

Privacy in the electronic communication sector: insights from the ISP industry

Innocenzo Genna
Genna Cabinet
Bruxelles

FIA Conference
Ghent, 16 November 2010

*The opinions expressed in this presentation do not represent the position of associations
where the Author holds management responsibility*

- Innocenzo Genna, consultant on telecoms and Internet regulation and policy at EU Level. Extensive experience in fixed and mobile entrants practice
- Currently director of Italian ISP association (AIIP) and Council officer of Euroispa
- Chairman of ECTA (European Telecommunications Competitive Association) from 2007 to 2009
- General Counsel of the Tiscali Group from 2002 to 2006
- Attorney, practising law since 1992

Scope of my intervention

- Just an informal intervention on the privacy subject in the electronic communications sector, based on my familiarity with relevant stakeholders
- Reminding the applicable data protection framework
- Describing the ISP business and how data protection rules apply to it
- Examination of specific cases

Relevant Data Protection framework

- Directive 95/46 on data protection in general
- Directive 2002/58 on privacy on electronic communications services (“ECS”)
- 2009 reform of the ECS framework modifying Directive 2002/58 in relation to:
 - cookies (art. 5,3)
 - securities breaches (art. 4)
 - unsolicited communications (art. 13)
- Directive 95/46 subject to review, consultation in process
- Relevant interactions with Directive 2000/31 on electronic commerce (information society services: “ISS”)

ISP/telcos position on the review of Directive 95/46

- Joint position paper of Cable Europe, ECTA, ETNO, Euroispa, GSM Europe
- Need to review and adapt data protection rules to the challenges of the evolving ECS sector with regard to various items:
 1. Applicable law; 2. International transfer of data 3. Harmonisation (lack of harmonisation); 4. Role of Article 29 Working Party; 5. Consent; 6. Transparency; 7. Personal data breach notifications; 8. Awareness; 9. Self regulation; 10. Personal data of minors; 11. Profiling; 12. Right to be forgotten; 13. Data portability

ISPs's activities and categories

2 main categories of ISPs:

- Access providers: providing Internet access and connectivity (data transportation)
 - like Belgacom, Tele2, Telenet, Cable/Wireless, etc
- Hosting providers: hosting data and managing platforms
 - Pure infrastructure lease: Akamai
 - Content/social platforms: Youtube, Facebook, etc

Impact of access/hosting differentiation on ISP liability

- The distinction between access and hosting ISP is reflected by Directive 2000/31, setting 2 levels of liability for ECS/ISS:
 - Access providers (art. 12): no liability (mere conduit principle)
 - Hosting and cache providers (arts. 13 and 14): no liability, unless actual knowledge of illicit content/activity (then removal obligation)
- Above differentiation relevant for application of different categories of rules, with direct or indirect impact on privacy:
 - Protection of confidentiality in private communications
 - Protection of personal data of minors and disabled categories
 - Protection of intellectual property rights
 - Net neutrality rules
 - etc etc

Case 1 (hosting): spam, anti-spam and filtering

- Spam (and unsolicited communications) prohibited by privacy and electronic commerce rules, with criminal sanctions
- Anti-spam filters may require intrusive inspection of communications, subject however to:
 - consent of the users
 - only electronic mail (irrelevant fraction of Internet traffic)
 - communications managed by hosting-ISP on its servers
- Similar filtering activities by access-ISP via routers technically very difficult, inefficient and legally doubtful

Case 2 (hosting): protection of minors/disabled categories

- The Vividown-Google case in Italy
- In 2006 some minors posted on Youtube a video of a disabled boy being bullied by others
- Google removed the video after intervention of Vividown, an association protecting disabled children; doubts about the prompt reaction of Google
- The court condemned 3 Google executives for violation of privacy rules: Youtube's privacy information was not found to be proper and adequate to prevent such accidents
- Court decision does not consider hosting liability limitation and seems to be weak on privacy
- Beside challenging the decision, Google made an agreement with Vividown to prevent future accidents

Case 3 (access): IPR infringements

Content and rights owners require access-ISP's to cooperate and fight online piracy through activities which may conflict with privacy rules:

- usage of software to discover piracy infringements in the Internet, and collection of evidences
- filtering of Internet traffic (through DPI: Deep Packet Inspection) to find and block pirated content
- disclosure of personal details related to IP addresses (allegedly involved with piracy)
- retention and process of personal data for IPR enforcement

See the Sabam-Scarlet case in Belgium

Case 4 (access): network management practices

- Network management practices are licit when providing security or solving traffic congestions, more controversial when intended to exclude or discriminate other companies/services
- Such practices may imply filtering and therefore interfere with privacy rights, depending on the concrete circumstances:
 - Discriminating categories of traffic (VOIP, P2P, etc) is not controversial per se
 - More enhanced filtering (like DPI) may raise concerns (relevant for IPR enforcement, VOIP detection, anti-terrorism etc)
- Proper evaluation requires case-by-case analysis:
 - are IP-packets wholly comparable to private correspondence?
 - “opening” IP-packets (payload inspection) is an illicit intrusion into personal life?
 - may intrusions be legitimated by the scope, consent etc?

Thank you

Genna Cabinet

Brussels

inno@innogenna.it