



Big Data Risks

- Algorithms, different transactions made in different places can be related to one same individual.
- Re-identification.
- Tracking and profiling without user consent or knowledge.
- Security.
- Transparency, discrimination, exclusion and economic imbalance.
- Inaccuracy, government surveillance.

7 PBD Principles

- Proactive not Reactive. Privacy-intrusive events, prevention.
- Privacy as Default Setting. No action required.
- Privacy Embedded into Design.
- Full Functionality. Positive-Sum, not Zero-sum.
- Full Life Cycle Protection. Collection, storage, disclosure, retention and deletion.
- Keep it Open. Transparency.
- Keep it User Centric. Respect User Privacy.

Privacy by Design in the Age of Big Data

Victor Roselló Mallol, CIPP / E
@vic_rosello

Privacy by Design, how? Not so much

John Edwards, Privacy Commissioner Ontario, 14th Sept.

Article 17 (Right to be forgotten)

Article 17 (Right to be forgotten)

What is all the fuss about?

"The Future of Privacy" WP29 (01.12.09).
32nd Int. Conference (27-29.10.10). Seoul.
Translation on PBD (7 PBD Foundation Principles).
New EU Data Protection Regulation (GDPR)
(25.01.12 - 14.04.16)
Art. 23: Privacy by Design and Privacy by Default.

Data quality (retention) / Purpose limitation

Purpose Limitation

Art. 6.1 (b) Directive: "(...) personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes".
Directive 2002/95/EC
- Accountability: balance: purposes: context, responsibility, proportionality, nature of data and targeted to data subject, data retention.
- Right to access: transparency.
- Right to be forgotten: deletion, rectification, erasure, right to be forgotten.
- Right to be forgotten: deletion, rectification, erasure, right to be forgotten.
- Right to be forgotten: deletion, rectification, erasure, right to be forgotten.
- Right to be forgotten: deletion, rectification, erasure, right to be forgotten.



Privacy by Design in the Age of Big Data

Victor Roselló Mallol, CIPP / E
@vic_rosello





YouTube

Let's get back to **1995...**

- Microsoft releases IE 1.0.
- Dot-com boom starts.
- Yahoo.com domain was registered.
- Opera version 1 was launched.
- ebay.com comes online.
- Java is introduced.
- USB standard is released.
- Film "The Net", with Sandra Bullock.

Privacy by Design, new? Not so much

- Ann Cavoukian, Privacy Commissioner Ontario. Mid 90's.
- Directive 95/46/CE.

Article 17. Security of processing.

Article 16. Confidentiality of processing.

Recital 46. "(...) appropriate technical and organizational measures be taken, (...) at the time of design (...)". Protection on rights and freedoms of Data Subjects

Let's get back to 1995...

- Microsoft releases IE 1.0.
- Dot-com boom starts.
- Yahoo.com domain was registered.
- Opera version 1 was launched.
- ebay.com comes online.
- Java is introduced.
- USB standard is released.
- Film "The Net", with Sandra Bullock.

Privacy by Design, new? Not so much

- Ann Cavoukian, Privacy Commissioner Ontario. Mid 90's.
- Directive 95/46/CE.

Article 17. Security of processing.

Article 16. Confidentiality of processing.

Recital 46. "(...) appropriate technical and organizational measures be taken, (...) at the time of design (...)". Protection on rights and freedoms of Data Subjects

Let's get back to 1995...

- Microsoft releases IE 1.0.
- Dot-com boom starts.
- Yahoo.com domain was registered.
- Opera version 1 was launched.
- ebay.com comes online.
- Java is introduced.
- USB standard is released.
- Film "The Net", with Sandra Bullock.

What is all the fuss about?

"The Future of Privacy" WP29 (01.12.09).

32nd Intl. Conference (27-29.10.10), Israel.
Resolution on PbD (7 PbD Foundation Principles).

New EU Data Protection Regulation. **GDPR**
(25.01.12 - 14-04-16)

Art. 23: Privacy by Design and Privacy by Default.

Data quality (retention) / Purpose limitation

- Legally binding for developers and data controllers.
- More powers to DPA.
- Privacy by Default / Give control to users.
- Data minimization.
- Controllability.
- Transparency.
- User Friendly Systems.
- Data Confidentiality.
- Data Quality.
- Use Limitation.

What is all the fuss about?

"The Future of Privacy" WP29 (01.12.09).

32nd Intl. Conference (27-29.10.10), Israel.
Resolution on PbD (7 PbD Foundation Principles).

New EU Data Protection Regulation. **GDPR**
(25.01.12 - 14-04-16)

Art. 23: Privacy by Design and Privacy by Default.

Data quality (retention) / Purpose limitation

What is GDPR?



Article 23
Data protection by design and by default

1. Having regard to the state of the art and the cost of implementation, 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 and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.
2. The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals.
3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures and mechanisms referred to in paragraph 1 and 2, in particular for data protection by design requirements applicable across sectors, products and services.
4. The Commission may lay down technical standards for the requirements laid down in paragraph 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Not only PbD...

- Right to be forgotten.
- Data portability.
- Data breaches notifications to data subjects.
- Not to be subject to automated processing decisions (except provided by law).
- Right to access.
- PIA's.



What is all the fuss about?

"The Future of Privacy" WP29 (01.12.09).

32nd Intl. Conference (27-29.10.10), Israel.
Resolution on PbD (7 PbD Foundation Principles).

New EU Data Protection Regulation. **GDPR**
(25.01.12 - 14-04-16)

Art. 23: Privacy by Design and Privacy by Default.

Data quality (retention) / Purpose limitation

Purpose limitation

Art. 6.1 (b) Directive: "(...) personal data must be collected for specific, explicit and legitimate purpose and no further processed in a way incompatible with that purpose".

Opinion 3/2013 WP 29:

- Relationship between purposes: context, reasonable expectation, nature of data and impact to data subject.
- Opt-in, always required.
- Access to decisional criteria. Logic of decision making algorithm.
- Data accuracy.
- Direct access to data.
- Allow data portability.

Purpose limitation

Art. 6.1 (b) Directive: "(...) personal data must be collected for specific, explicit and legitimate purpose and no further processed in a way incompatible with that purpose".

Opinion 3/2013 WP 29:

- Relationship between purposes: context, reasonable expectation, nature of data and impact to data subject.
- Opt-in, always required.
- Access to decisional criteria. Logic of decision making algorithm.
- Data accuracy.
- Direct access to data.
- Allow data portability.

Big Data Risks

- Algorithms, different transactions made in different places can be related to one same individual.
- Re-identification.
- Tracking and profiling without user consent or knowledge.
- Security.
- Transparency.
- Inaccuracy, discrimination, exclusion and economic imbalance.
- Increasing government surveillance.



**ACCESS AND
UNDERSTANDING**



**STRONGER
PRIVACY LAWS**



You Tube

7 PbD Principles

- Proactive not Reactive. Privacy-intrusive events, prevention.
- Privacy as Default Setting. No action required.
- Privacy Embedded into Design.
- Full Functionality. Positive-Sum, not Zero-sum.
- Full Life Cycle Protection. Collection, storage, disclosure, retention and deletion.
- Keep it Open. Transparency.
- Keep it User Centric. Respect User Privacy.

Privacy by Design in the Age of Big Data

Victor Roselló Mallol, CIPP / E
@vic_rosello

