OECD publishing

Please cite this paper as:

OECD (2013-10-11), "Privacy Expert Group Report on the Review of the 1980 OECD Privacy Guidelines", *OECD Digital Economy Papers*, No. 229, OECD Publishing, Paris.
http://dx.doi.org/10.1787/5k3xz5zmj2mx-en

OECD Digital Economy Papers No. 229

Privacy Expert Group Report on the Review of the 1980 OECD Privacy Guidelines

OECD

FOREWORD

This document describes the work of the Privacy Experts Group of the OECD Working Party on Information Security and Privacy (WPISP). The expert group was tasked by the WPISP to assist with the review of the OECD Privacy Guidelines. The document also includes an Annex that identifies a number of issues that were raised by the Expert Group but not fully addressed as part of the review process. These issues could be considered as candidates for possible future study.

The work of the expert group played an essential role in a process concluded on 11 July 2013 with the adoption by the OECD Council of the first revisions to the OECD Privacy Guidelines since their original release in 1980. The revised Guidelines and additional information about the review are available at: www.oecd.org/sti/ieconomy/privacy.htm.

The Committee for Information, Computer and Communications Policy agreed to make this expert group report public through a written process that concluded on 30 August 2013.

TABLE OF CONTENTS

REPORT ON THE WORK OF THE WORKING PARTY ON INFORMATION SECURITY AND PRIVACY GROUP OF PRIVACY EXPERTS IN CONNECTION WITH THE REVIEW OF THE 1980 OECD PRIVACY GUIDELINES

The review of the OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data ("Privacy Guidelines" or "Guidelines") arises out of the Seoul Declaration for the Future of the Internet Economy, which was adopted by Ministers in June 2008. The Seoul Declaration calls for the OECD to assess the application of certain instruments, including the Privacy Guidelines, in light of "changing technologies, markets and user behaviour and the growing importance of digital identities."[1]

The OECD Working Party on Information, Security and Privacy (WPISP) convened a multi-stakeholder group of experts to assist in the review process (the "Expert Group"). This Expert Group included experts from governments, privacy enforcement authorities, academics, business, civil society and the Internet technical community. The Expert Group was chaired by Jennifer Stoddart, Privacy Commissioner of Canada. Omer Tene was hired as a consultant to the Secretariat and has served as rapporteur to the Expert Group.

Preliminary work

Preparations for work for the review were conducted during 2010-11 in the context of the 30th anniversary of the Privacy Guidelines. The OECD organised three events on: *i)* the impact of the Guidelines; *ii)* the evolving role of the individual; and *iii)* the economic dimensions of personal data and privacy. It also produced two reports "The Evolving Privacy Landscape: 30 years after the OECD Privacy Guidelines", and "Implementation of the OECD Recommendation on Privacy Law Enforcement Co-operation", that serve as useful references for the review of the Guidelines. This material is available on the OECD website at: www.oecd.org/sti/privacyreview.

The OECD Working Party on Information Security and Privacy (WPISP) agreed on a process for conducting this review at its meeting on 2-3 December 2010. With the assistance of the Expert Group, a questionnaire was prepared as the first step in its review. The goal of the questionnaire was to gain an understanding of whether: *i)* the objectives (or "vision") that motivated member countries to develop Guidelines are consistent with member country views and priorities today; *ii)* the strategy reflected in the Guidelines for accomplishing those objectives remains appropriate; and *iii)* the policy principles reflected in the Guidelines are well tailored to accomplish those objectives in the current context.

The OECD circulated the questionnaire in February 2011 and received 19 responses from 16 member countries, as well as BIAC, CSISAC, and ITAC. It also received an opinion from the Bureau of the Consultative Committee of Convention 108 of the Council of Europe.

The terms of reference

Building on the preparatory work, responses to the questionnaire, and the June 2011 Communiqué on Internet Policymaking Principles,[2] a Terms of Reference document was prepared to memorialise the results of the review at that point, and provide orientation for further Expert Group discussions. The Terms of Reference articulate a shared view about current issues and approaches and provide the rationale for further work, concluding with a set of questions about the principles to guide the future work.

The Terms of Reference highlight that, as compared with the situation 30 years ago, there has been a profound change of scale in the role of personal data in our economies, societies, and daily lives. The environment in which the traditional privacy principles are now implemented has undergone significant changes, for example, in:

- The ***volume*** of personal data being collected, used and stored;
- The ***range of analytics*** providing insights into individual and group trends, movements, interests, and activities;
- The ***value*** of the societal and economic benefits enabled by new technologies and responsible data uses;
- The extent of ***threats*** to privacy;
- The ***number and variety of actors*** capable of either putting privacy at risk or protecting it;
- The ***frequency and complexity of interactions*** involving personal data that individuals are expected to understand and negotiate; and
- The ***global availability*** of personal data, supported by communications networks and platforms that permit continuous, multipoint data flows.

The Terms of Reference also highlight that OECD members already agree on a number of elements that are key to improving the effectiveness of privacy protections. These include, for example, making global privacy frameworks more interoperable; elevating the importance of privacy to the highest levels in governments through national privacy strategies; better equipping privacy enforcement authorities to work co-operatively across borders; cultivating a culture of privacy in organisations and individuals; embedding privacy by design into privacy management processes, and more.

The Committee for Information, Computer and Communications Policy declassified the Terms of Reference by a written process that concluded on 20 October 2011. The Terms of Reference were released at an OECD conference on Privacy Frameworks in Mexico City on 1 November 2011 and packaged together with materials from the 30th Anniversary in a booklet distributed there and available on the OECD website.[3]

Work of the expert group

Following the Terms of Reference, the Expert Group addressed a number of issues bundled around the following themes:

- The roles and responsibilities of key actors;
- Geographic restrictions on transborder data flows; and
- Proactive implementation and enforcement.

The Expert Group met in person five times between December 2011 and May 2012. For each meeting the Rapporteur, working with the Secretariat, prepared short discussion papers. Typically these papers included a set of proposals for possible changes to the Guidelines along with statements of supporting rationale.

At the first meeting the Expert Group discussed three background papers prepared by the Rapporteur, one covering each of the three main themes identified in the Terms of Reference.

The theme discussed at the second meeting was "proactive implementation and enforcement," and the proposals covered: *i)* organisational accountability; *ii)* security breach notification; and *iii)* strengthening enforcement.

At the third meeting, the theme discussed was "the roles and responsibilities of key actors," and the proposals discussed were on: *i)* the role of the individual*; ii)* the importance of education and awareness; and *3)* the role of consent.

The theme discussed at the fourth meeting this meeting was "geographic restrictions on data flows," and the proposals discussed covered: *i)* the rules governing transborder data flows; and *ii)* strengthening remedies.

The last meeting was held in May 2012 at the OECD, immediately prior to the WPISP meeting. At that meeting the Expert Group considered a complete set of proposals, covering all the areas previously discussed.

A complete record of the work of the Expert Group is available on the workspace, which has been open to any WPISP delegate for review and comment. It includes all draft proposals, comments received, meeting agendas, participant lists, and discussion summaries. It also includes references to developments in other international organisations and specific country developments. These references assisted the discussion within the Expert Group, by highlighting ideas and approaches reflected in the review processes which are currently ongoing around the world.

Approach and outcome of the work of the expert group

The Expert Group prepared proposals to update the OECD Privacy Guidelines in several key areas. The proposed revisions introduce a number of new concepts to the Guidelines, such as privacy management programs, security breach notification, national privacy strategies, education and awareness, and global interoperability. Other proposed revisions expand or update portions of the 1980 Guidelines such as accountability, transborder data flows and privacy enforcement.

The proposals by the Expert Group leave intact the eight "basic principles of national application" intact as reflected in Part Two of the 1980 Guidelines, as well as the definitions of key terms like "data controller" and "personal data". While the group has considered many issues that implicate these core principles and terms (see below), no clear direction emerged as to what changes might be needed at this stage.

In addition to these proposed modifications, the Expert Group prepared a new, supplemental explanatory memorandum. It includes an introduction that describes the context and process for the review. It then explains the rationale for the changes proposed to the Guidelines. It only covers the proposed modifications to the Guidelines and in that sense is intended only to supplement rather than replace the original explanatory memorandum prepared contemporaneously with the Guidelines in 1980.

The Terms of Reference identified a number of issues as important to member countries, not all of which resulted in proposals for changes to the 1980 Guidelines. Additional issues were also raised during the course of the review which likewise are not fully reflected in proposed revisions to the Guidelines. The following annex is a non-exhaustive accounting of these issues, which may serve to inform possible future study and discussion.

ANNEX

Issues identified for possible further study

The role of consent

In Alan Westin's canonical conceptualisation, privacy is framed as an individual's control over personal information. Under the 1980 Guidelines, consent is not a necessary requirement for personal data processing to take place. The role of consent is, however explicitly mentioned in several instances. The "collection limitation principle", for example, states that "data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject."

Many national laws, privacy enforcement authorities and data controllers place considerable emphasis on consent. By emphasising transparency and user consent (or "notice and choice"), current data protection frameworks may sometimes unduly burden both businesses and individuals. Some argue that the role of consent should be demarcated according to normative choices made by policymakers with respect to prospective data uses. In some cases, consent should not be required; in others, consent should be assumed subject to a right of refusal; in specific cases, consent should be required to legitimise data use. Others argue that individuals should be given more rather than less control over their personal data.

Specific concerns are raised by the use of consent in circumstances where there is a clear imbalance in the bargaining power of the parties, such as by employees in the workplace. Consent in these cases seems vacuous and its use by data controllers opportunistic. At the same time, for certain types of data processing consent seems essential (e.g., medical research); and consent is so intertwined with the concept of privacy that disentangling the two terms appears daunting.

In considering this issue going forward, the following questions merit further analysis:

1. Does the role of consent within the current framework need to be re-evaluated? Are there ways to improve the process through which consent is obtained or otherwise give individuals more control?

2. Should certain uses of personal data be authorised to facilitate a societal good, thereby minimising the role of individual choice? If so, should individuals be provided with an opt-out or should societal norms sometimes trump individual choice?

3. What are the appropriate boundaries of consent? Are there certain types of data usage which individuals, even when knowingly consenting, should be unable to authorise?

The role of the individual

When the 1980 Guidelines were adopted, the main collectors of personal data were governments, businesses and research institutions. They reflect a model where a data controller actively collected personal data from a data subject, sometimes using a third party ("agent") to process the data on its behalf. As such, the 1980 Guidelines focus, to a large extent, on the relationship between data controllers and data subjects.

Advances in information and communication technologies now allow individuals to engage with what is effectively an unlimited audience. While a leap forward in terms of individual empowerment, these new forms of communication also facilitate privacy-intrusive uses of information. As a result, individuals' privacy interests are threatened not only by public and private organizations, but also by their peers.

Furthermore, individuals may inadvertently impact their own privacy when using these new forms of communication (e.g., by disseminating content in ways they come to regret). The rise of social networking services and the ubiquity of mobile devices with internet connectivity are just two factors which have fundamentally changed the role of individuals.

While these new services have become as powerful as traditional databases, which large institutions populate and centrally define, governments cannot possibly impose on individuals the same type of restrictions and administrative burdens that are reasonably placed on businesses or government departments. Furthermore, applying these restrictions to the activities of individuals could easily become an unwarranted and dangerous constraint on individuals' freedom of thought, expression and association. At the same time, individuals should be in a position to take action if their privacy interests are adversely affected, even by one of their peers.

The proposed revisions to the guidelines call upon member countries to "consider the role of actors other than data controllers, in a manner appropriate to their individual role". This provision intends to make policymakers aware that there are other actors who, while not covered by the concept of data controller, nevertheless influence the level of protection of personal data. While this provision provides one basis for addressing the evolving role of the individual, additional analysis is necessary to determine which measures (beyond awareness raising) may be appropriate.

Questions for further consideration include:

1. Are there "good practices" that could help inform the use and dissemination of personal data by private individuals online? What constitutes 'reasonable use' of personal data by peers? Where do the boundaries lie?

2. What remedies should be available to individuals who wish to object to the use of their personal data by their peers? How can different types of data controllers facilitate the exercise of data subject rights?

3. Should certain technical means which could help individuals make better informed decisions be promoted? For example, should individuals be given feedback about their choices to share certain information (e.g., by showing them the size of the audience for information they are about to disclose)?

The role of purpose specification and use limitation

The use of personal data in ways that an individual did not anticipate at the time of data collection may violate that individual's sense of privacy. Very often, the context in which information is collected is determinative for the individual's expectation of how information will be used. At the same time, certain secondary uses of personal data may yield substantial benefits to society. Examples include advances in medical science, greater energy efficiency, and improved fraud prevention. Many of these applications, however, involve making use of personal data in ways not envisaged at the time of collection. As such, these practices appear at odds with two basic principles of the 1980 Guidelines, namely purpose specification and use limitation.

The 1980 Guidelines recognise that the purpose for which data is collected and used may change over time. Such a change of purpose should, however, only take place either with the consent of the data subject or by the authority of law (use limitation principle). The Explanatory Memorandum further specifies that "new purposes should not be introduced arbitrarily; freedom to make changes should imply compatibility with the original purposes". While this wording suggests flexibility where the new use may

be considered "compatible" with the original purposes, it does not readily accommodate new uses which are completely distinct from those purposes.

The use limitation principle implies that, in the absence of a legal basis which authorises the processing, all new uses of personal data require data subject consent. A rigid application of this principle may have undesirable consequences. First, this approach may unduly restrict certain re-uses of information which are deemed beneficial to society. Second, requiring data controllers to obtain consent from every individual concerned may impose a significant burden, particularly where the data relates to a large number of individuals, or where such individuals are not directly identified. On the other hand, individuals retain a legitimate privacy interest in limiting the usage of data relating to them. Furthermore, not every secondary use is necessarily "beneficial to society". Without clear limitations, personal data may easily be reused in ways that individuals find objectionable that do not serve any larger societal benefit.

Given the increase of potential applications of personal data, a number of questions related to the role of purpose specification and use limitation merit further consideration, among which:

1. Do the principles of purpose specification and use limitation unduly restrict uses of data which are beneficial to society? Should these principles be balanced against innovation and value creation?

2. Should there be strict limits regarding the re-use of personal data? Or should more flexible standards be applied, such as 'balance of interests' or 'fairness'? Should specific forms of acceptable re-use be specified in national laws, or should regulators try to carve out 'acceptable re-use principles'?

3. To what extent can anonymisation or other privacy enhancing technologies help strike the balance between individuals' privacy interests and government or business interests in re-use?

The definition of personal data

The Guidelines define "personal data" as "any information relating to an identified or identifiable individual". Data which are not personal data are outside the scope of the Guidelines. Hence, anonymisation and de-identification techniques are often advanced as means to enable prolonged retention, repurposing and/or analytics, while at the same time preserving privacy. Over the past decade, however, it has become clear that not all anonymisation and de-identification techniques are equally robust. As a result, the use of these techniques to eliminate privacy risks is increasingly questioned.

Some have argued that the nature of data as personal or not should be viewed as a continuum as opposed to the current binary. This could for example mean that data, which are only identifiable at great cost, would remain within the scope of the Guidelines, yet trigger the application of only a subset of the basic principles in Part Two. For example, providing a right of access and rectification with respect to data that are not readily identifiable could inadvertently increase privacy risks by requiring data controllers to authenticate identities and (re-)identify data to a greater extent.

Questions for further consideration include:

1. What role should anonymisation and de-identification techniques play where re-identification may remain a persistent risk? Are there other approaches which more effectively preserve privacy?

2. Should the binary distinction between "identifiable" and "non-identifiable" data be approached as a continuum recognising different degrees of identifiablity? If so, how would the degree of identifiability be measured?

Other issues

In addition to the issues highlighted in the previous paragraphs, the following issues were identified as being worthy of further consideration by members of the Expert Group:

- The *definition of data controller*: should this definition be updated, in light of increased diversification and cross-organisational collaboration in data usage?

- The role of *other actors (e.g. system designers)*: should the role of actors other than data controllers be better reflected in privacy frameworks? If so, to what extent?

- The *principle of collection limitation*: should this principle be revised to be more precise? Should additional efforts be made to adopt technological means which both minimise the amount of information collected and increase the control of individuals? How would this operate in the context of increasing capacity for valuable re-use?

- The need for *time limits on the storage of personal data*: should a new principle be introduced calling for the deletion of personal data once the purpose(s) for which they have been collected has been achieved?

- The *openness principle*: should the duty of data controllers to provide information be enhanced to provide greater transparency, particularly in a general context of much broader data use? Should data controllers be required to provide access to data in usable format?

- The principle of *individual participation*: should the Guidelines specify additional criteria to determine how "challenges" from data subjects should be resolved?

NOTES

[1] See, www.oecd.org/dataoecd/49/28/40839436.pdf.

[2] See, www.oecd.org/dataoecd/40/21/48289796.pdf.

[3] See, www.oecd.org/dataoecd/63/56/49710223.pdf.