

MINUTES OF MEETING OF THE DATA PROTECTION WORKING PARTY  
held at Impact House, Croydon, on 23 September 1999

**1.. Presentation.**

- 1.1 The Chairman explained the purpose of the meeting, which was to examine how Codes of Practice could be used to ensure privacy for personal data especially over the Internet. Although critical for electronic commerce, the issue was wider than that. She and Dara Christopher would first outline the background situation.
- 1.2 DC referred to the Right to Privacy, stemming from Article 8 of the Convention on Human Rights. Data protection legislation in the UK had provided safeguards for individuals in their private lives and Directives on the subject included the principle of supporting the rights of individuals. However, the applicability of this when individuals were browsing websites was not clear cut.
- 1.3 VT said that as part of revising existing legislation to allow for changing circumstances, Code of Practice should be considered as self-regulatory options. The focus on the Internet had arisen following the provisions in the Directive regarding the transfer of data overseas; Article 27 regarded Codes of Practice as an aid to compliance. Compliance with a Code would be taken into account when assessing an organisation's level of compliance. This could facilitate the legitimate transfer of personal data overseas.
- 1.4 VT quoted research which showed that very few websites had privacy policy statements on them and, if they did exist, they were hard to find or to understand. The completion of registration forms was often necessary to gain access to a site and personal details were required before purchases could be made. Mailing lists were compiled from this information, which resulted in a vast collection of data. (This contrasted with equivalent off line processes - one did not have to reveal one's identity to use a reference library or to make purchases in a shop). There were concerns that data matching was being used to form individual profiles.
- 1.5 DC said it was important for business to recognise that respecting personal privacy would not have a negative effect on the way business was done. Most US on-line users felt that the information requested of them was more than was necessary for the purpose of their use; there was a total lack of proportionality. There concerns were those of data protection, although they tended to view it as a privacy issue. There were, however, good commercial

reasons for building up user profiles and this could be acceptable if the core data protection principles were observed, in particular that users were informed how their data were being processed.

## **2. Discussion on the nature of the on-line privacy problem.**

2.1 Much on-line data capture took place in the background (eg with automatic hyper-links and cookies). Some sites, such as Amazon.com took more than a paragraph of code for cookie information. This enabled them, for instance, to discover what other software was on the PC. The information taken would then allow direct marketing identification of individual users.

2.2 When a website was accessed a link could be established by the ISP between them and the user's machine. The Data Protection Directive enabled a computer's identity to be classed as personal information, but this had not been carried into the UK Act. The issue was not with cookies per se but with what they were used to collect. They could be used without including any personal information. No standards existed in this area.

2.3 Cookies were just one example of the generalised growing concern about invasions of privacy made possible by use of the Internet. For instance, Microsoft had set up background automatic processing that read everything on the user's machine. They took all information from the PC, whether relevant or not. The user was not aware it was happening and had no way of disabling it. (Although those with the right technical knowledge could delete cookies from their machines, by then the information had already been transferred.) This raised issues of notice and giving the user informed awareness of what was happening; the Microsoft website now informed users wishing to download software that the search would take place and gave the user the option to abort the request before any data had been transferred.

2.4 It was not just a question of respecting users' privacy rights but of giving them a chance to control the use of their data and letting them have informed awareness with which to do so. A good on-line privacy statement should explain what was going on and give the user options at each stage. There should also be a mechanism for the user to delete or revise incorrect data. Privacy statements must be obvious and easily accessible from the Home Page.

## **3. Consideration of ways of achieving compliance**

3.1 A major problem was the global nature of the processing. The UK and Europe had tended to be in the forefront of legislation and codes in this area and nothing would happen globally unless a start was made somewhere. There was an urgent need to build up the confidence of Internet users and there were initiatives such as kite-marking to encourage this. It was suggested that the ODPR should give accreditation to those schemes which complied with the data protection requirements. DT referred to the BSI/DISC initiatives in this area which would give added value to the legislation. They were not, however, near a formal standard at the moment.

3.2 Most initiatives went down a similar route and did not necessarily help the consumer. The question was whether or not to formalise into a standard and require compliance. To be effective on the Internet, any standard would have to cover both the European and the US approaches to privacy and data protection. Enforcement would be difficult by the very nature of the world wide web.

**4. Consideration was given to what should be included in codes of practice.**

4.1 The responsibilities of those who created websites to include the right things in their designs were discussed. The processes required must be user friendly and simple to do. Most importantly, they must not be seen as a barrier to doing what the user went to the website to do.

4.2 Policy statements should be easy to find, clear and easy to understand. They should explain the site owner's responsibilities and users' rights, including how to obtain copies of data and make changes. The details in the statement would come from the legislation - certain things would have to be included to achieve compliance. This was felt to be no more onerous than what business were required to do in the paper environment.

4.3 The following were known to be happening:

4.3.1 The OECD were producing a privacy statement generator; this was still being beta-tested. (details at [oecd.org/scripts/pw/pwgenerate.asp](http://oecd.org/scripts/pw/pwgenerate.asp))

4.3.2 A Hong Kong guide for data controllers on developing privacy statement (criticised as being too long) - PIC (Personal Information Collection) statement ([www.pco.org.hk](http://www.pco.org.hk))

4.3.3 ICX-Shell/Post Office were working on a general code for the conduct of international business. This included electronic commerce aspects but not specifically so. They were looking for something of practical use to businesses seeking compliance. TBDF matters were included but it had not yet been decided whether that part of the code would apply outside Europe.

4.3.4 A Dutch Electronic Commerce Platform had a code of conduct that included data protection.

4.3.5 Global Business Dialogue on Electronic Commerce had an issue group working on the Protection of Personal Data, which was, inter alia, looking at the development of privacy policies.

4.3.6 Some codes were being prepared for electronic commerce generally, but included data protection matters.

4.3.7 There seemed to be evidence that designers were going to sites they liked and copying the ideas. Provided there were good statements there this was OK.

**5. Some limitations were identified.**

- 5.1 One danger was the abuse from within the company of the information collected for a proper purpose (e-fraud).
- 5.2 Privacy statements were useless if they were not complied with.
- 5.3 The cost of compliance was an issue.

**6. The role of the regulator was considered**

- 6.1 DT said the ODPR was looking for a practical, sensible approach to these issues. They preferred a self-regulatory approach to one based on law. The BSI/DISC code of practice was intended to add value to the legislation. As more bodies co-operated, confidence would be built and wider compliance achieved. Their work did not at present cover Internet issues specifically, but they would be doing an e-commerce review next year. This would be prepared by consultants and then put out for consultation.
- 6.2 It was suggested that harmonisation across the DP commissioners would be a good objective. There was merit in a standardised, harmonised code rather than a disparate collection.
- 6.3 A code which was produced and approved by the Commission would be a useful first step. European standards were probably higher than elsewhere in the world and gave a satisfactory solution for many trading nations. Since all Member States had to comply with the same directive it should not be too difficult to produce an acceptable pan-European code. DT mentioned the ODPR's belief that codes should be "owned" by those who used them and not prescribed by authority. The airline direct marketing code was cited as an example.
- 6.4 Any attempts at a global code would have to be at a very basic level and would have to be compatible with US policy. Safe-harbour was an example of Europe speaking to the US of what principles should apply.
- 6.5 The issue was seen to be partly one of awareness. Although the OECD Guidelines were widely respected and would be a good starting point for any international codes, many organisations did not know about them. It was thought that most UK businesses were, however, now aware of the ODPR.

**7. Actions by the working party relating to Codes of Practice:**

- 7.1 The working party would prepare a map of the initiatives to produce codes in this area. A first pass would be circulated by the end of the year, along with a short status report explaining the issues VT/  
DC/  
KN
- 7.2 Contact would be made with BSI/DISC (Bernadette Shine) to establish the

nature and timing of input from the working party to their exercise. VT

7.3 Evidence to the Trade and Industry Select Committee would be examined for details of relevant codes and other initiatives. VT/  
DC

**8. Other proposed working party activities:**

8.1 Comment to be made on data protection aspects of the e-communications bill and the IOCA review (in liaison with secure e-commerce working party).

8.2 Consideration of further secondary legislation to the 1998 Act.

**9. Copies of the following papers were distributed to those attending:**

OECD Report on International and Regional Bodies: Activities and Initiatives in Electronic Commerce. (Contents pages and section on *Protection of Privacy and Personal Data* only). Prepared for Ottawa Ministerial Conference, October 1998. (7 pages)

Global Business Dialogue on Electronic Commerce: Working papers and draft policy paper of Issue Group on *Protection of Personal Data*. (26 pages)

Speech by Francis Aldhouse (Deputy Data Protection Registrar) to 21<sup>st</sup> International Conference on Privacy and Personal Data Protection; Aug 99.: *Self Regulation - Codes of Practice to Standards*. (8 pages)

Article by Christopher Millard in "Computers and Law", Feb/Mar 99: *Data Protection and the Internet* (7 pages)

Article by Christopher Millard from "An International Who's Who of Internet and E-commerce" undated : *Four Key Challenges facing Internet and e-commerce lawyers* (3 pages).