Unclassified **DSTI/ICCP/REG(2006)5/FINAL**

Organisation de Coopération et de Développement Economiques
Organisation for Economic Co-operation and Development **24-Jul-2006**

English - Or. English

DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY
COMMITTEE FOR INFORMATION, COMPUTER AND COMMUNICATIONS POLICY

DSTI/ICCP/REG(2006)5/FINAL
Unclassified

Working Party on Information Security and Privacy

MAKING PRIVACY NOTICES SIMPLE: AN OECD REPORT AND RECOMMENDATIONS

English - Or. English

JT03212212

Document complet disponible sur OLIS dans son format d'origine
Complete document available on OLIS in its original format

FOREWORD

Privacy notices are an excellent tool to disclose an organisation's privacy practices and policies. Research suggests, however, that many notices are too lengthy, confusing, and contain complex legal language. This report recommends that privacy notices be short, simple and usable to make it easier for individuals to assimilate the information they contain and to compare the privacy practices of the organisations processing their personal data.

This report was presented to the Working Party on Information Security and Privacy in May 2006. It was declassified by the Committee for Information, Computer and Communications Policy in July 2006.

The report is published under the responsibility of the Secretary-General of the OECD.

© OECD/OCDE 2006

MAKING PRIVACY NOTICES SIMPLE: AN OECD REPORT AND RECOMMENDATIONS

More than 25 years after their adoption, the 1980 *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (Privacy Guidelines)* remain the basis for the work of OECD in the area of personal privacy providing guidance on the collection and processing of personal information in any medium. In the 1998 Ottawa Declaration, OECD Ministers reaffirmed the importance of the *Privacy Guidelines* and their commitment to the protection of privacy on global networks. Ministers also approved an action plan, which called upon the OECD to encourage the adoption and online notification of privacy policies to users.[1]

Among the projects undertaken by the OECD's Working Party on Information Privacy and Security (WPISP) to fulfil the Ministerial mandate was the development and dissemination of the OECD Privacy Statement Generator.[2] The Privacy Statement Generator is an educational tool that provides guidance to organisations on how to conduct an internal review of their existing practices and how to develop privacy policies. The key innovation of the Generator is that it can automatically produce a statement based on a user's answers to a series of questions about current personal data practices and indicate where those practices are not consistent with the *OECD Privacy Guidelines*. It remains a valuable tool to assist organisations in developing privacy statements for their websites. (See Annex A, available in DSTI/ICCP/REG(2006)5/FINAL/ANN).

The WPISP also developed "Privacy Online: OECD Guidance on Policy and Practice" (2003 Policy Guidance), which encouraged online organisations to (*i*) review their privacy practices and develop a privacy policy that would give effect to the OECD privacy principles and (*ii*) post their privacy policy on line in a prominent place. The 2003 Guidance encouraged businesses to embark on their own initiatives to promote and expand privacy protection on line.[3]

Stakeholders in OECD member countries have responded to this challenge by examining ways to develop privacy notices that would be easier for individuals to understand, compare, and use. There is a consensus on the need for short, simple, and usable privacy notices. The OECD welcomes the work of various stakeholders aimed towards achieving this goal.

Over the last couple of years, the WPISP has monitored ongoing initiatives to try to create simplified privacy notices. The OECD work programme for 2005-06 calls upon the WPISP to deliver guidance regarding the development of simplified privacy notices. This report describes current initiatives and offers policy guidance to governments and organisations in drafting simplified privacy notices.

I. Current initiatives

Governments and the private sector have recognised that the format and design of privacy notices can play an important role in educating individuals about an organisation's privacy practices. Current practices can be improved by delivering statements that are easier to read and understand, and that allow individuals to compare the privacy practices of multiple organisations.

A. Government initiatives

U.K. Fair Processing Notifications Research

In March 2005, the UK Office of the Information Commissioner announced the results of research it commissioned into the effectiveness of privacy notices in the financial sector, known as "Fair Processing Notices" (FPNs).[4] The key finding of the research was that the majority of people learn little from privacy notices in their current form. An executive summary of the report is attached as Annex B, available in DSTI/ICCP/REG(2006)5/FINAL/ANN.

The research found that approximately 60% of people say they care about what happens to their personal information, yet most people ignore FPNs, when presented in hard copy or on the Internet. The findings suggested that even when they do pay attention to FPNs, readers are not able to assimilate much of the information provided.

According to the research, the ineffectiveness of FPNs can be traced in part to problems in the design of the notices.[5] The styles currently used in FPNs are an ineffective way of conveying information, with notices being too long and repetitive, containing financial and legal jargon, inadequately identifying main points, and failing to engage the reader. The research found that efforts to focus a reader's attention by using tick boxes or signature boxes, for example, as well as using more compelling titles could improve the impact of a notice. Nearly three-quarters of those asked said they would pay more attention to better designed FPNs.

In commenting upon the results of the research, the UK Information Commissioner highlighted that companies can improve FPNs by:[6]

- Applying a clear and identifiable structure to all FPNs across all media.
- Including only necessary and relevant content.
- Using clear and understandable language, and cutting out jargon.
- Using a generic format 'template' for all FPNs.
- Designing FPNs appropriately for different media.
- Increasing consistency of approach within sectors.

US Government Notice Project

In 2001, eight US Government agencies launched a joint effort to explore principles for writing effective privacy notices.[7] The project was precipitated by the implementation of a new US financial privacy law that required financial institutions to provide their customers with notices describing their information collection and sharing practices and, for certain types of sharing, to provide an opt-out notice. The business community, consumer and privacy organisations, and academics all reported that the privacy notices were too lengthy, confusing, and contained complex legal language.

Following a public workshop in December 2001 entitled "Get Noticed: Effective Privacy Notices," in 2004 the agencies initiated a Notice Project to determine whether privacy notices could be designed that are easier for consumers to understand and use and that allow the consumer to easily compare different privacy notices.

To achieve its goal, the joint-agency project undertook extensive consumer research, organised in two phases. A research report concluding the first phase was publicly released on 31 March 2006.[8] The executive summary is available as Annex C in DSTI/ICCP/REG(2006)5/FINAL/ANN. This report describes qualitative research into the development of simplified privacy notices conducted through in-

depth, one-on-one interviews with consumers throughout the United States. This "usability" testing looked at how consumers actually use privacy notices and allowed researchers to probe consumers' attitudes toward and understanding of these documents. Over a 12-month period through a series of test rounds, the researchers gauged consumer reaction to draft notices. They then modified content and presentation after each test round to create a prototype notice that demonstrably improved consumer comprehension and ability to compare information practices.

The key research findings show that consumers need a context for understanding the information in privacy notices. For example, although consumers are gradually becoming aware of information sharing, most consumers do not have an operational understanding of how it works and how those practices affect them. The research also found that complex information needs to be simplified to make it easier for consumers to make better-informed choices about how their personal information will be used. The research concluded that good design enhances the readability of the privacy notices.

The US Government is currently conducting quantitative testing of the first phase results. This second phase is designed to assess a prototype notice developed during the first phase of the project along with examples of other notices by performing testing on a larger number of consumers. This phase will measure and compare the effectiveness of alternative privacy notices by testing for comprehension, usability, and comparability. The US Government anticipates results from this phase of testing within the year.

B. Industry initiatives

CIPL's Multilayered Notice Project

In 2001, the Center for Information Policy Leadership (CIPL)[9] began the multi-layered "highlights" notices project to foster the global harmonisation of multilayered notices and promote privacy notices that would communicate clearly, comply with applicable laws, and be consistent with the OECD *Privacy Guidelines* and other international standards.

The proposed notices take a layered approach in which a condensed, plain language notice would first be displayed in a template format. The CIPL template design is a short, one-page form with six boxes, each with a standard heading but with non-standard text. The template approach allows each company to complete the boxes with two or three summary statements of its own formulation. A full notice containing a complete description of the company's practices could either be linked to the short notice or made available on request.

Participants in the CIPL project have developed a paper entitled "Ten Steps to Develop a Multilayered Privacy Notice", available as Annex D in DSTI/ICCP/REG(2006)5/FINAL/ANN. It provides background on multilayered notices and a guide to the use of the CIPL template for the development of a multilayered notice.

II. Support for simplified notices and examples of their use

OECD work, including the Privacy Statement Generator and 2003 Policy Guidance, affirmed the importance of furthering the development of effective privacy notices. In particular, the documentation associated with the Privacy Statement Generator outlined a four-step process for developing a privacy policy (see Annex A to DSTI/ICCP/REG(2006)5/FINAL/ANN). The recent initiatives described above supplement OECD work by introducing a new dimension for making privacy notices more effective: a focus on simplicity. Such efforts to improve the effectiveness of privacy notices have been monitored by the OECD and provide the basis for the guidance offered below.

The concept of simplified privacy notices has been positively received at other international venues. In 2003, the International Conference of Privacy and Data Protection Commissioners adopted a resolution highlighting the importance for organisations to improve significantly their communication of information on how they handle and process personal information.[10] The resolution further called for the development of a condensed format for presenting an overview of privacy information that could be standardised world-wide.

In March 2004, an *ad hoc* international group of privacy experts from data protection authorities, government, civil society and business agreed on a memorandum which further developed the concept.[11] Later in 2004 the European Union's Article 29 Data Protection Working Party adopted an opinion that expressed support for the concept of a multi-layered format for data subject notices that use language and layout that is easy to understand.[12] The opinion also highlighted that short notices are legally acceptable provided they are used within a multi-layered structure that, in its totality, complies with national requirements.

A number of government and businesses have begun to implement simplified privacy notices on their websites. In Australia, the Federal Government's primary website uses a multi-layered privacy notice format, on the recommendation of the Australian Privacy Commissioner. In New Zealand, the Office of the Privacy Commissioner has adopted a short notice format,[13] as has the Office of the Information and Privacy Commissioner in British Columbia, Canada.[14] Other government users include the United States Postal Service, whose website has a privacy statement in a multi-layer format.[15]

Businesses around the world have now adopted privacy notices in the multi-layer format, with such notices now available on the websites of large multinationals and smaller businesses in 40 languages. Examples are included in the CIPL paper in Annex D to DSTI/ICCP/REG(2006)5/FINAL/ANN.

III. Recommendations

OECD member countries reaffirm that privacy notices are an excellent tool for implementing the "Openness Principle" of the OECD *Privacy Guidelines*, which provides that:

> There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

They underline that a privacy notice is an obvious way to disclose an organisation's privacy policy and practices, which should reflect how the basic principles of the *Guidelines* are being implemented. Short, simple, and understandable privacy notices are a useful addition to a complete notice, and better enable individuals to make informed decisions about their personal information.

Based on earlier OECD work and on current initiatives described above, OECD member countries encourage organisations to consider the following key steps for developing effective privacy notices:

1. ***Identify data flows***: Identify your organisation's practices regarding the collection, use, sharing, protection, and destruction of personal data.

2. ***Conduct a legal review***: Determine which laws, regulations, industry codes, contracts, corporate promises, or other legal requirements cover the collection and use of personal data by your organisation.

3. ***Prepare a comprehensive privacy policy statement:*** Prepare a comprehensive statement describing your organisation's policies and practices with respect to the handling of personal data. Conduct internal reviews to ensure the accuracy of the statement. The OECD Privacy Policy Statement Generator can be of particular assistance for this phase.

4. ***Develop a simplified notice***: Develop a shorter, clearer notice that includes key information that will enable consumers to understand how their personal data is used and any rights they have with respect to the organisation's use of that information.

5. ***Test the usability of the notice:*** Conduct testing to ensure that readers of the simplified notice find it comprehensible and user-friendly.

6. ***Disclose the simplified notice:*** Prominently display the simplified notice on the organisation's website or otherwise distribute it so that it can be readily and easily accessed and read by an individual whose personal data may be used by the organisation. Where needed, ensure easy accessibility to the comprehensive statement for those who want complete details, or where its availability is indicated by the legal review.

OECD member countries welcome initiatives, such as the CIPL's "Ten Steps to Effective Privacy Notices," the US Government Notice Project, and the U.K. Fair Processing Notifications Research, which are paving the way for simplified privacy notices and provide assistance in completing the steps above.

IV. Conclusion

OECD member countries are encouraged to disseminate this Report and its annexes and foster the implementation of the recommendations by interested stakeholders. They are also encouraged to foster continued research and discussion to further help guide organisations in better communicating about their privacy policies and practices.

NOTES

1 See, www.oecd.org/dataoecd/39/13/1840065.pdf.

2 See, www.oecd.org/document/39/0,2340,en_2649_34255_28863271_1_1_1_1,00.html.

3 OECD, "Privacy Online: OECD Guidance on Policy and Practice", p. 29-31 (2003). Available at: www.oecd.org/document/49/0,2340,en_2649_34255_19216241_1_1_1_1,00.html.

4 The complete report is available at: www.informationcommissioner.gov.uk/cms/documentUploads/Fair%20Processing%20Notices%20Research%20Final.pdf. The study covered notices delivered in hard copy, on a website, and through the telephone.

5 Research also highlighted that the attitudes of data subjects contributed to the effectiveness of the notice.

6 See, www.informationcommissioner.gov.uk/cms/DocumentUploads/DP%20Forum%207%20June%2005.pdf.

7 The participating federal agencies are: the Federal Trade Commission; Board of Governors of the Federal Reserve System; Federal Deposit Insurance Corporation; Office of the Comptroller of the Currency; National Credit Union Administration; and Securities and Exchange Commission.

8 See, www.ftc.gov/privacy/privacyinitiatives/ftcfinalreport060228.pdf.

9 The Center for Information Policy Leadership was founded in 2001 by leading companies and Hunton & Williams LLP to examine privacy and information security issues from a business-process perspective while respecting civil liberties and privacy interests. See, www.hunton.com/Resources/Sites/general.aspx?id=45.

10 See, www.privacyconference2003.org/resolution.asp. The International Conference returned to the issue at its 26th meeting in Wroclaw Poland: http://26konferencja.giodo.gov.pl/data/resources/CromptonM_paper.pdf.

11 See, www.hunton.com/files/tbl_s47Details/FileUpload265/681/Berlin_Workshop_Memorandum_4.04.pdf.

12 See, http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2004/wp100_en.pdf.

13 See, http://www.privacy.org.nz/about-us/website-privacy-notice.

14 See, www.oipcbc.org/website_policy.htm.

15 See, www.usps.com/homearea/docs/privpol.htm?from=home&page=0080privacy.