Electronic business and data privacy: The role of standardisation

Received: 30th November, 2000

Jos Dumortier

is a professor in law at the University of Leuven (Belgium) and the director of the Interdisciplinary Centre for Law and Information Technology (ICRI). As a consultant for the Belgian federal government, he has been very intensively involved in the transposition of the European data protection directive into Belgian law. He has also written the discussion report for the European Standardization Initiative in the field of data protection. He is the author of numerous books and articles about all kinds of legal issues related to e-business.

Caroline Goemans

is a researcher at the Interdisciplinary Centre for Law and Information Technology (ICRI).

Abstract The protection of the individual, with regard to processing of personal data in the context of global electronic business, remains problematic despite the wide range of regulatory initiatives in this area. The respective EU and US approaches are briefly set out in this paper, and are also explored, in the light of the potentials of standardisation, as possible operational guidelines which would complement the existing legal framework in the area of personal data protection.

INTRODUCTION

The success of electronic business largely depends on the potential to present the right products and services to the right person. Modern Web technology makes it possible to create a customised environment for every individual customer. The on-line store displays only commercial messages matching the customer's profile perfectly.

It is probable that the surface of the Web's personalisation potential has only been scratched. In the near future, more *integrated* personalisation can be expected, where the customer profile is maintained across all sales channels, and where improved techniques are used for managing customer and product categories and for offering real-time incentives and promotions.

Personalisation is only possible if the

customer is assured that their personal data, whether communicated by them or collected in the background, will not be misused. A serious impediment to the further development of electronic commerce is the consumers' fear that the information they communicate will be used in ways they would not authorise. Almost 87 per cent of US respondents in a survey of experienced Internet users stated that they were somewhat or very concerned about threats to their privacy on-line.¹

PERSONAL DATA PROTECTION LAW IN THE EUROPEAN UNION

It is evident that the processing of personal data in the context of electronic business has to remain within the limits of the law. In the European Union (EU)

Jos Dumortier
K.U.Leuven, ICRI,
Tiensestraat 41, B 3000
Leuven, Belgium.
Tel. +32 016 32 51 49;
Fax +32 016 32 54 38;
e-mail: jos.dumortier@
law.kuleuven.ac.be
www.law.kuleuven.ac.be/icri

the principal legal text on this issue is the European Data Protection Directive of 1995. The Directive contains a series of general rules that had to be transposed by the member states into their national law before the end of October 1998.²

The Directive pursues two closely linked objectives: on the one hand to ensure the rights of the individual with regard to the processing of their personal data and, on the other hand, to ensure that such data can move freely within the EU. It has to be taken into account that the Directive provides only a framework and that much of the effectiveness of the protection of personal data will depend on the various implementation mechanisms.

The consequence of the Directive is that data protection principles have to be embodied in comprehensive law, applicable to all sectors of the economy and providing the possibility for non-compliance to be sanctioned and for individuals to be given a right of redress. The law has to incorporate additional procedural mechanisms, such as the establishment of independent supervisory authorities with monitoring and complaint investigation functions.

For a commercial website owner in Europe, it means that personal data of a potential customer cannot be processed without taking into account the customer's national data protection legislation. In this legislation will be found a comprehensive set of general rules and procedures, directly deduced from the Directive. It remains, however, very delicate to translate this general legal framework into specific guidelines directly applicable to the context of electronic business. The Directive therefore states that member states and the Commission, in their respective spheres of competence, must encourage trade associations and other representative organisations to draw up codes of conduct in order to facilitate the

application of the Directive. These codes should take account of the specific characteristics of the processing of personal data carried out in certain sectors, and respect the national provisions adopted for its implementation. In the philosophy of the Directive the rules on personal data protection with regard to on-line commerce have to be developed in a dedicated code of conduct.

THE US APPROACH

The USA has approached the regulation of the use of personal information in a different way. European laws attempt to protect individual rights more or less in a preventive manner, through an active, authoritative state role, at least as far as the general legal framework is concerned. In contrast, US regulatory philosophy is more based on a tradition of open society and minimal state intervention. In order to minimise state intrusion on information flows, the USA approaches the regulation of personal data processing more through attention to discrete sector and subsector activity. Comprehensive law is rare.³ Nonetheless, the practical effects of the contrast between the approaches on either of the Atlantic must not be overestimated.

A number of US trade associations have promulgated fair information practice guidelines to promote standards for the treatment of personal information in specific industries. Companies have established policies and practices, including internal codes of conduct and procedures offering supplementary protection. A growing number of websites display a button referring to one or more pages explaining the site's privacy policy.

In 1998, the Federal Trade Commission (FTC) requested trade associations and industry groups to

voluntarily submit copies of their on-line information practice guidelines and principles. Examination of those guidelines proved that they did not address all the core fair information practice principles that are widely accepted in the USA.⁴

In its 1999 report, the FTC stated that the results of two new surveys of commercial websites suggested that on-line businesses were providing significantly more notice of their information practices than they were in 1998. The new results showed, however, that, despite these efforts, the vast majority of even the busiest websites had not fully implemented certain fair information practice principles. Problems mainly concerned the provision of reasonable access for on-line consumers to personal data collected from and about them, and the maintenance of adequate security for that information.⁵ Finally, in its 2000 Report,⁶ the FTC concludes that self-regulatory efforts from industry alone have not been sufficient. Accordingly, the FTC recommends that Congress enact general, technologically-neutral legislation, based on widely accepted, fair information practices. The FTC recognises, however, that industry self-regulation, as well as consumer and business education, should still play important roles.

SEALS AND OTHER PRIVACY PROTECTION TOOLS AND SERVICES

Even in the USA there is a growing understanding that the mere publication of some self-developed privacy policy principles on the website is not enough to increase the confidence of on-line consumers with regard to the protection of their personal data. An individual consumer is generally unable to evaluate the quality of a company privacy code

and does not have any means of control on the compliance of the company with its stated principles.

One possible answer to this concern is the delivering of 'seals' representing the website's information policy for users' personal information. Companies can submit their privacy policy to a, more or less, neutral third party and receive a trustmark if this policy meets certain criteria. It remains uncertain, however, how effectively the compliance of the company with its privacy principles is controlled. The companies themselves also remain responsible for the development of their privacy policy. In practice some of these policies are very obscure and difficult to evaluate by an average Web user.

There is also increasing availability of anonymity services, combining the use of pseudonyms, strong encryption and network facilities. One proxy-based service lets users both block information that typically gets sent to a website and create aliases for site registration. Another service sends the user's Internet traffic through a series of privacy-enhancing detours and invites the user to create several pseudonyms to use for different on-line interests. The user alone decides how much — or how little — personal information to disclose with each pseudonym and how many different pseudonyms to create.

To summarise, a new industry is springing up to help on-line consumers get better control of the use of their data. Practically every week new privacy protection services or tools are announced. As privacy becomes an industry of its own, however, competing standards, guidelines and systems may make consumers and Web publishers alike throw up their hands in frustration. The wide variety of services and the constant development of new creative ideas in this domain is undoubtedly very

positive. As in every other sector, however, creativity, innovation and competition have to be combined with a certain degree of standardisation.

The role of standardisation

More than any other area, electronic business has come to depend on standards to ensure inter-operability and ubiquitous adoption of technology. Clearly, both businesses and users can participate more effectively when systems work together, and the standardisation process can contribute mightily to achieving this success. Individual consumers will feel more confident when systems operate seamlessly, efficiently, securely and effectively through common approaches. Precisely this objective has been the driver for one of the standardisation initiatives in the context of the Internet, the 'P3P'. The platform for privacy preferences (P3P) is an initiative of the World Wide Web Consortium (W3C) enabling users to negotiate with a Web service on the use of personal information. The negotiation is steered by a standardised procedure.⁷

This kind of standardisation is not necessarily an obstacle for innovation or competition. On the contrary, one has only to look at the very competitive mobile telephony market in Europe to see how standards and competition can go hand in hand. Standardisation could create a more transparent market in privacy protection services for consumers. It would improve their ability to compare various offers and make it easier for them to move from one provider to another. This could even lower the access to the market and stimulate competition.

Aware of the potential role of standardisation, the EU Commission mandated CEN/ISSS⁸ to further examine the issue. Following an open seminar in

March 2000, CEN/ISSS established the 'Initiative for Privacy Standardization in Europe' (IPSE) to investigate whether there is a case for standardisation as an operational tool to help business and other market players to implement the EU Directive on personal data protection. Following the investigation, IPSE will be examining its specific requirements in a set of recommendations.

Acknowledgment

This paper is based upon a report on behalf of CEN/ISSS for presentation at the Open Seminar on 'Standardization: A business tool for data privacy', which took place in May 2000 in Brussels.

References

- 1 Cranor, L.A., Reagle, J. and Ackermann, M. (1999) 'Beyond Concern: Understanding net users' attitudes about on-line privacy', AT&T Labs Research Technical Report TR 99.4.3, <http://www.research.att.com/projects/privacystudy>
- 2 'Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data', *Official Journal L* 281, 23/11/1995, pp. 0031–0050, http://europa.eu.int/eurlex/en/lif/dat/1995/en_3-951.0046.html
- 3 Schwartz, P. and Reidenberg, J. (1996) 'Data privacy law. A study of US data protection', Michie Law Publishers, Charlottesville.
- 4 Federal Trade Commission (1998) 'Privacy on-line: A report to Congress', <http://www.ftc.gov/reports/privacy3/index.htm>
- 5 Federal Trade Commission (1999) 'Self-regulation and privacy on-line', report to the Congress, <http://www.ftc.gov/reports/privacy/index.htm>
- 6 <http://www.ftc.gov/os/2000/05>
- 7 World Wide Web Consortium (1999) 'Platform for privacy preferences (P3P)', Working Draft 26th August, <http://www.w3.org/p3p>
- 8 <http://www.cenorm.be/iss>

Further reading

- Anwang, G. (1999) 'The stuff you want', *PC Magazine*, Vol. 18, No. 17, 5th October, p. 103.
- Dumortier, J. and Goemans, C. (2000) 'Online data privacy and standardisation: Towards a more effective protection?' In 'A decade of Research @ the Crossroads of Law and ICT', De Boeck and Larcier, Brussels, pp. 53–69.

Miller, M. (1999) 'E-relationships are vital, *PC Magazine*, Vol. 18, No. 20, 16th November, p. 4.

Swire, P. (1996) 'Self-regulation and government enforcement in the protection of personal information', report submitted to the National

Telecommunications and Information Administration (NTIA) <http://www.acs.ohio-state.edu/units/law/swire1/psntia6.htm>

US Department of Commerce (1999) 'Elements of effective self-regulation for protection of privacy', <http://www.ecommerce.gov/staff.htm>