NRI Papers No. 180 December 1, 2012

Privacy in Big Data Society

—Shifting from the Protection of "Personal Information" to the Protection of "Privacy"—

Shintaro KOBAYASHI, Taku YASHIRO, Tomohisa ITOH and Sawako OKUMI

Nomura Research Institute

NRI Papers No. 180
December 1, 2012

Privacy in Big Data Society

—Shifting from the Protection of "Personal Information" to the Protection of "Privacy"—

Shintaro KOBAYASHI, Taku YASHIRO, Tomohisa ITOH and Sawako OKUMI

Due to the widespread use of smartphones, the popularity of social media and the rise of big data business, it has become easier to identify specific individuals based on information that was previously regarded as being non-personal. Given this situation, Japan's Act on the Protection of Personal Information has become insufficient to ensure the protection of privacy.

Incidents involving invasions of privacy have occurred both in Japan and overseas. While seen as a transient problem in Japan that was caused by the rapid spread of smartphones, the activities of global companies such as Google can be construed as a challenge to the ways of protecting personal information and privacy, which requires a review of institutional and social mechanisms.

Japanese consumers are not particularly aware of the circulation of their personal information on the Internet, and so have little idea of how to safeguard their privacy. Instead, they tend to rely on the protective measures taken by service providers as well as those adopted by the government.

At the beginning of 2012, both the United States and the European Union (EU) announced revisions to their privacy legislation. While the U.S. is encouraging the industry's self-regulatory efforts, the EU is moving towards strengthening its legislation. Nevertheless, both the U.S. and the EU are moving to address the issues based on a similar awareness. The proposed regulations aimed at (1) behavioral targeting, (2) automatic profiling and the buying/selling of personal data and (3) the protection of children's privacy will also have a major impact on Japan.

To appropriately deal with the coming of big data society, there is a need to review the current protection system and enable a shift from the protection of "personal information" to the protection of "privacy" by implementing measures such as a "Privacy by Design" program. Enforcement of the My Number law, for which legislative proceedings are now underway, will be a touchstone in this regard. (My Number refers to an identification number for social security and taxation.)

With the widespread popularity of smartphones and social media, every day sees the generation of more and more personal data. While big data business is being promoted, invasions of privacy including the unauthorized use of data are frequent, leading to a sense of uneasiness in our networked society.

While big data is regarded as being an area of growth for the next generation information systems, one of the major challenges that the industry faces is the protection of privacy. In pursuit of "big data society" in which information about individuals can be safely used and provided, this paper points to the issues of "privacy" that do not fit into the scope of "personal information" and proposes ways of dealing with these issues. This proposal is based on a survey on changes in consumer awareness as well as on the trends in the governmental policies of Europe and the United States.

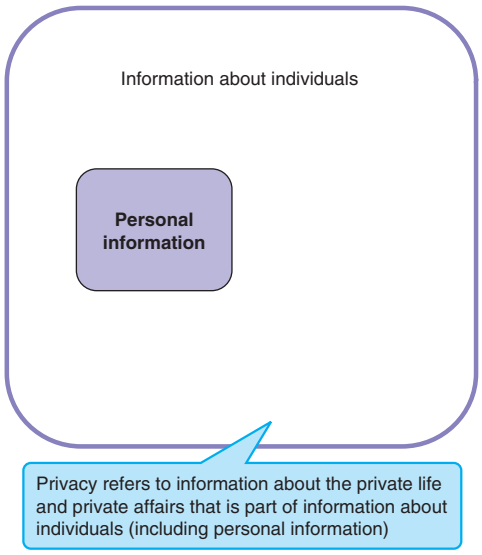
Because this paper makes a clear distinction between "information about individuals," "personal information" and "privacy," these terms are first defined and their relationship clarified (Figure 1).

"Information about individuals" is a term that refers to information related to an individual in the broadest possible sense.

"Personal information," as defined in Japan's Act on the Protection of Personal Information, is "information about a living individual that can be used to identify a specific individual by name, date of birth or other descriptions contained in such information (including information that can be easily matched to other information, thereby enabling the identification of a specific individual)."

While there is no statutory definition of "privacy," it is generally understood to refer to those matters related to the private life and private affairs of individuals or a household, or those matters that a person wishes to keep secret. Privacy refers to information about the private life and private affairs that is part of information about individuals (including personal information). Therefore, privacy and personal information do not constitute a one-to-one relationship.

Figure 1. Relationship between "information about individuals," "personal information" and "privacy"



I Protection of Personal Information Does Not Assure Privacy

1 Concerns about the failure to protect personal information still remain

When Japan's Act on the Protection of Personal Information came into effect in 2005, there was a degree of "overreaction" such as people saying that it would be impossible for a school to create a list of contact telephone numbers. Subsequently, the Act gradually came to be better understood, and has now become firmly established in our social lives as an important institution. In fact, according to a survey[1] conducted by the Consumer Affairs Agency, the number of complaints related to personal information and the number of cases involving a leak of personal information have both been on the decrease.

However, there remains considerable concern among consumers about the protection of personal information. According to a survey[2] conducted by the Ministry of Internal Affairs and Communications regarding concerns that responding consumers had in using the Internet, more than 70 percent answered that they "were worried about the protection of their personal information," with the percentage being on the increase when survey data in 2006 and 2010 are compared. As for the positioning of measures to protect personal information among businesses, a survey undertaken by the Ministry of Economy, Trade and Industry[3] revealed that more than 80 percent of responding companies answered either "these measures will become more and more important" or "these measures will remain highly important." Then, what is the issue that heightens consumer concerns over their personal information and that requires companies to continue to take measures of assurance?

2 Three Internet-related environmental changes

It is thought that consumers have become more anxious and companies more aware of the need for measures to protect personal information as a result of three Internet-related environmental changes.

(1) The rapid spread of smartphones

In fiscal 2011, shipments of smartphones exceeded those of ordinary feature phones for the first time. These

terminals have become a familiar sight in people's lives. Smartphones make it much more convenient to access the Internet. In addition to giving the user access to the Internet anywhere and at any time, the devices can provide services that are dependent on the user's location with a built-in GPS (global positioning system) function. As a result, smartphones accumulate huge amounts of personal information such as a list of telephone numbers, as well as browsing histories and even tracks of where the user has actually been, which constitute information related to privacy. As discussed in Chapter II, there have been many instances where apps (application software) have infringed on the user's privacy by inappropriately accessing such information.

(2) Increased use of social media

With the spread of smartphones has come the explosive growth of the use of social media mostly among the younger generation. Because Facebook, the world's largest social networking service (SNS) with more than one billion users, requires that users must use their real names, huge amounts of personal information are generated every day and are circulated between friends and acquaintances.

Generally, an SNS enables users to specify the scope of disclosure depending on the type of information they upload, such as "friends," "friends of friends" and "public." However, in some cases, the default setting for disclosure is "public." This has caused cases in which information uploaded as secret has become available for everyone to see.

(3) The rise of big data business

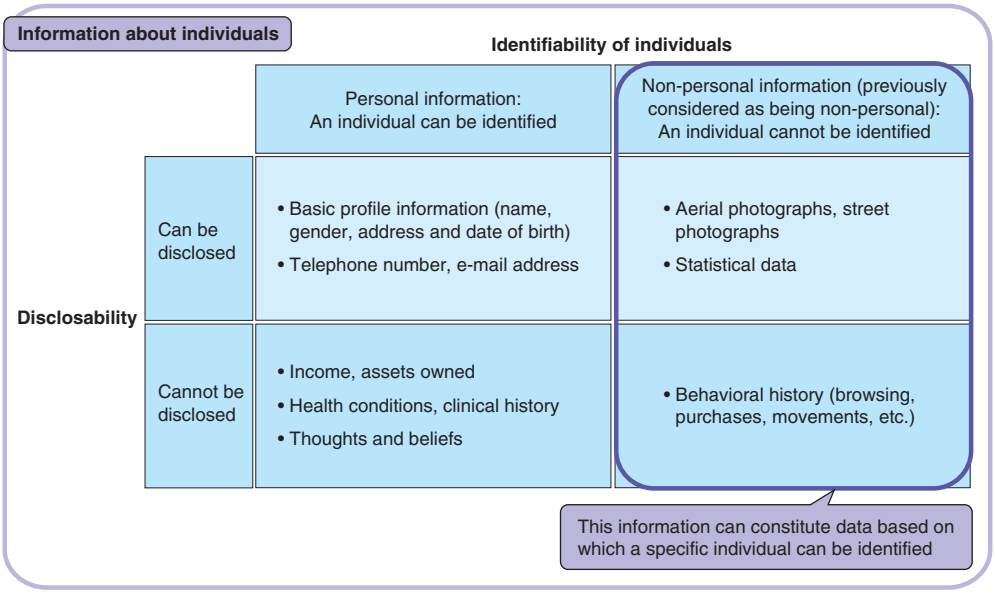
Big data business, which takes huge quantities of raw, unstructured data and processes it in order to extract information that could have significance for business, also presents a major threat to the protection of personal information and privacy.

In Japan's Act on the Protection of Personal Information, a distinction is made between personal and non-personal information based on "ease of matching" (whether the information can be easily matched with other information, thereby enabling identification of a specific individual). However, now, huge amounts of information about individuals, including information that was previously classified as being non-personal, flow on the Internet. Furthermore, we are approaching a society where big data business makes it possible to easily identify specific individuals by using such data (Figure 2).

For example, the addresses of crime scenes that are published in news articles can be identified by using the aerial photographs provided by online map services such as Google Maps. There have also been cases where the behavioral history data of a specific individual were identified by matching anonymized behavioral history data with data in a commercial database.[4] In addition, services have appeared that provide a profile of a specific individual (profiling services) by gathering an assortment of information that is found on the Internet.

Japan's Act on the Protection of Personal Information provides for the "protection of the rights and interests of individuals by protecting personal information." The protection of the rights and interests of individuals stipulated in this Act includes the protection of privacy.[5] However, for the following reasons, it is difficult for the Act to deal with the issue of privacy in big data society. Both private-sector companies and government bodies are required to take measures whose emphasis is shifted from the protection of personal information to that of privacy.

Figure 2. Examples of personal information and non-personal information (previously considered as being non-personal)



- It is difficult to make a clear-cut distinction between personal information and non-personal information.
- Even the non-personal data collected by Internet-based businesses could lead to an invasion of privacy.
- Non-personal information that circulates on the Internet without a person's knowledge can be used to profile that person or track his/her behavior.

II Invasion of Privacy in Big Data Society

1 Classification of recent instances of privacy infringement

With the rapid adoption of smartphones and the spread of social media, there have been many new instances of privacy infringement. The main causes of privacy infringement cases that have occurred over the last few years can be broadly classified into two patterns based on the awareness of the companies that have committed them (Table 1).

The first pattern stems from the rapid spread of new information terminals such as smartphones and a lack of awareness of privacy protection on the part of service providers. Among the companies providing application software (apps) for smartphones, there are many venture businesses, some of which may not have sufficiently considered matters of privacy. This is compounded by the fact that the rapid rise in the popularity of these new services has left the necessary institutional systems such as guidelines trailing behind. However, in response to the problems caused by these unknowledgeable companies, security software that can detect insecure apps for smartphones has been appearing, and a legal system is being developed to bring it into line with modern realities. That is, these cases are basically just a passing phase, and will gradually be eliminated.

The second pattern of incidents has its origin in service providers challenging the ambiguity of privacy as it exists in big data society. Even though major U.S. platforms such as Google and Facebook have been legally challenged concerning some of the new services that they have offered, they continue to boldly offer services that challenge the ambiguous area of privacy. To deal with these types of services, there is a need for basic institutional and social frameworks for protecting personal information and privacy.

2 Pattern 1: Cases of privacy infringement caused by service providers' lack of awareness

As examples of invasion of privacy that stemmed from service providers' lack of awareness, consideration is given to the cases of "Viewn" and "AppLog." Both cases are characteristic of big data society in that neither case involved existing personal information, but both cases invaded privacy by collecting non-personal information.

Viewn offers apps that enable users to subscribe to electronic newspapers and magazines on information terminals such as iPhone, iPad and Android for a flat fee. Problems arose in November 2011 when Viewn released an app that included a function of collecting the user's browsing history and terminal identification information without the user's consent (Figure 3).[6]

Viewn acquired users' browsing histories in order to distribute sales to the newspaper companies and magazine publishers that published the articles available through apps and collected terminal identification information to examine the eligibility for membership benefits for the first 30 days. Because it was not possible to identify individuals from the collected data, Viewn assumed that these data would not constitute personal information. In fact, it is actually very difficult to identify individuals from their browsing histories. However, if a user's browsing history that may contain a magazine (an

Table 1. Classification of major privacy invasion cases occurred in big data society

	Japan		United States	
Service name	Viewn	AppLog	Google Buzz	Facebook
Provider	Viewn	Milog	Google	Facebook
Problem	The newly released service had a function of collecting the user's browsing history without user consent and sending it to the server	The problem stemmed from not obtaining user consent or not providing a full explanation, and that content of information transmitted was not transparent to users	Without obtaining prior user consent, information provided for Gmail was used for other purposes such as for setting user names by default	Facebook changed its website so certain information that users may have designated as private was made public. The company did not notify users or get their consent in advance.
Pattern	These problems were caused by service providers' lack of awareness and insufficient security measures		These problems have their origin in service providers challenging ambiguous areas where there are no explicit laws and regulations	
	As a result of the rapid spread of smartphones, these cases have been occurring in a transient manner, and will gradually be eliminated with the spread of security software, etc.		There is a need for basic institutional and social frameworks for protecting personal information and privacy	

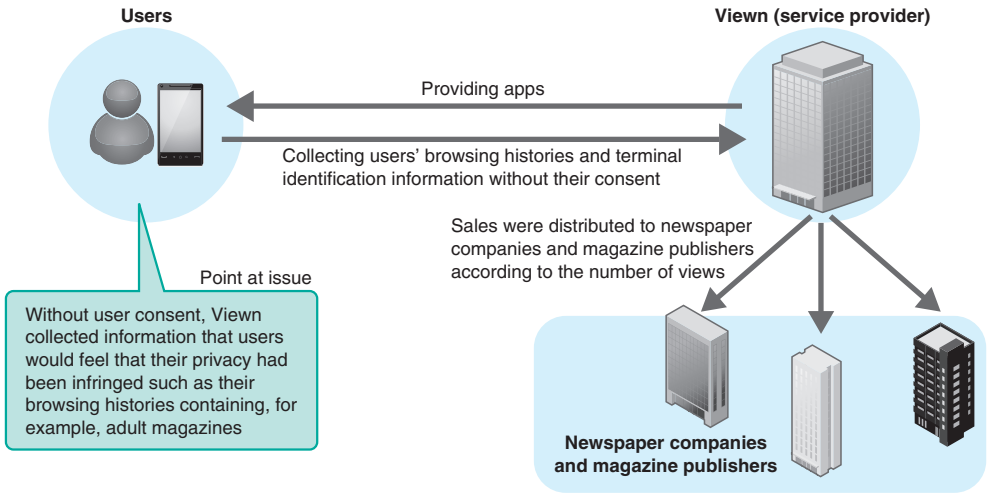
adult magazine, say), which the user does not want anyone else to know about, is obtained without his or her consent, the user would feel that his or her privacy had been infringed. After it was pointed out on websites that Viewn was collecting browsing histories without user consent, the company changed its Terms and Conditions, which now state that the service collects browsing histories and terminal identification information.

In the case of AppLog,[7] the problem stemmed from not providing a full explanation when obtaining user consent. Milog's AppLog is a program that is designed to monitor and record the use of apps that are installed on Android devices, with app developers incorporating AppLog into their products and being compensated by Milog depending on the number of times their app is downloaded. Meanwhile, Milog analyzes the user information that it obtains and sells the results to advertising agencies (Figure 4). Because of the effects of this privacy case, Milog went out of business in April 2012.

The problem with AppLog lay in the fact that when the use of an app into which AppLog was incorporated was first started, a simple message was displayed, stating that "terminal information is transmitted in order to optimize the delivery of advertising." In fact, without reading Milog's privacy policy, it was difficult to understand that AppLog gathered information on the use of all apps installed on the terminal, and this data was analyzed relative to the user's age group and gender. Because users were not aware that information was being collected on the use of every app on their terminal, they felt that their privacy had been compromised.

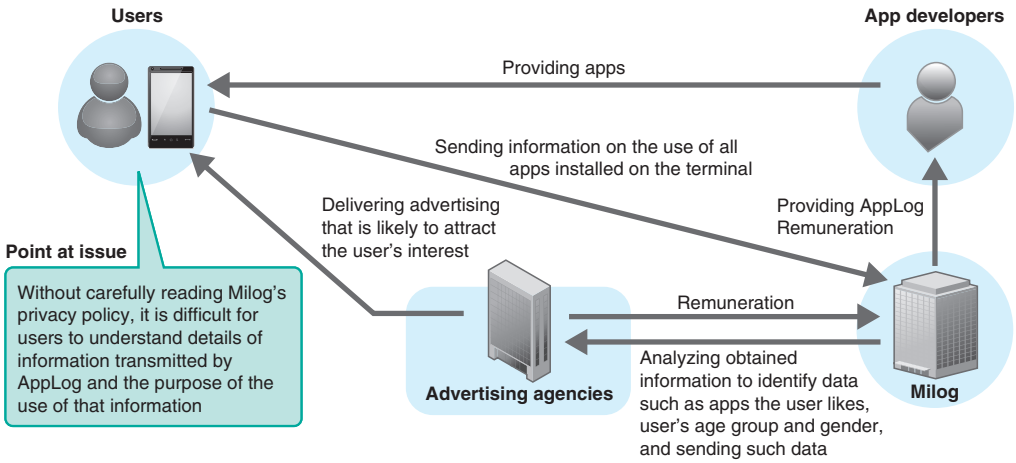
As described above, privacy issues can occur even with the collection of non-personal information in big data society. In particular, the cases described above were a result of the rapid spread of new information terminals such as smartphones, together with a lack of awareness of privacy issues on the part of service providers. However, Viewn and AppLog were not isolated

Figure 3. Problem with app "Viewn" provided by Viewn



Source: Compiled based on "Denshi shimbun/zasshi ni otoshiana, Viewn ya sankei ni yuza jyoho no shushu kino (A trap in electronic newspapers and magazines – Viewn and Sankei have a function to collect user information)," bizmash!, January 2012.

Figure 4. Problem with Milog's AppLog



Source: Compiled based on "Apuri riyo jikan ya kaisu maruwakari "AppLog" ni hihan (Fully acquiring information on the time during which an app is used as well as on the number of times an app is used: criticism of AppLog)," October 5, 2011, Asahi Shimbun.

cases—there are actually large numbers of apps that retrieve information from smartphones, etc., in a way that users might feel their privacy compromised. Unauthorized apps for Android devices, in particular, have proliferated since the second half of 2011, with more than 4,000 cases being identified only in 2011 (Figure 5).

Although these incidents present a big problem when they occur, it is possible to look forward to them being gradually eliminated by the spread of security software for detecting unauthorized apps on smartphones, as well as through the development of the legal system by the government and the establishment of rules by industry associations.

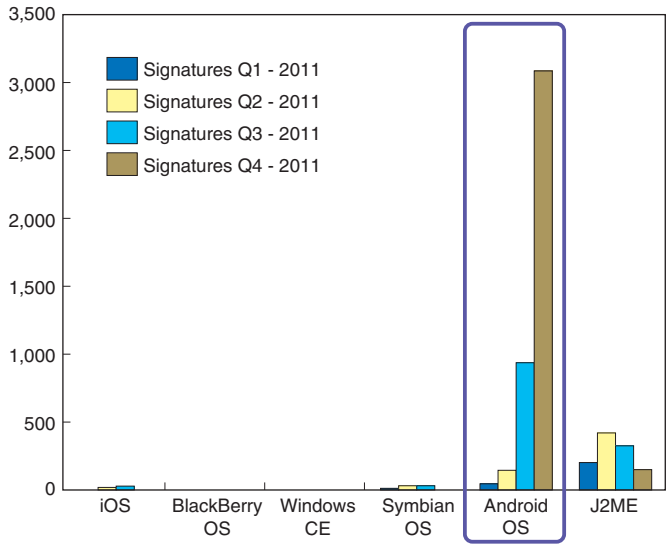
3 Pattern 2: Service providers challenging the legal system

As examples of companies that have challenged the legal system, a look was given at the cases of Google Buzz and Facebook.

In February 2010, Google launched its Buzz social networking service through its Gmail web-based email product. The problem that Google Buzz presented was that Google used information gathered from Gmail without obtaining the consent of users in advance.[8] When Google launched Buzz, its privacy policy stated that "When you sign up for a particular service that requires registration, we ask you to provide personal information. If we use this information in a manner different than the purpose for which it was collected, then we will ask for your consent prior to such use." However, Google used information provided for Gmail for another purpose—Google Buzz—without obtaining user consent in advance, which led users to feel that their privacy had been compromised (Figure 6).

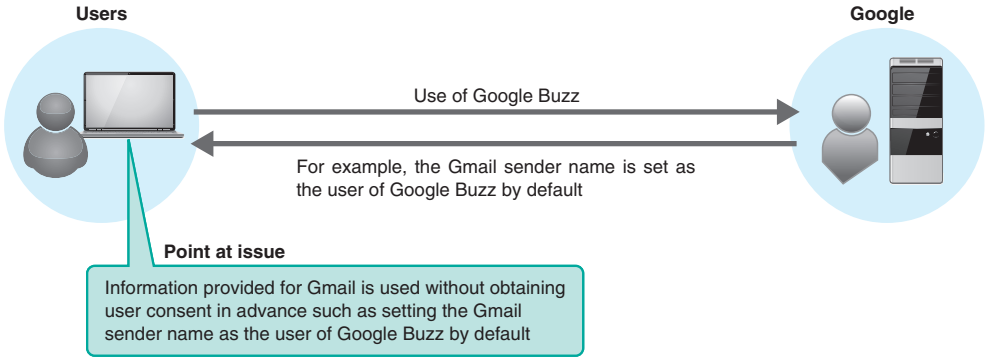
In December 2009, Facebook changed its website so certain information that users may have designated as private—such as their Friends List—was made public. They did not notify users that this change was coming, or get their consent in advance. In addition, Facebook

Figure 5. Number of mobile malware signatures



Note: Malware is short for malicious software (programs).
Source: Japan Smartphone Security Association, "Malware taisaku WG katsudo hokoku (Report on the Activities of the Malware Countermeasure WG)," 2012.

Figure 6. Point at issue with Google Buzz



represented that third-party apps that users installed would have access only to user information that they needed to operate. In fact, the apps could access nearly all of users' personal data—data the apps did not need.[9] A number of these instances led users to feel that their privacy had been infringed.

The U.S. Federal Trade Commission (FTC) charged that both the Google Buzz and Facebook services had caused harm to consumers through their "unfair or deceptive acts or practices," and required them to implement a comprehensive privacy program and undergo independent, third-party audits every two years for the next 20 years.

Despite the above-mentioned order by the FTC to implement corrective action, Google continues to challenge the ambiguous area of privacy. For example, in March 2012, the company switched from having separate privacy policies for each of its services to a single document, integrating user data from each service in order, it claimed, to provide a more personalized service.

In the same way as with Google, the FTC also ordered Facebook to implement corrective action. Nevertheless, year by year, Facebook has been expanding the scope of the disclosure of user information as default settings, to the detriment of privacy protection.

In response to service providers such as Google and Facebook that are constantly pushing the boundaries of privacy, there is a need for basic institutional and social mechanisms that can safeguard personal information and privacy.

III Consumer Knowledge of Privacy

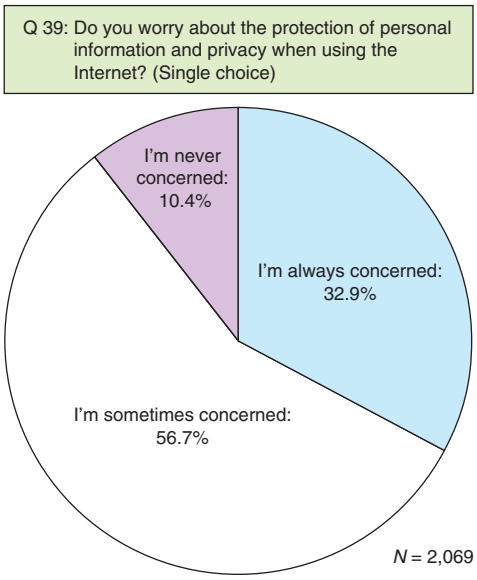
1 Young Japanese people are not sufficiently aware of the specific damage they could suffer

As described in Chapter II, there have been many incidents that could have led to invasion of privacy. Given this situation, what are the perceptions of consumers about the frequent occurrence of such incidents?

According to the results of a Questionnaire Survey on Information and Communications Services conducted by Nomura Research Institute (NRI) in July 2012, about 90 percent of responding consumers are either "always concerned" or "sometimes concerned" about the protection of their personal information and privacy when using the Internet (Figure 7).

On the other hand, according to Japan's Information Technology Promotion Agency (IPA), Japanese consumers (in particular, young people) are less aware of the external use of their personal information than are consumers in Europe. The comparison was made between the results of an Internet poll of Japanese people aged 15 to 25 conducted by IPA in 2010 and those of a similar survey done by the Institute for Prospective Technological Studies (IPTS),[10] targeting young people in four member countries of the European Union (EU), specifically, the UK, Germany, France and Spain (Figure 8). In response to the question about the possibility of "My personal information is used without my knowledge," 65 percent of young Japanese people responded that they were either "very concerned" or "somewhat concerned," while the figure was 82 percent for the European respondents. As such, regarding the external use of personal information, awareness in Japan was about 20 points lower.

Figure 7. Consumer perceptions about the protection of personal information and privacy when using the Internet



Source: Questionnaire Survey on Information and Communications Services conducted by Nomura Research Institute (NRI) in July 2012.

While many young Japanese people are aware of the fact that their personal information is used without their knowledge based on their online personal information, their perceptions about how their personal information may be used in specific situations are low. Such low levels of perceptions suggest that they have little idea of the degree of damage that they could possibly suffer.

2 Few young Japanese people take protective measures

The survey items explaining the specific content of the external use reveal that the perceptions of Japanese respondents are lower by about 30 points than of European respondents. These items are: "my identity is reconstructed using personal data from various sources," "my views and behaviors may be misrepresented based on my online personal information" and "my reputation may be damaged by online personal information." These findings suggest that in comparison with young European people, their Japanese counterparts are

less aware of the scope of specific effects that may be brought about when online personal information is used by others.

In addition, the proportion of young Japanese people who have taken measures to protect their own personal information is relatively low overall, as compared with their European counterparts (Figure 9).

Specifically, in response to questions as to whether they "read the privacy policy of websites," "use dummy email account to shield my identity," "erase cookies,[11]" "adapt my personal data so that no linking between profiles is possible," "change the security settings of my browser to increase privacy" and "use tools limiting the collection of personal data (e.g., firewall, cookie filtering)," the proportion of young Japanese who responded with "always" or "often" was lower than that of young Europeans.

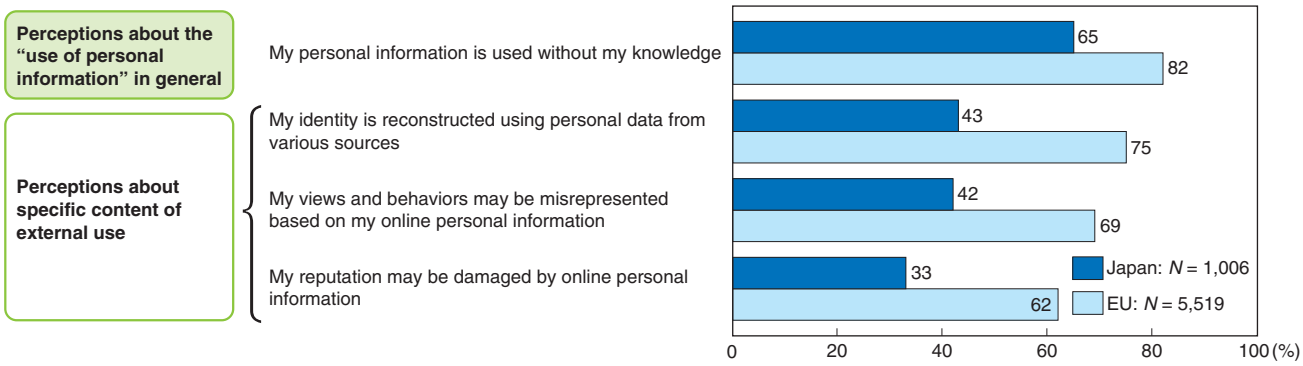
The only item where young Japanese respondents scored higher was in response to a question asking whether they "check that the transaction is protected or the site has a safety badge before I enter valuable personal data." This item relates to the security and safety measures that are employed by third parties, rather than by the users themselves.

3 Young Japanese people rely on others to protect their personal information

First, let's consider why, relative to young people in the EU, fewer young Japanese people implement measures to protect their personal information.

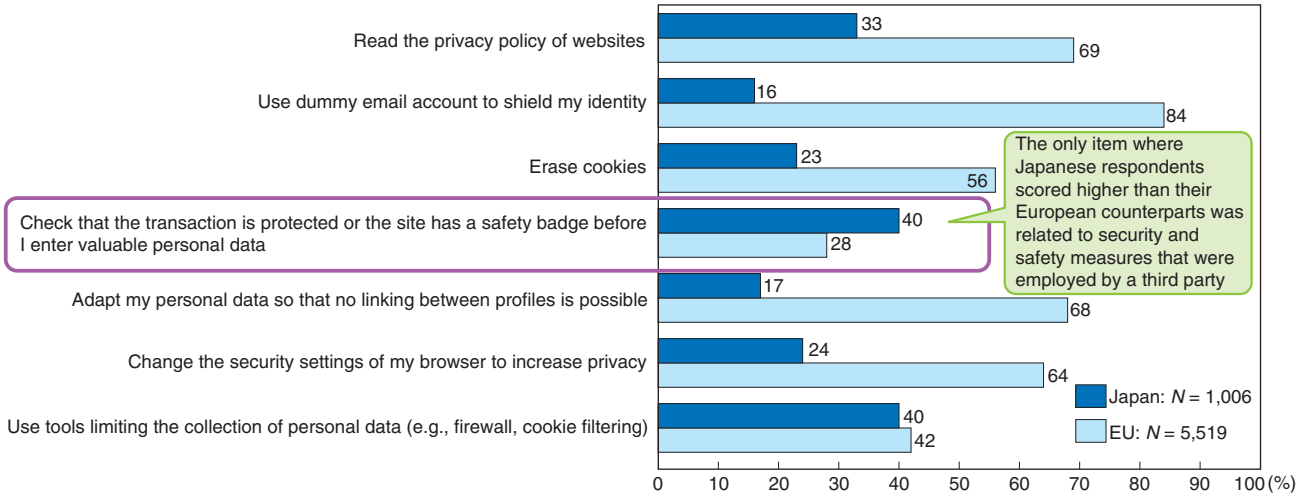
One factor to consider is that, compared to their counterparts in the EU, young Japanese people are very inclined to ascribe the responsibility for protecting their personal information to companies. As shown in Figure 10, in response to a question as to whether the responsibility to protect personal information should lie with companies, individuals, everyone in society as a whole, the government, or the courts, police and prosecutors, 40 percent of young Japanese people selected "strongly

Figure 8. Perceptions about the use of personal information among young people (comparison between Japan and EU)



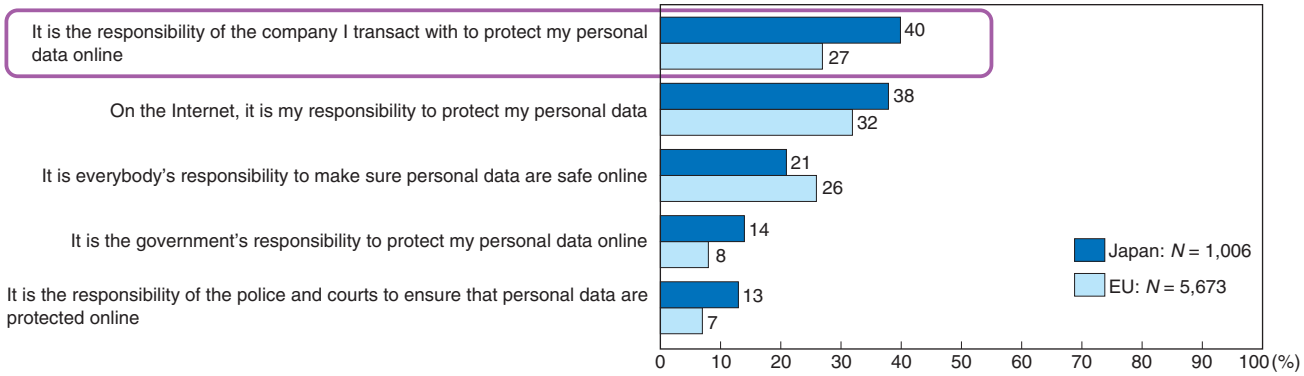
Note: Figures indicate the percentages of respondents who selected "very concerned" or "somewhat concerned."
Source: Compiled based on the "Report of the Survey on Perceptions and Acceptance of Risks concerning eID-related Security and Privacy" conducted by the Information Technology Promotion Agency (IPA) in August 2010, and "Young People and Emerging Digital Services: An Exploratory Survey on Motivations, Perceptions and Acceptance of Risks" conducted by the Institute for Prospective Technological Studies (IPTS).

Figure 9. Measures taken by young people to protect their personal information (comparison between Japan and EU)



Source: Compiled based on the "Report of the Survey on Perceptions and Acceptance of Risks concerning eID-related Security and Privacy" conducted by the Information Technology Promotion Agency (IPA) in August 2010.

Figure 10. Responses to the question "who is responsible to protect personal data online" (comparison between Japan and EU)



Note: Figures indicate the percentages of respondents who selected "strongly agree" or "agree."
Source: Compiled based on the "Report of the Survey on Perceptions and Acceptance of Risks concerning eID-related Security and Privacy" conducted by the Information Technology Promotion Agency (IPA) in August 2010.

agree" or "agree" for "companies should be responsible for safeguarding personal information"—fully 10 points more than that in the EU.

These findings clearly show that, compared to young people in the EU, young Japanese people are not as aware about protecting their personal information online by themselves. Instead, they place much more trust in companies to implement protection measures. This situation is a major source of concern about the protection of privacy, given the rapid increase in the number of incidents involving the invasion of privacy and the fact that many service providers are overseas companies that do not fall under the jurisdiction of Japanese law.

IV U.S. and EU Move to Strengthen Their Regulations

If we turn our attention to overseas, we find that the protection of privacy has become a pressing issue, and that efforts to review legislation are underway in both the United States and Europe. Although both regions are moving toward tighter regulations, their approaches are very different in that the U.S. is stressing self-regulation, while the EU is tending towards stricter governmental control. In this chapter, we will compare the main points of the new privacy laws proposed in the U.S. and the EU, while looking at three issues that need to be addressed in Japan.

1 The U.S.: Seeking to attain a balance between privacy protection and industrial development

Personal information protection legislation in the U.S. varies by industry or field, that is, it is "sector-specific," with no general law that corresponds to Japan's Act on the Protection of Personal Information. Two examples of such laws are:

(1) The Fair Credit Reporting Act (FCRA) in the area of credit information
(2) The Health Insurance Portability and Accountability Act (HIPAA) in the field of medical care

With the absence of any general law, the protection of personal information and privacy in those industries and fields that are not covered by a specific law has been entrusted to the discretion of businesses. Compared to Japan and the EU, both of which have general laws, the environment in which information about individuals can be used in the U.S. is relatively lax, perhaps pointing to the country's stance of giving priority to industrial development.

However, as pointed out in Chapter II, while businesses using information about individuals are thriving, the number of cases of consumer privacy being invaded has been increasing as is seen in the cases of Google and Facebook, which has led to a growing trend towards calling for stricter regulations. Faced with these circumstances, in February 2012, the Obama Administration announced a "Consumer Privacy Bill of Rights," which laid down consumer rights more clearly than before and which encouraged businesses to take self-regulatory measures.[12] Given that many privacy bills have been introduced in Congress, the announcement of this blueprint can be interpreted as a measure to avoid the imposition of new obligations and regulations on businesses by introducing the consumer bill of rights that has no legally binding effect.

The Consumer Privacy Bill of Rights defines seven rights for consumers online (Table 2). These rights include:

(1) Individual control: Consumers have a right to exercise control over what personal data organizations collect from them and how they use it.

Table 2. Outline of rights provided in the U.S.'s Consumer Privacy Bill of Rights

Individual control	Consumers have a right to exercise control over what personal data organizations collect from them and how they use it
Transparency	Consumers have a right to easily understandable information about privacy and security practices
Respect for context	Consumers have a right to expect that organizations will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data
Security	Consumers have a right to secure and responsible handling of personal data
Access and accuracy	Consumers have a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to consumers if the data are inaccurate
Focused collection	Consumers have a right to reasonable limits on the personal data that companies collect and retain
Accountability	Consumers have a right to have personal data handled by companies with appropriate measures in place to assure they adhere to the Consumer Privacy Bill of Rights

Source: Compiled based on the U.S.'s Consumer Privacy Bill of Rights.

(2) Respect for context: Consumers have a right to expect that organizations will collect, use and disclose personal data in ways that are consistent with the context in which consumers provide the data.

Overall, while these principles encourage consumers to actively become involved in the protection of their own privacy, businesses are also encouraged to take self-regulatory measures.[13]

2 EU: Strengthening the protection of privacy as a "human right"

Throughout the EU, following the introduction of the EU Data Protection Directive in 1995, each of the EU member states has enacted its own domestic legislation and has implemented measures to protect personal information and privacy. However, this Directive was formulated before the Internet spread to its current extent. To appropriately respond to a rapidly evolving networked society, there have been ongoing discussions as to how best to amend the Directive.

Ultimately, in January 2012, the European Commission announced a comprehensive reform of the EU Data Protection Directive in the form of a legislative proposal for a General Data Protection Regulation.[14] Unlike the existing EU Data Protection Directive that gives each member state the discretion to form its own laws, the proposed General Data Protection Regulation will be positioned in such a way in which the entire EU is subject to the same rules. Behind this move is a sense of urgency to consistently promote the protection of privacy throughout the community and eliminate the differences between individual countries in order to respond to rapid changes.[15]

The proposed General Data Protection Regulation, which is based on the fundamental principle of "privacy is one of the most important human rights,[16]" establishes new rights such as the "right to be forgotten" and the "right not to be subject to a measure based on profiling by means of automated processing." In addition, stricter regulations are also imposed on businesses, which include the imposition of penalties. Even if a company does not have a physical presence within the EU, the company will be subject to this Regulation if it offers goods or services to the citizens of the EU, a fact that companies in Japan cannot afford to ignore (Table 3).

3 Three issues to be addressed

Considering the review of privacy policies in the U.S. and Europe, the following paragraphs discuss the three issues that are assumed to have a major impact on Japan. They are: (1) behavioral targeting, (2) automated profiling and the buying/selling of personal data and (3) protection of children's privacy. Since none of these issues are specifically addressed by Japan's Act on the Protection of Personal Information, these issues need to be addressed to enhance the legal framework as well as from the viewpoint of international coordination.

(1) Behavioral targeting

"Behavioral targeting," whereby companies such as advertisers use cookies or web beacons[17] to collect and analyze an individual's browsing history and provide that individual with online advertisements and services that are tailored to his or her preferences, has been deployed by many related businesses.

However, because this technique could be interpreted as being an invasion of privacy,[18] there has been increasing pressure from U.S. consumer groups and European data protection authorities to impose stricter regulations. This brings up the issue of creating a mechanism that can differentiate between "users who wish to receive" online advertising that is tailored to their preferences and "users who do not."

In response to such requests, the U.S. has promoted industry self-regulatory efforts based on an "opt-out"[19] scheme by means of a "Do Not Track" mechanism. The intention of the "Do Not Track" system is to introduce a means whereby users can specify on their own web browsers whether they accept being tracked, such that

Table 3. Outline of rights specified in the proposed EU General Data Protection Regulation

Name		General Data Protection Regulation
Fundamental principle		Protection of human rights
Conditions for consent		Opt-in (requiring data controllers and processors to obtain prior consent of data subjects)
Features	Control over own data	Strengthening consumer control over their own data through transparent privacy policy (Article 11), obtaining explicit consent (Article 7), ensuring easy access to own data (Article 15), ensuring the right to be forgotten (Article 17), and so on
	Security	In addition to requiring data controllers and processors to take technical measures to protect privacy (Article 30) and encouraging the establishment of data protection certification mechanisms (Article 39), the Regulation requires notification of a personal data breach to the supervisory authority within 24 hours (Article 31)
	Responsibility of data controllers	Strengthening the accountability of data controllers through "Privacy by Design" (taking measures to ensure the protection of privacy from the service design stage) requirements (Article 23) and data protection impact assessment related to sensitive personal information (Article 33)
	Right to object	Stipulating the right to object to automated profiling based on personal data (Article 19) and the right not to be subject to a measure that is based solely on automated profiling (Article 20)
	Child privacy	For the processing of personal data of a child below the age of 13 years, requiring controllers to obtain prior consent of the child's parent or custodian (Article 8)
	Territorial scope	This Regulation also applies to businesses not established in the Union, but offering goods or services to data subjects in the Union (Article 3)

Source: Compiled based on the proposed EU General Data Protection Regulation.

the intentions of those "users who do not agree" to receive online advertising and other services based on behavioral targeting can be respected (Figure 11).

However, because the FTC has deemed that the self-regulatory measures based on the "Do Not Track" mechanism have not attained the desired level of effect, the commission has committed to strengthening its supervision of the "Do Not Track" system.[20] In response, Microsoft announced that it had changed the default setting of its Internet Explorer web browser to "Do Not Track." However, the online advertising industry is taking a stance in opposition to Microsoft's decision.[21]

On the other hand, the EU has adopted a policy whereby emphasis is placed on a user's controlling his or her own personal information. This opt-in policy requires businesses to obtain the prior explicit consent of a user before using cookies or similar tools for behavioral targeting.[22] However, because cookies have become indispensable tools for the use of the Internet, a complete change to "opt-in" would adversely affect convenience and would interfere with site operations. As such, some sites still rely on the "opt-out" approach.

(2) Automatic profiling and the buying/selling of personal data

"Automatic profiling" involves using cookies and similar tools to track and infer an individual's behavior, as well as collecting personal information that the individual posts to websites in order to automatically create a profile of the individual. For example, the private information that an individual writes to an SNS or blog is collected by a profiling company and then used to publish, with no check of accuracy, a "history" of the individual.

The problems lie in "without the consent of an individual," "profiling is performed automatically," "without any check of accuracy" and "data is made public." In addition, once data on an individual has been accumulated, because there are many data brokers who are willing to sell and buy that data, there have been cases where incorrect data has been associated with an individual.

Since the beginning of 2000, the United States has encouraged the industry to enable users to select whether they allow themselves to be profiled, and to ensure the accessibility to collected data by the relevant individual and the safety of that data.[23] However, recognizing that these self-regulatory efforts were not having the desired effect, in March 2012, the Federal Trade Commission (FTC) suggested that Congress consider enacting data broker legislation.[24] In fact, in June 2012, the FTC fined Spokeo $800,000 for marketing profile data in violation of the Fair Credit Reporting Act.[25] As such, tighter regulations have already been imposed on companies that compile and sell profile data (Figure 12).

In the EU, the proposed General Data Protection Regulation established the right of every natural person not to be subject to automated processing intended to evaluate certain personal aspects relating to the natural person or to analyze or predict in particular the natural person's work performance, economic situation, location, health, personal preference, reliability or behavior, while restricting profiling services to ensure that such right is not infringed.

France has already seen a case where a fine was imposed on a buyer of profile data. In this case, a data broker collected the personal information of real estate owners entered in online advertisements and then sold such data to a real property reports company. This company then used the purchased data to feed advertising to the property owners without obtaining their prior consent. The French data protection authority, CNIL,

imposed a fine of €20,000 on the real property reports company that purchased the data (Figure 13).[26]

(3) Protection of children's privacy

With the spread of online services that are accessed mostly by youngsters, as exemplified by SNS, both the U.S. and the EU have identified the protection of children's privacy as an important issue. Children use online services as if they were parts of games. While such behavior makes them computer literate at an early age, their lack of social experience and language skills often results in them casually posting details about their lives online. Even if they realize that their posting was inappropriate and want to delete the information they posted, it is actually very difficult to completely delete such information once it has been posted on the Internet.

In the U.S., the Children's Online Privacy Protection Act (COPPA) requires that children under 13 may only

Figure 11. U.S.'s "Do Not Track" mechanism

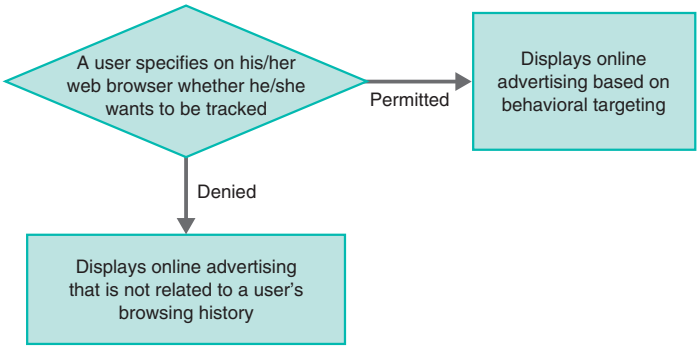
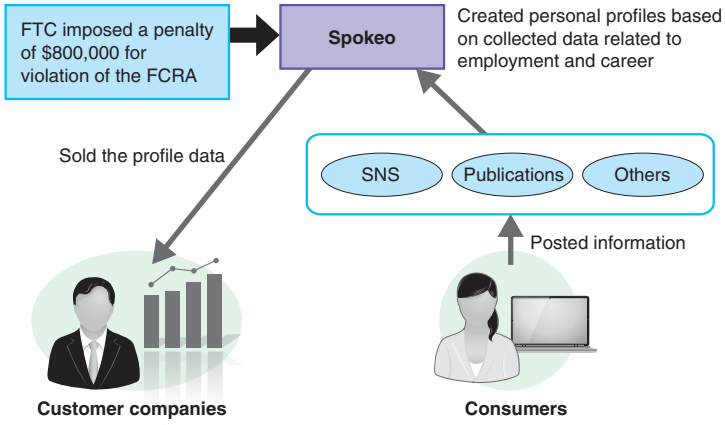
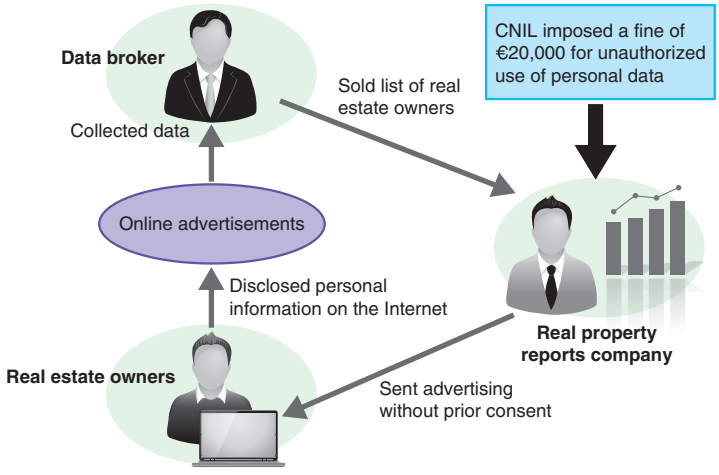


Figure 12. Civil penalty imposed on a company compiling and selling profile data in the U.S.



Notes: FCRA = The Fair Credit Reporting Act, SNS = social networking service.
Source: Compiled based on FTC website.

Figure 13. Fine imposed on the buyer of profile data in France



Note: The CNIL is the French data protection authority.
Source: Compiled based on Privacy and Information Law Blog.

use online services with their parents' consent. However, because service providers have failed to fully comply with this law, the FTC is expected to strengthen its enforcement.[27]

In much the same way as in the U.S., the proposed new EU-wide regulation (General Data Protection Regulation) requires companies to obtain parental consent to process the data of children under 13. These measures bring the EU in line with the U.S. for the protection of children's privacy. In addition, the right to be forgotten, which will be newly established in the proposed regulation, takes specific account of children's privacy. As such, service providers that publish personal data on websites such as social media sites will become responsible for erasing all links to and copies of an individual's data from the Internet in response to a request from the relevant individual.

V Protection of Privacy Required in Big Data Society

As it makes its way toward big data society, as discussed in the previous chapters, Japan also urgently needs to address the issue of privacy protection. In this chapter, the authors present five points related to the protection of privacy in which three entities, namely, "users," "Internet service providers" and "government agencies and third parties," are involved, and consider how each entity should deal with these five points (Figure 14).

1 Default settings and ways to obtain user consent that satisfy user expectations (combination of opt-in and opt-out)

While the fundamental principle is to respect the wishes of individuals in collecting and using information related to those individuals, it is reasonable to assume that many Japanese users will not want to lose the convenience of using websites by having to provide their consent to insert cookies when they visit those sites, as is required in the EU. On the other hand, those same users will likely be uncomfortable about cookies being used by service providers to collect behavioral information such as users' browsing histories, which is then shared among multiple firms.

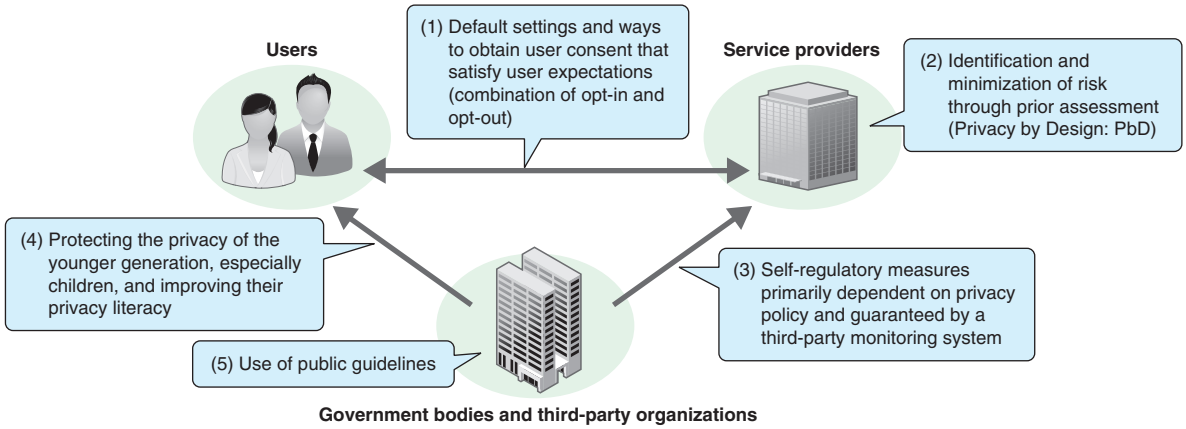
For this reason, the authors propose that the scope of information collection and use/provision that can be expected by users in the context in which information was collected, that is, the scope that can be assumed by users, should be examined. Based on the results of such examination, default settings for the disclosure of personal information should be established and situations in which consent must be obtained should be determined.

For example, because many Japanese tend to be reluctant to provide their names or identifying photographs, the default setting for the scope of the disclosure of personal information on an SNS site should be set as high as "friends only." An opt-out approach could be adopted for any minor changes such as changes to the administrator's name. However, for providing the information to other sites, an opt-in method should be adopted to obtain prior explicit consent of the user. In addition, the statement that is displayed when requesting the user's consent should specify precisely how the information is going to be used, rather than relying on general statements such as "for the purposes of after-sales service."

However, it is unlikely that in the highly competitive Internet industry, these changes would occur of their own accord. In order to have service providers look beyond the success of their own businesses and move toward the healthy development of the industry, it will be necessary to establish an environment in which public organizations first lay down guidelines, after which service providers, under the coordination of industry associations, implement appropriate measures.[28]

In addition, in much the same way as with the "Do Not Track" system that the U.S. FTC operates, an expectation can be given to the development of a mechanism

Figure 14. Five points in achieving the protection of privacy in big data society



whereby an information system can recognize the privacy settings of a user and automatically adjust its processing accordingly. For example, if a user sets his or her desired level of privacy protection to one of three levels —high, medium or low, then a site being accessed by that user will automatically tune itself to the user's default setting, while restricting those services to which the user must opt in. In this way, the user will be given a sense of relief while the site remains easy to use.[29]

2 Identification and minimization of risk through prior assessment (Privacy by Design: PbD)

In big data society, the probability becomes higher that an individual could be identified from information that was actually regarded as being non-personal in the past. Therefore, any service that intends to collect information about individuals should, prior to the start of the service, assess the possibility of invasion of privacy, and identify and minimize any such risks through the implementation of "Privacy by Design (PbD)" (Figure 15).

The U.S., Canada and Australia require all administrative bodies to implement a "Privacy Impact Assessment (PIA)" as a means of implementing PbD for their e-government projects, and the implementation of a PIA has become common in these countries. The proposed new EU-wide regulation requires both public and private sectors to implement a PIA. In Japan, the "My Number" law, for which legislative proceedings are underway, will require administrative agencies to implement a "personal information protection assessment."

When PIA is implemented, the authors propose a quantitative examination of the risk of economic loss. If the return expected from a service is compared with the risk of economic loss that any invasion of privacy would incur, it would become possible to justify a budget needed for investing in implementing privacy protection measures, which would facilitate the implementation of PbD.

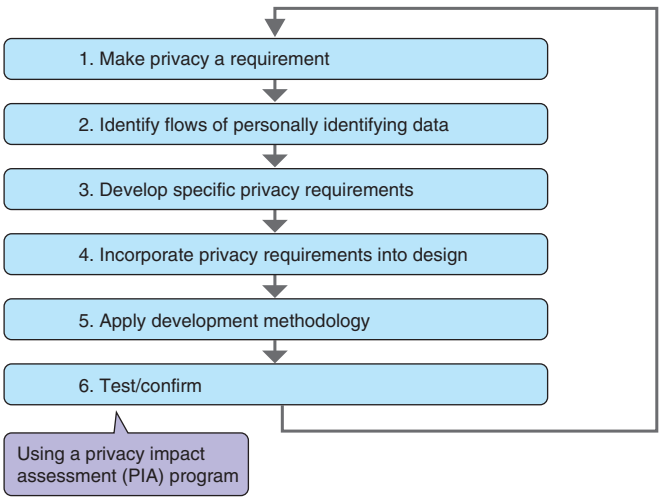
3 Self-regulatory measures primarily dependent on privacy policy and guaranteed by a third-party monitoring system

As seen in the cases of Google and Facebook that were described in Chapter II, in the U.S., a privacy policy is considered as a set of promises made by a service provider to its customers for the protection of privacy. If any unfair or deceptive acts or practices are observed in operating a privacy policy, the FTC can order corrective action under the provisions of Section 5 of the Federal Trade Commission Act (FTC Act). In the EU, as shown in Figure 9, a high proportion of young people read the privacy policies posted on the websites that they visit in order to protect their own privacy. The privacy policy functions as a tool to govern the protection of privacy by service providers in the EU.

In Japan, given that the Act on the Protection of Personal Information does not address the issue of privacy, there is a need for service providers to post their privacy policies on their websites and then abide by their policies.[30] As a first step toward these self-regulatory measures, public bodies and industry associations should determine the matters that must be included in the privacy policy.

A third-party monitoring system is needed to enhance the efficacy of privacy policies. Because in Japan there is no regulatory authority overseeing the protection of privacy, as there is in the U.S. and the EU, private-sector organizations such as auditing companies and authorized personal information protection organizations would have to be called upon to fulfill this role.

Figure 15. Privacy by Design (PbD) operation processes



Source: Compiled based on Ann Cavoukian, "Privacy by Design Curriculum.

Table 4. Fundamental principles of guidelines for the handling of user information sent through smartphones

[Fundamental Principles]

(1) Ensuring transparency	Service providers shall notify users of the details of the target information in terms of its collection, storage and use, as well as a means available for users to be involved in such collection, storage and use. Otherwise, such details shall be put in a state where users are easily noticeable. When service providers notify users of the collection of their personal information or publicize such collection to users, or acquire the consent of users, such notification, publication and acquisition shall be conducted in an easily recognizable and understandable manner.
(2) Securing the opportunity of user involvement	Service providers shall notify users of the necessary matters related to the collection of their personal information (e.g., information to be collected, the purpose of its use, a range of information that is to be provided to third parties) or publicize such matters to users, or obtain the consent of users in accordance with the context of the characteristics of relevant services. In addition, service providers shall provide users with a means of being involved in the handling of their personal information such as halting the collection or use of such information.
(3) Ensuring data collection through proper means	Service providers shall collect target personal information by proper acceptable means.
(4) Ensuring proper management of user information	Service providers shall take necessary and proper measures for the management of target personal information such as preventing such information from being disclosed, lost, or damaged, etc.
(5) Appropriately handling complaints and requests for advice	Service providers shall appropriately and promptly respond to any complaints and requests for advice with respect to the handling of target personal information.
(6) Privacy by Design	Service providers shall incorporate privacy requirements into design to respect and protect the personal information and privacy of users at the stage when new applications and services are developed or when websites to which applications are provided, software and terminals are developed. Service providers shall fully recognize the users' rights to their personal information and privacy and their expectations in this regard, and shall design and develop applications and services from the users' perspectives in a user-friendly manner.

Source: Study Group Concerning Various Problems with ICT Services based on User Viewpoints, the "Final Report of the Working Group on the Handling of User Information Sent through Smartphones: Smartphone Privacy Initiative," August 2012.

4 Protecting the privacy of the younger generation, especially children, and improving their privacy literacy

Although young people find it extremely easy to adapt to new technologies, their experience of the real world is limited, such that they do not pay sufficient attention to their privacy and can easily become victims. In fact, the number of malicious applications that target young people is rapidly increasing. Given this situation, the protection of children's privacy, in particular, has become an urgent issue. As explained in Chapter IV, in both the U.S. and the EU, before children aged below 13 can access Internet services, service providers must obtain the consent of their parent or guardian. Sooner or later, Japan needs to implement a similar system.

The right to be forgotten, as proposed in the EU, is currently being considered with particular attention being paid to young Internet users. Recently, the Privacy Commissioner of Canada said "the fact that electronic records of many of the mistakes of today's youth will persist for decades to come is cause for deep concern."[31] However, a concrete method of achieving this right to be forgotten is still at a trial-and-error stage.[32] Therefore, focus should first be placed on privacy education for the younger generation so that they become more "privacy literate."

5 Use of public guidelines

The Ministry of Internal Affairs and Communications has issued guidelines for the handling of user information sent through smartphones, and is promoting self-regulatory efforts to protect privacy on the part of industry and service providers (Table 4). In addition, under an identification number (My Number) system for social security and taxation for which legislative proceedings are underway, the "personal information protection assessment," which is the Japanese version of PIA, is to be introduced. To this end, draft guidelines have already been formulated.[33] In developing businesses, service providers that handle information about individuals will find it effective to follow these public guidelines.

In the first half of 2012, both the U.S. and the EU successively announced proposed revisions to their privacy laws. Japan is also moving to protect privacy with the introduction of the My Number system. Overall, we are entering a new age of privacy. As we move towards big data society, both the public and private sectors are required to commit to achieving focus that shifts from the protection of "personal information" to that of "privacy."

Notes:

1 "Outline of the Status of the Enforcement of the Act on the Protection of Personal Information 2010," the Consumer Affairs Agency, Government of Japan, August 2011.

2 "Survey on the Trend in Communications Usage 2006" and "Survey on the Trend in Communications Usage 2010," the Ministry of Internal Affairs and Communications.

3 "Survey on Efforts concerning the Protection of Personal Information 2011," the Ministry of Economy, Trade and Industry, March 2011.

4 Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, UCLA Law Review, Vol. 57, 2009.

5 According to *Kojin jyoho hogo-ho no chikujyo kaisetsu* (Article-by-Article Explanation of the Act on the Protection of Personal Information) written by Katsuya Uga and published by Yuhikaku Publishing Co., Ltd. in 2005, the rights and interests of individuals include both "personal and property rights and interests."

6 "Handling of data such as users' browsing histories related to Viewn service (January 12, 2012)," Viewn's website (http://www.viewn.co.jp/news/20120112_01.html) (in Japanese).

7 "Kabushiki kaisha mirogu daisansha iinkai hokokusho 2011 nen 12 gatsu 16 nichi (Report of the Third-Party Committee Investigating the Milog Case), December 16, 2011."

8 Federal Trade Commission, "FTC Charges Deceptive Privacy Practices in Google's Rollout of Its Buzz Social Network," March 30, 2011 (http://www.ftc.gov/opa/2011/03/google.shtm).

9 Federal Trade Commission, "Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises," November 29, 2011 (http://ftc.gov/opa/2011/11/privacysettlement.shtm).

10 IPTS (Institute for Prospective Technological Studies) is one of the seven scientific institutes of the European Commission's Joint Research Centre (JRC). Its mission is to provide customer-driven support to the EU policy-making process by developing science-based responses to policy challenges that have both a socio-economic as well as a scientific/technological dimension.

11 A cookie is a mechanism for temporarily storing information about an Internet user on the user's own computer through its web browser when the user is browsing a website. Because data such as user information, the last date the user visited the site and how many times the user visited the website are recorded in a cookie, it is used to identify the user for purposes such as authentication.

12 The White House, "We Can't Wait: Obama Administration Unveils Blueprint for a "Privacy Bill of Rights" to Protect Consumers Online," February 23, 2012 (http://www.whitehouse.gov/the-press-office/2012/02/23/we-can-t-wait-obama-administration-unveilsblueprint-privacy-bill-rights).

13 Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change," FTC REPORT, March, 2012 (http://ftc.gov/os/2012/03/120326privacyreport.pdf).

14 EUROPEAN COMMISSION, "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)," Jan. 25, 2012.

15 Comments by European Commission's Vice President at the time of the announcement of a proposal for a General Data Protection Regulation (European Commission, "Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses," January 25, 2012).

16 The provisions of Article 8, Paragraph 1, the European Convention on (for the Protection of) Human Rights, stipulate that "Everyone has the right to respect for his private and family life, his home and his correspondence."

17 A web beacon is a small image file embedded in a web page or an email, and is used to track who is reading a web page or an email.

18 "Self-Regulatory Principles For Online Behavioral Advertising," FTC Staff Report, February 2009.

19 An "opt-out" scheme is a rule in which a user's personal information is used without obtaining the prior explicit consent of the user, and the use of the personal information is stopped at the request of the user. However, adoption of the "opt-out" system requires notification/announcement of the usage purpose of personal information.

20 Bloomberg, "FTC Calls for Laws to Boost Consumer Privacy Protections," Mar 27, 2012 (http://www.bloomberg.com/news/2012-03-26/ftc-calls-for-laws-to-boost-consumer-privacyprotection-online.html).

21 "Microsoft Windows 8 includes default Do Not Track privacy feature," The Washington Post, May 31, 2012 (http://www.washingtonpost.com/blogs/post-tech/post/microsoft-windows-8-includes-default-do-not-track-privacyfeature/2012/05/31/gJQAQ8N74U_blog.html).

22 Directive 2009/136/EC (Cookie Directive).

23 Federal Trade Commission, "Online Profiling: A Report to Congress," June 2000.

24 Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change," FTC REPORT, March 2012 (http://ftc.gov/os/2012/03/120326privacyreport.pdf).

25 Federal Trade Commission, "Spokeo to Pay $800,000 to Settle FTC Charges Company Allegedly Marketed Information to Employers and Recruiters in Violation of FCRA," June 12, 2012 (http://ftc.gov/opa/2012/06/spokeo.shtm).

26 Privacy and Information Law Blog, "France: Sending of direct marketing communications: list brokers and clients: CNIL finds liability on both sides," February 13, 2012 (http://privacylawblog.ffw.com/category/sanctions).

27 Thompson Coburn LLP, "United States: FTC Strengthens Law Protecting Children's Personal Information," 12 March 2012 (http://www.mondaq.com/unitedstates/x/168174/Privacy/FTC+Strengthens+Law+Protecting+Childrens+Personal+Information).

28 The Ministry of Internal Affairs and Communications (MIC) has organized the Study Group Concerning Various Problems with ICT Services Based on User Viewpoints. The MIC published "Final Report of the Working Group on the Handling of User Information Sent through Smartphones: Smartphone Privacy Initiative" in August 2012. This report spells out the fundamental principles for the protection of privacy.

29 A similar concept is adopted in the Platform for Privacy Preferences Project (P3P). P3P enables websites to express their privacy practices in a standard format that can be retrieved automatically and interpreted easily by users' computer tools. P3P has not been implemented widely due to the difficulty and lack of value.

30 Although Japan's Act on the Protection of Personal Information does not specifically address the policy of the

protection of personal information, the provisions of Article 24 (Public Announcement of Matters Concerning Retained Personal Data, etc.) of the Act specify the matters that must be put in a state in which the relevant person can access the data.

31 Website of the Privacy Commissioner of Canada (June 2012).

32 Google's Dashboard provides a choice to not display information about individuals in search results.

33 Cabinet Secretariat, "Draft Guidelines for Specific Personal Information Protection Assessment" (March 2012).

Shintaro KOBAYASHI is a senior consultant at NRI's ICT & Media Industry Consulting Department and Center for Strategic Management & Innovation. His specialties include IT public policy and management.

Taku YASHIRO is a researcher at NRI's Public Management Consulting Department. His specialties include information law, development finance policy and Southeast Asia political and economic situation.

Tomohisa ITOH is a consultant at NRI's ICT & Media Industry Consulting Department. His specialties include business strategy, marketing and IT strategy in the fields of information and communications, finance, consumer products and service; support for establishing legal systems in the information and communications field.

Sawako OKUMI is a consultant at NRI's Financial Business Consulting Department. Her specialties include business reform and system PMO in the credit card industry and personal information protection policy.

As a leading think tank and system integrator in Japan, Nomura Research Institute is opening new perspectives for the social paradigm by creating intellectual property for the benefit of all industries. NRI's services cover both public and private sectors around the world through knowledge creation and integration in the three creative spheres: "Research and Consulting," "Knowledge Solutions" and "Systems Solutions."

The world economy is facing thorough structural changes led by the dramatic growth of IT industries and the rapid expansion of worldwide Internet usage—the challenges of which require new concepts and improvement of current systems. NRI devotes all its efforts to equipping its clients with business strategies for success by providing the best in knowledge resources and solutions.

NRI Papers present selected works of NRI Group's 7,000 professionals through its worldwide research network. The mission of ***NRI Papers*** is to contribute new ideas and insights into business management and future policy planning, which are indispensable for overcoming obstacles to the structural changes in our society.

Inquiries to: Corporate Communications Department
Nomura Research Institute, Ltd.
E-mail: nri-papers@nri.co.jp