Privacy by Design on Digital ID

Dr. İsa Sertkaya

September 26, 2019

isa.sertkaya@tubitak.gov.tr
TÜBİTAK BİLGEM UEKAE
Blokchain Research Lab.

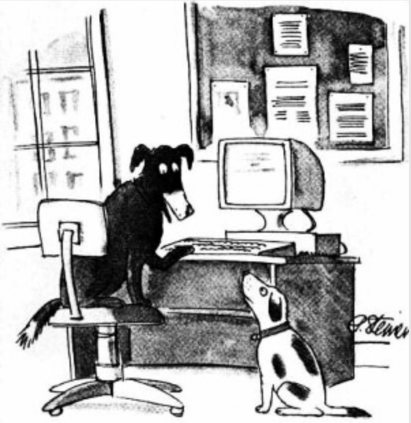
Contents

1. Fakery & Fraud

2. Privacy by Design

3. Privacy Goals

4. Privacy Design Strategies, Techniques



"On the Internet, nobody knows you're a dog."

–Peter Steiner, published by The New Yorker on July 5, 1993

Fakery & Fraud

Fakery and Fraud

WE CAN'T COMPETE ON PRICE.
WE ALSO CAN'T COMPETE ON QUALITY, FEATURES OR SERVICE.
THAT LEAVES FRAUD, WHICH I'D LIKE YOU TO CALL MARKETING.
www.dilbert.com scottadams@aol.com
© 2007 Scott Adams, Inc./Dist. by UFS, Inc.
9-13-07

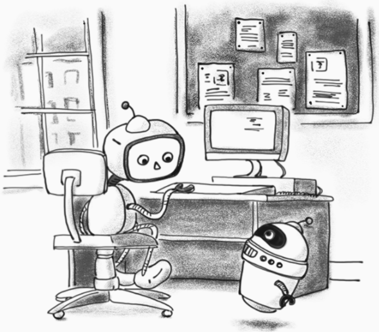
> *"The Washington Post examination found that for some popular product categories, such as Bluetooth headphones and speakers, the vast majority of reviews appear to violate Amazon's prohibition on paid reviews."*

Fakery and Fraud on a Massive Scale

- *Igal Zeifman*: “Imperva report (2016) estimates bots -good and bad- are responsible for 52 percent of web traffic”
- *Guy Rosen*: “Facebook (2018), in Q1, disabled about 583 million fake accounts, most of which were disabled within minutes of registration”
- *Yoel Roth & Del Harvey*: “In May 2018, Twitter identified and challenged more than 9.9 million potentially spammy or automated accounts per week.”

> *“Juniper Research identified the main problems as fake websites and internet domains, fake accounts, and bot farms that generate fake views by robots, not people. ”*
>
> *— Gideon Spanier – How to tackle marketing fraud, (Sep. 6, 2018)*

> *“Juniper Research has warned that marketing fraud will cost advertisers an estimated $19 billion (£15 billion) and rising in 2018, close to 10 per cent of global digital ad expenditure.”*
>
> *— Gideon Spanier – How to tackle marketing fraud (Sep. 6, 2018)*



"On the Internet, nobody knows you're a bot."

–Oliver Reichenstein, Make Bots Identifiable

Privacy by Design

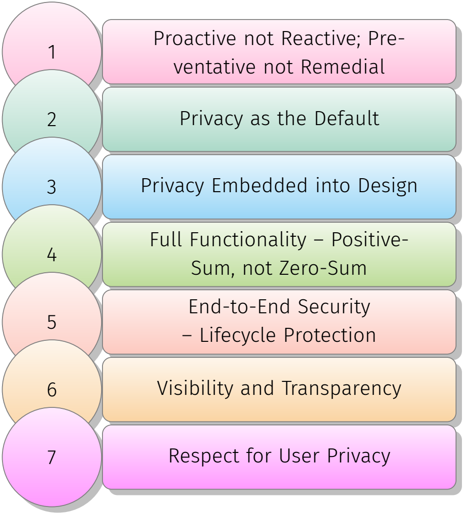
Privacy by Design

“the concept of Privacy by Design extends to a trilogy of encompassing applications:”

- IT systems,
- accountable business practices,
- physical design and networked infrastructure.

–Cavoukian 2010

Privacy by Design: 7 Foundational Principles



1. Proactive not Reactive; Preventative not Remedial
2. Privacy as the Default
3. Privacy Embedded into Design
4. Full Functionality – Positive-Sum, not Zero-Sum
5. End-to-End Security – Lifecycle Protection
6. Visibility and Transparency
7. Respect for User Privacy

1. Proactive not Reactive; Preventative not Remedial

Privacy by Design approach anticipates and prevents privacy invasive events before they happen. PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred - it aims to prevent them from occurring.

2. Privacy as the Default

Privacy by Design seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice.

2. Privacy as the Default

- *Purpose Specification*: Specified purposes should be clear, limited and relevant to the circumstances.
- *Collection Limitation*: the collection of personal information must be fair, lawful and limited for the specified purposes
- *Data Minimization*: the collection of personally identifiable information should be kept to a strict minimum.
- *Use, Retention, and Disclosure Limitation*: the use, retention, and disclosure of personal information shall be limited to the relevant purposes identified to the individual, for which he or she has consented

3. Privacy Embedded into Design

Privacy by Design is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered.

3. Privacy Embedded into Design

- A systemic, principled approach to embedding privacy should be adopted – one that relies upon accepted standards and frameworks, which are amenable to external reviews and audits
- Wherever possible, detailed privacy impact and risk assessments should be carried out and published, clearly documenting the privacy risks and all measures taken to mitigate those risks
- The privacy impacts of the resulting technology, operation or information architecture, and their uses, should be demonstrably minimized

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

Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum “win-win” manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. Privacy by Design avoids the pretense of false dichotomies, such as privacy vs. security, demonstrating that it is possible, and far more desirable, to have both

5. End-to-End Security – Lifecycle Protection

Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved. This ensures that all data are securely retained, and then securely destroyed at the end of the process, in a timely fashion. Thus, Privacy by Design ensures cradle to grave, secure lifecycle management of information, end-to-end.

5. End-to-End Security – Lifecycle Protection

- Entities must assume responsibility for the security of personal information (generally commensurate with the degree of sensitivity) throughout its entire lifecycle, consistent with standards that have been developed by recognized standards development bodies.
- Applied security standards must assure the confidentiality, integrity and availability of personal data throughout its lifecycle including, inter alia, methods of secure destruction, appropriate encryption, and strong access control and logging methods.

6. Visibility and Transparency

Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to both users and providers alike. Remember, trust but verify!

6. Visibility and Transparency

- *Accountabilty*: The collection of personal information entails a duty of care for its protection. Responsibility for all privacy-related policies and procedures shall be documented and communicated as appropriate, and assigned to a specified individual. When transferring personal information to third parties, equivalent privacy protection through contractual or other means shall be secured.
- *Openness*: Information about the policies and practices relating to the management of personal information shall be made readily available to individuals.
- *Compliance*: Complaint and redress mechanisms should be established, and information communicated about them to individuals, including how to access the next level of appeal. Necessary steps to monitor, evaluate, and verify compliance with privacy policies and procedures should be taken.

7. Respect for User Privacy

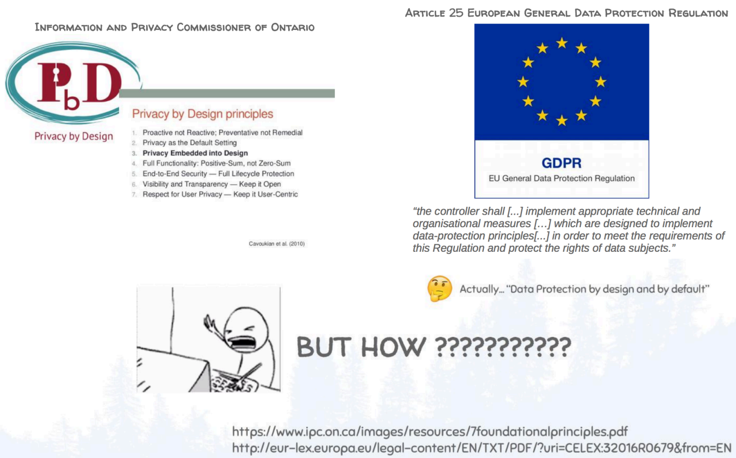
Above all, Privacy by Design requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric!

7. Respect for User Privacy

- *Consent*: The individual’s free and specific consent is required for the collection, use or disclosure of personal information, except where otherwise permitted by law. Consent may be withdrawn at a later date.
- *Accuracy*: personal information shall be as accurate, complete, and up-to-date as is necessary to fulfill the specified purposes. individuals.
- *Access*: Individuals shall be provided access to their personal information and informed of its uses and disclosures.
- *Compliance*: Organizations must establish complaint and redress mechanisms, and communicate information about them to the public.

© Weng lei – Imaginechina

© Hu yan – Imaginechina



INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO

PbD

Privacy by Design

Privacy by Design principles

1. Proactive not Reactive; Preventative not Remedial
2. Privacy as the Default Setting
3. **Privacy Embedded into Design**
4. Full Functionality: Positive-Sum, not Zero-Sum
5. End-to-End Security — Full Lifecycle Protection
6. Visibility and Transparency — Keep it Open
7. Respect for User Privacy — Keep it User-Centric

Cavoukian et al. (2010)

ARTICLE 25 EUROPEAN GENERAL DATA PROTECTION REGULATION

GDPR

EU General Data Protection Regulation

“the controller shall [...] implement appropriate technical and organisational measures […] which are designed to implement data-protection principles[...] in order to meet the requirements of this Regulation and protect the rights of data subjects.”

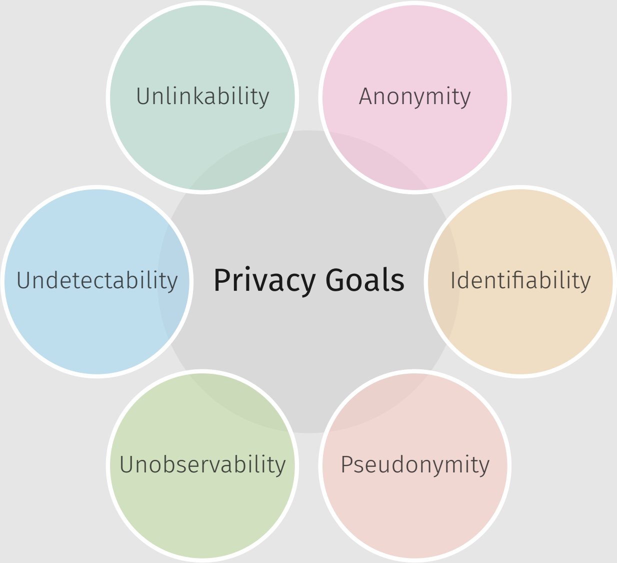
🤔 Actually… “Data Protection by design and by default”

BUT HOW ??????????

https://www.ipc.on.ca/images/resources/7foundationalprinciples.pdf
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

–Carmela Troncoso, Gürses, Troncoso, and Diaz 2011

Privacy Goals



Privacy Goals

Unlinkability

Anonymity

Undetectability

Identifiability

Unobservability

Pseudonymity

–Pfitzmann and Hansen 2010

Anonymity (Pfitzmann and Hansen 2010)

“Anonymity of a subject means that the subject is not identifiable within a set of subjects, the anonymity set.”

or more quantifiably,

“Anonymity of a subject from an attacker’s perspective means that the attacker cannot sufficiently identify the subject within a set of subjects called the anonymity set.”

Unlinkability (Pfitzmann and Hansen 2010)

Unlinkability of two or more items of interest (IOIs, e.g., subjects, messages, actions, …) from an attacker's perspective means that within the system (comprising these and possibly other items), the attacker cannot sufficiently distinguish whether these IOIs are related or not.

Undetectability (Pfitzmann and Hansen 2010)

Undetectability of an item of interest (IOI) from an attacker's perspective means that the attacker cannot sufficiently distinguish whether it exists or not.

Unobservability (Pfitzmann and Hansen 2010)

Unobservability of an item of interest (IOI) means

- undetectability of the IOI against all subjects uninvolved in it and
- anonymity of the subject(s) involved in the IOI even against the other subject(s) involved in that IOI.

Pseudonymity (Pfitzmann and Hansen 2010)

- A pseudonym is an identifier of a subject other than one of the subject’s real names.
- The subject which the pseudonym refers to is the holder of the pseudonym
- A subject is pseudonymous if a pseudonym is used as identifier instead of one of its real names.
- Pseudonymity is the use of pseudonyms as identifiers.

Identifiability (Pfitzmann and Hansen 2010)

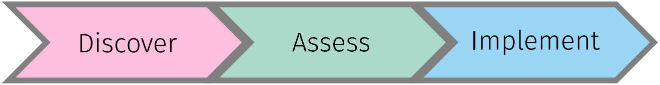
Identifiability of a subject from an attacker’s perspective means that the attacker can sufficiently identify the subject within a set of subjects, the identifiability set.

Identity (Pfitzmann and Hansen 2010)

An identity is any subset of attribute values of an individual person which sufficiently identifies this individual person within any set of persons. So usually there is no such thing as “the identity”, but several of them.

Privacy Design Strategies, Techniques

Privacy Design Strategies


Discover

Assess

Implement

Privacy Techniques

- Authentication
- Verifiable credentials
- Secure private communications
- Communications anonymity and pseudonymity
- Privacy in databases
- Statistical disclosure control
- Privacy-preserving data mining
- Private information retrieval
- Privacy-preserving computations
- Transparency-enhancing techniques
- Intervenability-enhancing techniques

References

- Cavoukian, Ann (2010). “Privacy by design: the definitive workshop. A foreword by Ann Cavoukian, Ph. D”. In: *Identity in the Information Society* 3.2, pp. 247–251.
- Gürses, Seda, Carmela Troncoso, and Claudia Diaz (2011). “Engineering privacy by design”. In: *Computers, Privacy & Data Protection* 14.3, p. 25.
- Pfitzmann, Andreas and Marit Hansen (Aug. 2010). *A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management*. http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf. v0.34.