

Ensuring respect for privacy on the Internet

Dr. Lee A. Bygrave

<lee.bygrave@jus.uio.no>

<http://folk.uio.no/~lee>

Presentation for panel session "Counteracting Privacy Violations on the Internet", 26th International Conference on Privacy and Data Protection, Wroclaw, 14-16 September 2004

University of Oslo
Norwegian Research Centre for Computers and Law
<http://www.jus.uio.no/iri/english/index.html>



Application of law to Internet

Important question is NOT: do laws apply to Internet?
But rather: HOW do they apply to Internet?

Latter question leads to two further questions:

1. Do the laws apply with sensible results?
2. Do laws give sufficient prescriptive guidance?

University of Oslo
Norwegian Research Centre for Computers and Law
<http://www.jus.uio.no/iri/english/index.html>



Application of data privacy law

- Most major data privacy laws (eg, Directive 95/46/EC (DPD)) drafted with little account of Internet
- Main exception = Directive 2002/58/EC (DPEC)
- But DPEC applies only to network providers, not content providers; hence, says relatively little about appropriate conditions for Digital Rights Management Systems (DRMS)
- Key definitional issues left unresolved: eg, scope of "personal data" concept with respect to e-mail addresses, IP addresses and attached clickstream data
- Status of electronic agents?

University of Oslo
Norwegian Research Centre for Computers and Law
<http://www.jus.uio.no/iri/english/index.html>



The judiciary to the rescue?

- Little clarifying case law
- BUT major decision of European Court of Justice in Lindqvist case (101/01, decision of 6th Nov. 2003)
- Sensible decision that helps clarify application of DPD Art 3(2) and Art 25 in context of website publishing
- But leaves several questions unanswered: eg, when can a webpage with personal data be sufficiently private to fall within exemption in Art 3(2)? How are we to treat the provision of links to another person's webpage that contains their personal details?

University of Oslo
Norwegian Research Centre for Computers and Law
<http://www.jus.uio.no/iri/english/index.html>



The risk of regulatory overreaching

- Some instances in which application of data privacy rules does NOT have entirely sensible results.
- Good example = DPD Art. 4(1)(c): the data privacy law of an EU state may apply outside the EU if a data controller, based outside the EU, utilises "equipment" located in the state to process personal data for purposes other than merely transmitting the data through that state
- Above rule runs risk of regulatory overreaching in online environment; leads in turn to mockery of the law

University of Oslo
Norwegian Research Centre for Computers and Law
<http://www.jus.uio.no/iri/english/index.html>



Legislative support for PETs

- Most data privacy laws contain little direct support for use of Privacy-Enhancing Technologies (PETs)
- DPD = case in point
- Article 17 and recital 46 are concerned *prima facie* with security measures
- Difficulties in introducing more PET-specific rules, but these difficulties are surmountable
- Goals of anonymity (and/or pseudonymity) need to be specified more clearly, as do the means of their achievement (in terms of systems development)
- German legislation as model, cf, "Systemdatenschutz"

University of Oslo
Norwegian Research Centre for Computers and Law
<http://www.jus.uio.no/iri/english/index.html>



Role of “netiquette”

- Netiquette = useful but not sufficient condition for ensuring respect for privacy in online environment
- Touted advantages = flexibility; user “ownership”; non-legalistic (hence simple) terminology
- Possible problems = “lightweight” normative effect (eg, uncertainty in terms of creating binding or influential precedent); relatively transitory
- Cf Norway’s “Net Tribunal” (Netnemnda)

University of Oslo
Norwegian Research Centre for Computers and Law
<http://www.jus.uio.no/iri/english/index.html>



Co-Regulation

- “Top-down” legislative action must be supplemented by “bottom-up” code making
- Self-regulation by itself is insufficient; self-regulatory initiatives often more fruitful when threat that the state will otherwise “cover the field” through legislation
- Few co-regulatory schemes currently working with respect to Internet industry; cf Australia’s Internet Industry Association Privacy Code of Practice (2001 draft) still awaiting approval
- Involvement of DPAs in Recommendations for Consideration (RFC) and other Internet standards?

University of Oslo
Norwegian Research Centre for Computers and Law
<http://www.jus.uio.no/iri/english/index.html>



Education in schools

- Courses on “information ethics” (including data privacy) are arguably the most enduring solution
- Much still to be done; too much focus hitherto on getting ICT into schools; too little focus on teaching youth about the ethical ramifications of using ICT
- Increasing interest from secondary and primary school teachers for appropriate materials on data privacy
- Data protection authorities should be involved in developing course materials, and should get more resources to do so

University of Oslo
Norwegian Research Centre for Computers and Law
<http://www.jus.uio.no/iri/english/index.html>

