RETHINKING THE CONCEPT OF INFORMATION PRIVACY: A JAPANESE PERSPECTIVE

Yohko Orito and Kiyoshi Murata

Abstract

On 1 April 2005, the Japanese government enforced Act on the Protection of Personal Information (APPI) with the aim of protecting personal data. However, APPI itself has led to numerous disputes and overzealous interpretations. This response may have occurred not only as a result of social, cultural and economic circumstances, but also because APPI is not appropriate for use in a society in which large amounts of personal data have already been collected, stored, used, shared and circulated.

In this article, we reconsider the concept of personal privacy and propose, from a Japanese perspective, a definition of this right that is suitable to the modern information society. This requires answering the following questions. Who owns the personal data that are collected, stored and used by an organisation? Is it acceptable to reconsider the concept of information privacy based on a certain socioeconomic context?

1 Introduction

The concept of the right to personal privacy was born in the United States during the late of the 19th century when Warren and Brandeis [1890] defined it as “the right to be let alone”. This classic definition reflected the rampant journalism of the time, which was often based on gossip. The advent of information and communication technology (ICT) and its penetration of society have altered the classic understanding of the right to privacy. Today, this right has come to mean the right to information privacy, or the right of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others [Westin, 1967]. This definition implies a close relationship between privacy and personal data, although the protection of personal data is not equivalent to the protection of privacy. Actually, information privacy legislation usually centres on the regulation of the collection, storage, processing, use and circulation of personal data.

In developed countries, the right to information privacy seems to be acknowledged as a universally accepted human right. Indeed, in this information age, protection of this right serves as a basis for freedom of thought and speech and the autonomy of individuals. In view of the circumstances surrounding the right to information privacy and the fact that massive amounts of personal data are collected, stored, processed, transferred, shared and

used by organisations, it has become a matter of urgency to enact legislation protecting this right in both the private and public sectors. One useful reference for such legislation is the Organisation for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data [OECD, 1980] based on Westin's [1967] definition of the right to information privacy. In fact, Japan's Act on the Protection of Personal Information (Act No.57 of 2003; hereafter APPI, or protection act), which enforced on 1 April 2005, corresponds to the OECD guidelines.

However, is it justifiable that APPI corresponds to the OECD guidelines? Is APPI, and Westin's [1967] definition of the right to privacy, appropriate for the modern information age? In fact, APPI's passage has brought about confusion concerning the protection of personal data in Japan, which has made us question the effectiveness of APPI, the OECD guidelines and the definition of the right to information privacy.

In this article, we reconsider the concept of information privacy and propose, from a Japanese perspective, a definition of this right that is suitable for the modern information society. This requires answering the following questions. Who owns the personal data that are collected, stored and used by an organisation? Is it acceptable to reconsider the concept of information privacy based on a certain socioeconomic context?

In the next section, we describe some of the confusion surrounding APPI and examine the effectiveness of the concept of information privacy in the Japanese socioeconomic context. In Section 3, we discuss the need to rethink the concept of this right and propose a revised concept. Finally, we consider the meaning of this revised concept in a global context.

2 The Right to Information Privacy in the Japanese Socioeconomic Context

2.1 Overzealous Interpretations of APPI

Japan enacted a law on personal data protection for the public sector in 1988, but until recently, entrusted the private sector to self-regulation. As a result of external pressure from the international community, such as Directive 95/46/EC on the processing of personal data [European Parliament and the Council of the European Union, 1995], on 1 April 2005, Japan enforced APPI, a law applying to both the public and private sectors. APPI regulates "entities handling personal information" (individuals and organisations that handle the personal data of more than 5,000 individuals) and requires them to undertake measures to ensure the proper handling of these data. APPI's introduction and its associated punitive clauses have raised awareness among both individuals and

corporations of the need to address personal data protection and to spread awareness about the protection act.

This response has led to mixed results, including excessive rigidity in interpreting APPI. This was highlighted by the JR Fukuchiyama train disaster on 27 April 2005. To abide by the act, hospitals refused to disclose information on the names and conditions of the victims. Consequently, victims' relatives were unable to acquire vital information about their loved ones.

APPI has also brought about confusion. For example, some citizens, students and parents have refused to provide personal data for community membership lists or student lists [National Consumer Affairs Center of Japan, 2005]. These people arbitrarily assumed that they had the right of refusing to provide personal data based on APPI. Some people have refused to fill out the census form on the authority of the protection act, although APPI does not apply to the census. Moreover, to comply with APPI, several local governments have refused to reply to the enquiries of defendants who are engaged in lawsuits.

These cases suggest that overzealously adhering to APPI has resulted in losing sight of its original objectives; the protection act presumes the usefulness of personal data and intends to promote the use of personal data counterbalanced with their protection.

Japanese firms' efforts at personal data protection are a form of "cold feet" compliance; firms hesitate to do anything that is questionable, if though it would be legal. Ambiguous expressions in certain clauses of the protection act reinforce this tendency. Indeed, since its enforcement on 1 April 2005, no firm has been prosecuted for any violations. Companies struggle to avoid any damage to their reputation that might be incurred by being the first defendant brought to trial. In fact, many Japanese firms are believed to have spent significant amounts of money setting up schemes for compliance.

2.2 Japanese Socioeconomic Circumstances Surrounding Personal Data Protection

De George [2003:40] wrote that culture affects the notion of privacy; different societies have different views about what constitutes privacy, how important it is and to what extent it needs or deserves protection. For example, many Japanese use the word puraibashi, an adopted word for privacy, without clearly understanding its meaning [Murata, 2004]. Compared to Westerners, owing to sociocultural and linguistic characteristics, the Japanese often consider the right to privacy as being a subjective and timeserving concept, and attach less importance to this right and to the protection of

personal data [Orito and Murata, 2005]. This has led the Japanese to consider that protecting the right to information privacy is equivalent to abiding by APPI. In this regard, the aforementioned excessive responses to the protection act may reflect the Japanese people's lack of interest in, and understanding of, the right to privacy.

However, it is doubtful that APPI conforms to the Japanese business situation. Most Japanese firms design, construct and operate their business processes on the premise of the availability of ICT, especially database and network technology. Many Japanese firms have built and maintained individual customer databases over the years and have utilised these databases with flexible database management systems to make their business operations more effective and efficient and to attain a high level of customer satisfaction. The sharing of personal data digitally among partner firms has recently become one of the most promising ways of constructing successful virtual business organisations. ICT has irreversibly transformed the concept of the business organisation and the way businesses are managed. Government services are starting to be provided via the Internet using personal authentication systems. Individuals also enjoy customised goods and services that firms using ICT can provide by analysing customers' preferences, desires and past service use. In light of these circumstances, if organisations behave in an excessively risk-averse manner with respect to personal data handling in order to comply with APPI, the quality of the goods and services they provide will be significantly undermined.

2.3 Effectiveness of the Concept of the Right to Information Privacy in Japan

The present realities of ICT and the digital processing and circulation of personal data could not have been imagined in 1967 when Westin defined the concept of the right to information privacy or even in 1980 when the OECD released its guidelines. It is said that the development of ICT, which has been described in dog years, outpaces that of other technologies sevenfold. Therefore, legislation for the protection of the right to information privacy based on OECD guidelines or Westin's [1967] definition may be unreasonable, and APPI, which adheres fundamentally to the OECD guidelines and thus endorses Westin's [1967] definition, may already be outdated.

In fact, the Japan Federation of Bar Associations [2006] proposed a revision of the protection act. The proposal suggests adding statements to clarify the interpretation of APPI and to stipulate the importance of achieving a favourable balance between the protection and use of personal data.

Westin [1967] proposed the concept of the right to information privacy in a technological environment in which large firms and governments collected, stored and used personal

data mainly within the organisations, and thus, the circulation of personal data was limited compared to the present day. Now it is very difficult for people to control the flow of their personal information; a massive amount of personal data, including personally identifiable information, has already been (and is still being) collected and stored in digital form in private and public databases. The fact that digital data can be copied losslessly, transferred to other entities and easily matched to other data reinforces the uncontrollability of the distribution of personal data.

In this regard, Westin's [1967] definition of the right to information privacy is inappropriate for the modern information society. Moreover, if this definition were applied to a law enacted for the protection of personal data or information privacy, the law might even become harmful to society; the concept of information privacy implies that an individual has the right to control the circulation of his or her own data. However, if a significant number of people were to exercise their right and call on organisations to verify the presence and accuracy of their personal data, the ordinary activities of these organisations would be disabled and the quality of the services the organisations provided would deteriorate.

In general, an ineffective and unrealistic concept of a right in a society tends to result in contempt for the right itself as well as for the importance of that right in the society. In this respect, reconsidering the concept of the right to information privacy is an urgent issue in Japan. Considering the irreversibility of ICT in business and society, we should consider the concept based on the present technological situation.

3 Rethinking the Right to Information Privacy

3.1 Who Owns Personal Data?

Usually, personal data are presumed to be owned by the data subjects. Based on this idea, the OECD guidelines stipulate the Individual Participation Principle as follows [OECD, 1980].

> An individual should have the right:
> a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
> b) to have communicated to him, data relating to him within a reasonable time;
> at a charge, if any, that is not excessive;
> in a reasonable manner; and
> in a form that is readily intelligible to him;
> c) to be given reasons if a request made under subparagraphs(a) and (b) is denied,

and to be able to challenge such denial; and

d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

However, in a highly networked society, the rights described in this principle cannot be ensured by individual data subjects because of their inability to determine the locations of, and to control the circulation of, their personal data. To compensate for this inability, the organisations that store or use personal data for their business are expected to commit to managing and protecting personal data in a socially favourable manner of their own responsibility. Hence, a certain part of the right to information privacy or ownership of personal data should be relegated to those organisations that store or use personal data, the organisations must accept their fiduciary responsibility with respect to the use and protection of these data. As we noted previously, it is not realistic, and in fact may be harmful, in today's information society to allocate ownership of personal data exclusively to individual data subjects.

3.2 Proposal of a Revised Concept of the Right to Information Privacy

To justify the transfer of the right to privacy from individual data subjects to relevant organisations, a consensus must be reached on the rules to ensure the beneficial and favourable circulation of personal data. Subject to the establishment of these practical rules, the right to privacy could be defined as follows.

An individual should have the right:

1. to ensure that accurate and recent personal data are collected by relevant organisations,
2. to ensure that these data are stored in the databases managed by these relevant organisations,
3. to ensure that the stored data are protected from improper disclosure,
4. to ensure that the stored data are used to promote his or her own personal welfare, and
5. to terminate the use of personal data by these organisations.

These rights must be accompanied by the imposition of the following duties on relevant organisations or personal data management entities:

1. to collect accurate and recent personal data according to socially authorised rules;
2. to store these data;
3. to disclose, transfer and share the stored data according to socially authorised rules;
4. to use the stored data effectively to promote the individual's welfare, as evaluated against a socially authorised valuation standard;
5. to terminate the use of stored personal data upon request by the individual on rational

grounds through socially authorised procedures; and
6. to disclose the methods of personal data management according to socially authorised rules.

3.3 Rethinking Information Privacy in the Global Context

The revised concept of the right to information privacy proposed in the preceding section reflects Japanese socioeconomic circumstances, including the situation surrounding the enforcement of APPI. We should note that the revision is inevitably ethnocentric. This may evoke questions about the effectiveness of this revised concept in the global context because personal data can easily be transferred across borders in the current ICT environment.

However, the worldwide phenomenon of ICT and its widespread availability should more or less affect the effectiveness of Westin's [1967] concept of the right to information privacy in any country in the world. Therefore, the revision of the concept of this right could become mandatory for a wide range of countries, and the development of a globally acceptable concept of the right could be demanded. One way to do this may be to further revise the concept based on the social, cultural and economic circumstances in each country and then compare the revised concepts with one another. The revised concept proposed here is the first step towards the development of a globally acceptable concept of the right to information privacy suitable for the modern information age.

4 Conclusion

In view of the present situation in Japan, the conventional concept of the right to information privacy, as well as APPI based on this concept, is inappropriate and outdated. The revision of this concept is an issue of urgency. The revised concept proposed here includes the transfer of ownership of personal data from individual data subjects to relevant organisations along with the imposition of fiduciary responsibility upon the organisations.

Our proposal is made from a Japanese perspective. This may raise concerns about the effectiveness of the revised concept in the global context. However, because ICT is advancing on a global scale, the revised concept could become mandatory for a wide range of countries. Our proposal is the first step towards developing a globally acceptable concept of the right to information privacy that is appropriate for the modern information age. Societies could realise this concept through the integration of opinions about the right to such privacy based on local sociocultural and economic situations.

Acknowledgement

This study was supported by an Academic Frontier project for private universities entitled "Global Business and IT Management: Global e-SCM": a matching fund subsidy was provided by MEXT (the Ministry of Education, Culture, Sports, Science and Technology), 2002-2006.

References

De George, R.T. (2003), The Ethics of Information Technology and Business, Blackwell.

Japan Federation of Bar Associations (2006), Position Document Concerning Revision of the Act for Protection of Personal Data,
on line at www.nichibenren.or.jp/ja/opinion/report/data/kojin_joho.pdf accessed 16.01.2007

Ministry of lnternal Affairs and Communications, Japan(2006), White paper Information and Communications in Japan, online at
http://www.johotsusintokei.soumu.go.jp/whitepaper/eng/WP2006/2006-index.html accessed 16.01.2007

Murata, K. (2004), Is Global Information Ethics Possible? Opinions on the Technologically-Dependent Society, Journal of Information, Communication and Ethics in Society, 2(5): 518-519.

National Consumer Affairs Center of Japan (2005), A Trend and Problems Observed in a Recent Consultation Example Concerning Personal Data on line at
http://www.kokusen.go.jp/cgi-bin/byteserver.pl/pdf/n-20051107_2.pdf accessed 16.01.2007

OECD (1890), OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, online at
http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html accessed 16.01.2007

Orito, Y. and Murata, K. (2005), Privacy Protection in Japan: Cultural Influence on the Universal Value, Proceedings of ETHICOMP 2007.

The European Parliament and the Council of the European Union (1995), 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, online at
http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML accessed 16.01.2007

Warren, S. D, and Brandeis, L. D. (1890), The Right to Privacy, Harvard Law Review, 4 (5): 193-220.

Westin, A. F. (1967), Privacy and Freedom, Athneum.