UNIVERSITÀ DEGLI STUDI DI BRESCIA

PEERE

Data hugging, reputation and research information

Giorgio Pedrazzi

University of Brescia

UNIVERSITÀ DEGLI STUDI DI BRESCIA

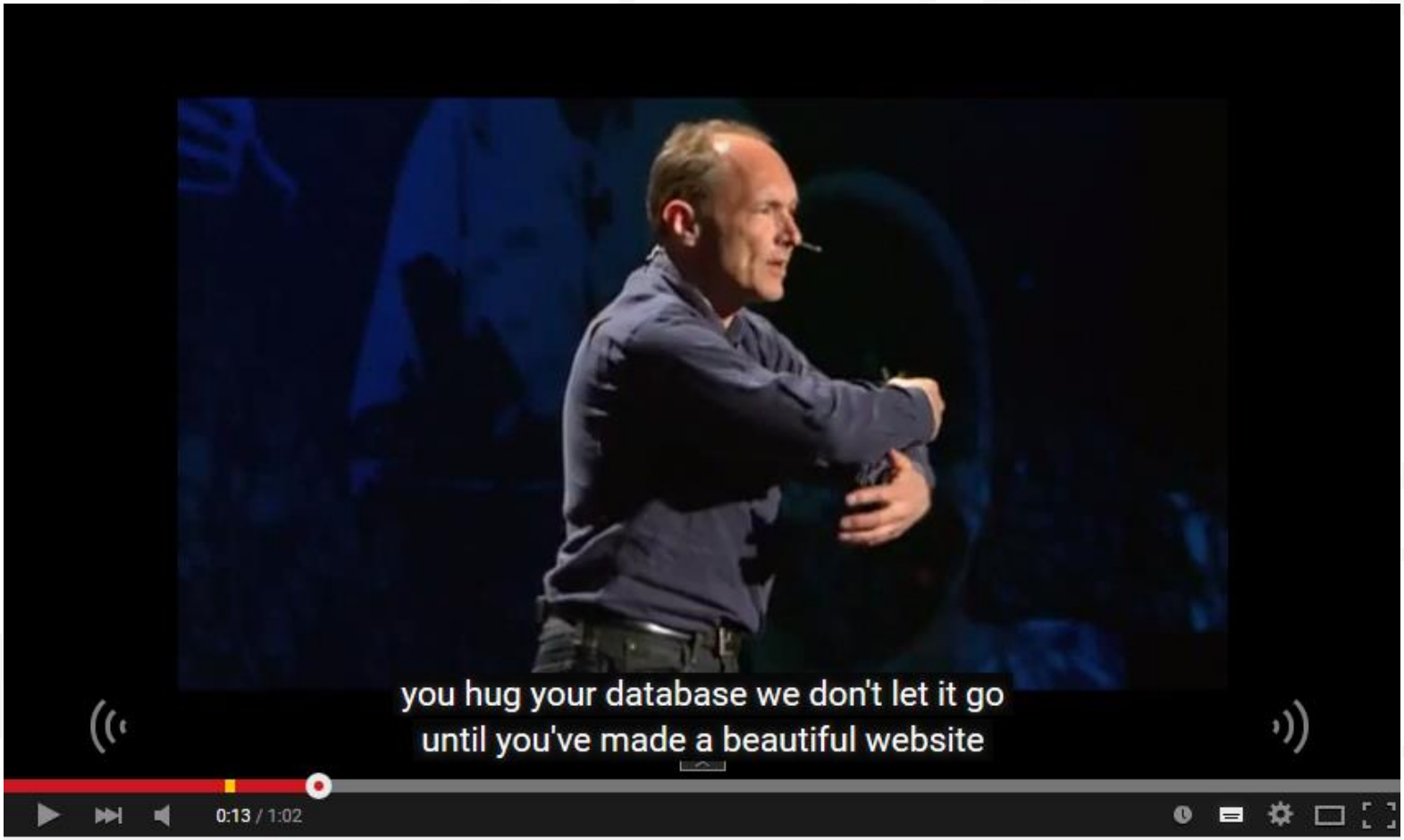
Giorgio Pedrazzi

is adjunct professor of Information Technology and Law and Private Law at the University of Brescia, lawyer and consultant in privacy and data protection, insurance and tort law, videosurveillance, paperless administration, e-commerce and consumer law. He wrote more than 30 articles published on law reviews and is at present working in two research projects on the legal issues in the development of smart cities.

SUMMARY

1. RESEARCH INFORMATION AND PERSONAL DATA
2. RISKS AND TOOLS
3. PRIVACY IMPACT ASSESMENT

DATA HUGGING



Tim Berners-Lee Stop Hugging Data

PERSONAL DATA and INFORMATION are interchangeable words?

ARTICLE 29 DATA PROTECTION WORKING PARTY

The Article 29 Working Party is an independent European working party that deals with issues relating to the protection of privacy and personal data. The data protection authorities (DPA) of the EU Member States are members of the Working Party

The WP was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

Example No. 9: information contained in the minutes of a meeting.

01248/07/EN WP 136 Opinion 4/2007 on the concept of personal data Adopted on 20th June

An example of the need to perform the analysis with regard to each piece of information separately concerns the information contained in the minutes of a meeting, recording typically the attendance of participants Titius, Gaius and Sempronius; the statements made by Titius and Gaius; and a report of proceedings on certain topics as summarized by the author of the minutes, Sempronius.

Example 9

As personal data relating to Titius one can only consider the information that he attended the meeting at a certain time and place, and that he made certain statements. The presence in the meeting of Gaius, his statements and the proceedings about an issue as summarized by Sempronius are NOT personal data relating to Titius.

Example 9

. This is so even if this information is contained in the same document, and even if it was Titius who triggered the issue to be discussed at the meeting. It is therefore excluded from Titius' right of access to his own personal data.

SCIENTIFIC REVIEW PRINCIPLES

- reliability,
- impartiality,
- verifiability,
- independence

PRIVACY PRINCIPLES

- legitimacy,
- data minimization,
- purpose limitation,
- transparency,
- data integrity,
- data accuracy

PRIVACY RIGHTS AND TOOLS

- right of access,
- rectification,
- erasure,
- objection,
- right to be forgotten,
- right to data portability

PRIVACY BY DESIGN

A key element in privacy by design are the Fair Information Principles (FIPs), that are set “to limit collection, use and disclosure of personal data, to involve individuals in the data lifecycle, and to apply appropriate safeguards in a continuous manner.” This means “the separation of personal identifiers and content data, the use of pseudonyms and the anonymization or deletion of personal data as early as possible”. SCHAAR

PRIVACY AND RESEARCH

PEERE…change of perspective: a shift from “patient information” to “researcher information”

research participant paradigm

Protecting Individual Privacy in Evaluation Research. Washington, DC: The National Academies Press, 1975

PRIVACY IN PEER REVIEW

RISKS

any professional concerned with collecting, processing, using or determining the fate of personal data (whether as policy-setter, administrator, publisher or researcher) should be aware of the RISKS involved

DISSEMINATION

If this [dissemination of FBI criminal history records] is done properly, it's not a breach of privacy.

Clarence Kelley, FBI Director5 U.S. News and World Report, 15 October 1973, p. 59

WP art. 29 on RISKS

Fundamental principles applicable to the controllers (i.e. legitimacy, data minimization, purpose limitation, transparency, data integrity, data accuracy) should remain the same, whatever the processing and the risks for the data subjects.

WP 218 Statement on the role of a risk-based approach in data protection legal frameworks Adopted on 30 May 2014

WP art. 29 on RISKS

However, due regard to the nature and scope of such processing have always been an integral part of the application of those principles, so that they are inherently scalable.. See e.g. the use of "adequate", "appropriate", "reasonable" and "necessary" in Articles 6 and 7 of Directive 95/46/EC

TRUST & ETHICS

Research goals

Balancing values at stake

Process Evaluation

ACADEMIC REPUTATION

Researcher deals with information, spread and disseminate information, rely on information for their academic career

Reputation depends on how these information circulate and how accurate they are

Reputation also depends on the transparency of process evaluation

ITALY DPA

Purpose of the disclosure of data is relevant.

Researchers' evaluation should not be disclosed in processes involving universities' evaluation for public funding

As stated by Italian DPA in an interview to a newspaper on 3 november 2012

What to do in…

…a data sharing initiative where two or more organisations seek to pool or link sets of personal data.

see PIA code practice

ICO - UK

PRIVACY IMPACT ASSESSMENT

A privacy impact assessment is a methodology for assessing the impacts on privacy of a project, policy, programme, service, product or other initiative which involves the processing of personal information and, in consultation with stakeholders, for taking remedial actions as necessary in order to avoid or minimise negative impacts.

PRIVACY IMPACT ASSESSMENT

A PIA is more than a tool: it is a process which should begin at the earliest possible stages, when there are still opportunities to influence the outcome of a project. It is a process that should continue until and even after the project has been

David Wright and Paul De Hert, Introduction to Privacy Impact Assessment,p.6

PRIVACY IMPACT ASSESSMENT

A good PIA will engage stakeholders from the outset as a way of gathering their views and ideas about how any intrusive privacy impacts can be avoided or mitigated

David Wright and Paul De Hert, Introduction to Privacy Impact Assessment,p.6

ANONIMIZATION TECHNIQUES

randomization

generalization

noise addiction

k-anonymization

l-diversity

ANONYMISED DATA

Anonymised data would therefore be anonymous data that previously referred to an identifiable person, but where that identification is no longer REASONABLY possible

LIMITS OF ANONYMIZATION:

controllers must take into account the technological means which are likely reasonable to allow identification or pose risks for the individuals' privacy

RISKS IN ANONYMIZATION

SINGLING OUT , which corresponds to the possibility to isolate some or all records

which identify an individual in the dataset;

INFERENCE, which is the possibility to deduce, with significant probability, the

value of an attribute from the values of a set of other attributes.

RISKS IN ANONYMIZATION

LINKABILITY, which is the ability to link, at least, two records concerning the same data subject or a group of data subjects (either in the same database or in two different databases). If an attacker can establish (e.g. by means of correlation analysis) that two records are assigned to a same group of individuals but cannot single out individuals in this group, the technique provides resistance against "singling out" but not against linkability;

AOL INCIDENT

A typical instance of the misconceptions surrounding pseudonymisation is provided by the well-known “AOL (America On Line) incident”. In 2006, a database containing twenty million search keywords for over 650,000 users over a 3-month period was publically released, with the only privacy preserving measure consisting in replacing AOL user ID by a numerical attribute

AOL INCIDENT

This led to the public identification and location of some of them. Pseudonymised search engine query strings, especially if coupled with other attributes, such as IP addresses or other client configuration parameters, possess a very high power of identification.

QUOTE

Privacy, like the weather, is something everyone talks about. But unlike the weather, there is much that should, and can, be done about it.

Gary T. Marx, M.I.T www.garymarx.net

Like today's weather is a really HOT topic

WHAT SHALL WE DO NOW?

Check the types of data, minimising the use in the dataset

Explore the tools available to avoid identification

Develop guidelines on impact assessments


THANK
YOU
GRACIAS
ARIGATO
SHUKURIA
DANKSCHEEN
JUSPAXAR
GOZAIMASHTA
EFCHARISTO
GRAZIE
MEHRBANI
SUKSAMA
EGHIET
TASHAKKUR ATU
YAQHANYELAY
BOLZÏN
MERCI
BÏYAN
SHUKRIA

CONTACTS

https://unibs.academia.edu/GiorgioPedrazzi
http://it.linkedin.com/in/giorgiopedrazzi
https://www.facebook.com/gpedrazzi
SkipeID: gpedrazzi
Twitter: @PedrazziGiorgio
mobile: +393356883042
it.linkedin.com/in/giorgiopedrazzi/en