

EURIM Working Group Minutes

Theme/WP: Data Protection Working Party
Ref: 00-WP01-Min03
Drafted by: Kate Norman
Date prepared: 24/07/00
Circulation: WP1 and T6; all TL&rapp.

Minutes of the Internet Privacy Models launch meeting held at ICL, Finsbury Square, London EC2 on Thursday 13th July 2000

1. Introductions

Lord Renwick welcomed everyone to the meeting then asked Philip Virgo to explain the background to the initiative.

PV said that once an organisation was using the Internet it was in multiple jeopardy from regulators around the world, not least those in the USA. Sets of local legislation could be very draconian - resulting in "safe harbours" with minefields in them. It was necessary to find a way through the minefields. The ODPC did not have the resources to do the type of thing that was planned under this project but the objective was to produce something that they would be prepared to rubber-stamp.

2. Dara Christopher - Web Statements

(DC was the initiator of this project a year previously when she worked as a lawyer for Huon Corporation. Since leaving them, she has been involved in providing practical advice on data protection matters to clients with websites.)

DC said that the European Commission was taking a hardline stance in relation to the US situation, saying that there was no general legislation that was relevant. The US response was to suggest a two-tier approach - one for data influenced by European data controllers and another for internal use only. This would create real problems for US businesses and for those trading with the.

She considered that web statements would become a key issue in terms of how they could show data subjects that they were protected. The US would at some stage have to implement the proposals in the pipeline and then companies would find that the only practical way of showing the world they were compliant would be through web statements - which would become very important components of any site. They would give customers confidence in the security and data integrity of a site and would help ensure the organisation complied with applicable laws and codes. In addition, a web statement helped in the harmonisation of a company's policy in a complex legal area and raised internal corporate awareness of how personal data were processed and the need to handle them correctly. Merely thinking about these issues created dialogue between departments, which was essential in a climate where personal data were increasingly being captured for data mining purposes.

DC then outlined the key ingredients of a good web statement. It must:

- identify the data controller(s) within the organisation;
- describe how data are collected and processed;
- list the purposes for which personal data are collected;
- indicate when there could be disclosure to third parties;
- show how changes to personal data are handled;
- address security and technological issues;
- make appropriate disclaimers;
- indicate the policy for review and updating of the statement.

Describing how data were processed and the purposes were, she said, the most difficult part of the statement to get right. As it was crucial to get customer prior consent there had to be certainty that the website captured this in the correct way. Opt-out clauses were required at all times, not just at first contact with the customer. The right to get access (eg against a warrant) must also be reserved.

Problems included the excessive collection of data and insufficient disclosure of processing purposes. There was a tendency to use very wide descriptions, eg: “data needed in order to operate our business efficiently”. Often it was possible to opt-out only from third party use, not from the use of one’s data within an organisation. Language was sometimes ambiguous and excessive retention of personal data was widespread.

DC said that the US was very active in self-regulatory initiatives and described some of these. Online privacy seals confirmed adherence to a code and the best included verification and audit procedures. The American Advertising Federation distributed generic web statements to its members which they could then tailor to their needs. Certified e-commerce sites are said to meet certain standards and claim that their disputes procedures include UK based customers. There was widespread industry support for the self-regulatory organisations, whose codes and guidelines were said to be in broad agreement with EU data protection principles.

In summary, she said that a well drafted web statement would help customer confidence. Anyone whose website was applicable to US and Canadian customers should consider applying for an appropriate seal. It was desirable also to have compliance tests. An independent policy was required in addition to a seal.

3 Nicola McKilligan - the need for practical solutions

(NMcK had previously worked at the ODPC and was now consulting to clients on data protection matters.)

NMcK offered an industry perspective on the value of an initiative to bring self regulation into this area. In the early days, she said, the Internet had been seen as the Wild West - but now the sheriffs were in town. Industry in general was keen to comply but this was a very confusing time for them. The Data Protection Act applied in the on-line environment the same as it did off-line. Its provisions included the Euro-centric requirement of the Data Protection Directive not to transfer to territories with inadequate protection. It was difficult to comply with this in the global environment of the Internet. The French were trying to say that in the context of cookies French law would apply globally. There were also initiatives on hand on the

way data could be processed. The ODPC itself was being reviewed; the telecommunications directives were under review. Industry, she said, wants to comply but does not know what procedures to put in place now to secure compliance in the future.

Self-regulation was an essential part of securing compliance on the net, but it was difficult to decide which code to sign up to and then how to put it into practice on the website. Privacy policies were, she stressed, only as good as the procedures that backed them up. She queried the extent to which a web statement could be relied on to prove compliance under the law. Was it actually telling people up front what you intended to do?

There was a lack of guidance from regulators at the moment on what was the best way for industry to go. No statements had been made on how to run websites. A company could have a good off-line policy but not know how to transfer it to the on-line environment. While there may soon be guidance from the UK Commissioner, she cannot give advice about compliance with the requirements of other countries. Germany was particularly difficult. There was a danger that people would say it was all much too difficult and ignore the requirements completely. It must be made feasible and self regulation must be practical. In her view being able to buy templates off-the-shelf would immediately cut through the minefields. They would offer a cost-effective quick fix but other initiatives would also be needed. Industry and regulators both had a part to play in educating consumers to know what to expect. It was doubtful if there could ever be complete protection for consumers on the web, but they can be told what type of thing to look out for. Regulation, self-regulation and education might just be able to form a bridge. It was, she said, in all our interests to see this achieved. In future, when thinking about privacy we will increasingly be thinking of information privacy - out there in an open network. We needed a practical pragmatic approach now to ensure our futures were secure.

4. Discussion

Asked to clarify how privacy models would work and their relationship to privacy statements, PV said that the original specification drawn up by the working party had been to provide a set of generic templates indicating how the web site would be operated, who would do it, how it would be controlled and what would be said on the web, the whole package to be something a corporate lawyer was willing to approve. While agreeing that a privacy statement was a critical part of showing the world that you were complying, he said it was catastrophic if not done correctly. The statement was merely the public face of a model which must run right through the organisation and be part of its CRM strategy.

Opt-in versus opt-out was still the subject of debate. While there were attempts by industry in the US to kill off opt-in, since their Courts considered that silence did not mean assent, the value of opt-out had been destroyed.

There were key differences between US and EU legislation and particular difficulties arose with merged databases that came under contrasting regulations. Another issue was the type of redress. DC indicated that there were common denominators between the different regulatory areas in the US which should make a good base for

acceptance by the EU.

There was concern that whereas seals might all seem to the consumer to mean the same thing that was not the case. Although based on the same principles, background regulations would differ. There needed to be consistency in the approval of seals and funding of the operation of the approving body was critical. DT pointed out that the ODPC did not look to try to stamp approval on seals but conceded that it could support an external exercise to do that. Trustmark in the UK offered the consumer the opportunity to check against a list of approved seals that any individual one was genuine.

UK consumers had to be very wary of providing data to US based organisations since, notwithstanding promises made in web statements, foreigners could only get redress in the US courts if there was someone over there willing to act on their behalf.

5. Next steps

PV said that the requirement was to produce not just a statement generator but also the mechanisms that resulted in a working tool. He suggested that a start could be made by taking existing best practice, get agreement that was indeed something acceptable and then get it approved. Gradually more models would be added in as the “best of breed” in individual sectors were developed and identified.

He thought that the initial models would be some of the cleanest systems around because they would have been developed to get consumer trust. It was essential to know that privacy statements married back into reality, that cover offered was genuine and that the parties involved were contractually bound to deliver.

MG said that ICL’s customers were asking how they could get consumer confidence in this area and confirmed that her company was willing to undertake the initial work on providing acceptable models.

It was recognised that seeking de jure standards would take too long but that it might be possible to produce templates that amounted to a de facto standard.

DK indicated that BSI would be pleased to see such an initiative and there was a possibility that they could provide an approval logo.

The marketing advantages of being known to follow best practice should help take-up and lead to a lower cost service. It was, however, recognised that many businesses would need independent help to implement the models correctly. The crunch point would be to get organisations to change their business models to incorporate more genuine privacy.

Audit was an important consideration. Although the EC have an audit right, the UK DP Commissioner’s powers relate to the investigation of complaints. DT said that although the ODPC did not have a direct resource enabling them to carry out audits, they expected soon to produce an audit manual developed in conjunction with data controllers.

Although costs would fall as take up increased, it was recognised that there would

still be problems associated with the smallest web traders who could not afford to buy in advice and who might well not understand the issues involved. It was hoped that ultimately standard website packages would have the key privacy features built in as default - perhaps with the ISP being required to disconnect anyone not using the package correctly.