

When privacy law meets technology A marriage of convenience?



Claudia Cevenini

Contract professor of New technologies and Law
II Faculty of Engineering
University of Bologna, Italy



ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA
SEDE DI CESENA

LAW

- regulates conflicting interests
- decides which one should prevail

Right to be left alone VS Right to know

Freedom of the press VS protection of fundamental rights

PRIVACY LAW

- if and upon what conditions personal data may be processed
- to what extent one can control its own data

EVOLUTION OF TECHNOLOGY

Privacy regulation has become more complex and demanding

Companies want to advertise VS People want to be left alone

EUROPE

Strong privacy rules for advertising and promotional calls
(not enough: low punishment levels, need for technical tools)

ITALY

Derogation until June 2010: citizens overwhelmed with calls.
(In Italy there are almost 4 million companies...)

CASE IN POINT

by Tom Fishburne


LAWYERS ARE FROM MARS, TECHIES ARE FROM VENUS

HE'S JUST NOT LISTENING: THE AMENDED FRCP REQUIRES A LEGAL HOLD AND AN EARLY CASE ASSESSMENT SO WE CAN AVOID RULE 502

SHE'S JUST NOT LISTENING: OUR TIERED STORAGE SUBSYSTEM AND FEDERATED SEARCH ONLY ALLOW ENTITY EXTRACTION WITH THE RIGHT ACL PERMISSIONS

GOOD, GOOD, NOW HOW DOES THAT MAKE YOU FEEL?



CaseCentral 

LAW and ICT

- different reasoning patterns
- different languages
- different geographical limitations

PRIVACY IN THE INFORMATION SOCIETY

- can no longer afford this separation
- need for common understanding and synergies

DIFFERENT SPEEDS

- fast-moving ICT and trailing legal provisions
- need for certainty (=stability) of the law

NEED FOR KNOWLEDGE

To regulate something, the law needs to understand it

Q: What is cloud computing?

A1: A lawyer or a judge might think of some Photoshop device to take pictures of clouds

A2: "A computing capability that provides an abstraction between the computing resource and its underlying technical architecture (e.g., servers, storage, networks), enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction."
(National Institute of Standards and Technology)

PRIVACY ISSUES

- loss of control on data
- possible transfer of data to third countries
- security

LEGAL PEOPLE

need to understand what this is all about

TECHNICAL PEOPLE

need to be aware of how not to break the law

ACTIONS

- ban the cloud?
- 'cut' it into national sections?

THE ROLE OF LAW IN IS

- prevent misbehaviour by threatening a sanction or
- actively support the development and use of safer, privacy-compatible technologies?

EU MEMBER STATES

- very strict privacy rules
- severe sanctions

PROBLEM

- control is necessarily limited
- only a small number of data mishandling is punished

UNITED KINGDOM

- Companies breaching the Data Protection Act may be fined up to 500.000 pounds (over 770.000 US dollars).
- The privacy protection authority will decide on a case-by-case basis (e.g. actual damage, amount of lost data, etc.).
- 2008 – personal data of hundreds of thousands of employees and candidate employees of the Ministry of Defence were lost.
- Not an isolated case: in 4 years, 747 laptops and 121 storage devices were lost.

The **law** intervenes **after** the damage is done.

What about **codes of conduct** and **best practices**?

EU Commissioner for Information Society and Media

- “**Europeans** must have the **right to control** how their **personal information** is used.”
- The **Commission** will take **action** if **Member States** fail to **implement privacy rules**.
- Need of **consent** before processing personal data.
- **Privacy** must be “a **high priority** for **social networking providers** and their **users**”.

EU Directive on privacy and electronic communications (2002/58/EC)

- confidentiality of communications
- prohibiting unlawful interception and surveillance without consent

EU Data Protection Directive (95/46/EC)

- provision of information before data processing
- free, express, specific consent to data processing

EC-promoted agreement on Social networking

Major social networks have engaged to improve privacy, especially of minors. SN have taken responsibility to ensure child safety and committed to enable and encourage users to employ a safe approach to personal information and privacy.

A different view has been expressed by Facebook's ideator Mark Zuckerberg:

If he were to create Facebook again today, user information would by default be public, not with privacy settings decided by the user.

- Safer Internet day (9 February) - Microsoft research
- Young people do not adopt protection measures
- Risks: cyberstalking, paedophilia, moral violence, etc.
- 73 % young Italians accept friendship from strangers
- 76 % exchange pictures and videos (also not their own) with strangers
- 23 % give their home address
- Pathological need to express oneself - show off - consolidate one's identity
- Massive uploading of sensitive data (political opinion, religion, sexual orientation, etc.)

Is the age of privacy over?

Would we be happy with the end of privacy?

What consequences would it imply for us to share personal information with everyone?

What perspective is more suitable for today's web users?

Should privacy law be rethought?

Should law always lag behind ICT or act preventively by setting a basic framework which may flexibly adapt to the future?

A big issue: trade-off between the need for certainty and stability of the law and the urge to keep the pace with an extremely rapid technological evolution.

Different opinions: some affirm that the framework in force may flexibly be adapted to issues set by new technologies, others state that perhaps certain paradigms should be rethought.

Who is right? *Ai posteri l'ardua sentenza.*

Thank you very much for your attention!

claudia.cevenini@unibo.it