Study Group on Consumer Issues with ICT Services

An Examination of Lifelog-Monitoring Services

May 2010

http://www.soumu.go.jp/english/ict

1. Introduction

With the increasing functionality and prevalence of networked and mobile devices, attention has been focusing on business models founded on extracting information from lifelogs — logs of individuals' day-to-day lives. Examples of these models include behavioral advertising businesses that deliver ads based on one's past Web browsing or purchasing history, location-based assistance services, and statistical services that analyze Web browsing or purchasing histories with one's age group and other attributes. Although these new business models are expected to be an area of significant growth in the coming years, they have prompted concerns and fears among consumers because of their privacy and personal information implications. There are also suggestions[1] that the road ahead for these new services may not be so smooth as some anticipate.

Working from this understanding, the Study Group conducted an examination of the related issues. We first developed a general view of the present state of lifelog-monitoring services in Japan and in other countries and regions. Next, we looked at the associated legal issues in Japan, primarily from the perspective of personal information protection and privacy protection. Following these examinations, we authored a set of principles calling on businesses to exercise care and consideration in certain matters, from the viewpoint of easing consumer concerns and ensuring a safe and secure Internet usage experience. We decided to create a set of informal, consumer-centric principles instead of administrative guidelines, which strongly resemble regulations, because lifelog-monitoring services are still in their infancy and impeding their growth should be avoided. In addition, we decided to encourage businesses to draft self-regulatory guidelines. Other mitigating factors were that lifelog-monitoring services are very diverse and that it is difficult at the present time to envision how these services will evolve in the future. For this reason, too, we decided not

[1] This point was brought up by the Study Group on the Communications Platform, which was formed on February 27, 2008, and chaired by Hitoshi Aida, professor at the graduate school of University of Tokyo. The study group released its final report on January 30, 2009. In the report, the study group stated: "…while the enormous potential marketability of these new customization businesses [that make use of information] is recognized, there needs to be a careful and deliberate examination concerning what usage is permissible when such businesses make use of data from users' attributes or histories (browsing histories, purchase histories, and behavior histories) or of analyses of these data."

to proceed beyond drawing up a set of informal, consumer-centric principles and calling on businesses to form their own guidelines tailored to their individual circumstances.

Finally, we produced an overview of behavioral advertising using deep packet inspection technologies and surveyed the legal issues this form of advertising raises.

In Japan, we enjoy very advanced networked and mobile devices and we lead the world in constructing the infrastructure needed for the development of advanced lifelog-monitoring services. Despite this, consumer concerns are currently curbing the advancement of these new services. It is our hope that this proposal will help pave the way for the further advancement by lifelog-monitoring services as a guide to addressing and alleviating consumer concerns about these services.

2. State of Lifelog-Monitoring Services in Japan[2]

Lifelogs were little used prior to the development of advanced networked and mobile devices. Now, however, lifelogs are beginning to be actively monitored for behavioral advertising or processed for statistical purposes, among other applications. After giving a definition of lifelog, this chapter looks at the two main types of lifelog-monitoring services being used today: services providing information matching consumer interests, views, or preferences and services providing statistical information.

(1) Lifelog: a definition

In short, a lifelog is a log of an individual's life built up over time. It is a very broad concept and includes all information that can conceivably be accumulated about a person. Even if we restrict our scope to digital information, lifelogs can include Web site browsing histories, purchasing and payment histories on e-commerce sites, location information obtained from mobile devices' global positioning system (GPS) data, information obtained from sensors on mobile devices or automobiles, photos taken with digital cameras, blog entries, records of friendships and relationships posted on social networking service (SNS) sites, and information extracted from contactless IC cards, such as transit histories stored on train passes.

Lifelogs were not often referenced in the past, since the collectable digital lifelog information was limited to user-entered registration information or browsing histories acquired with cookies or similar techniques. With recent technical innovations, however, it is feasible to develop services that can easily capture and dynamically utilize a diverse range of lifelog data. Examples of active utilization include analyzing lifelogs to deliver advertisements that match consumer preferences and interests or the compiling of statistics by collecting numerous lifelogs.

A number of technological developments have fueled the active collection and usage of lifelog data. The first of these is the development of sensors and their

[2] Much of this chapter is based on materials submitted by Shinji Terada, an observer at the Study Group's proceedings. See Mr. Terada's publication "Lifelog Business" (Impress R&D, 2009) for more details.

inclusion in all sorts of devices, which has greatly simplified the collection of diverse lifelog data. Second, access to massive amounts of cheap storage has made the collection and storage of an enormous number of lifelogs possible. Third, the advancement of technologies that search, analyze, transmit, and publish large amounts of data has enabled the provision of more refined and precise information.[3] Finally, faster and cheaper networks have fueled the inexpensive circulation of large amounts of data, which in turn is driving more lifelog collection and usage.

(2) Two directions for lifelog usage

Services actively mining lifelog data have become feasible, as described above. These services are constantly transforming, developing, and diversifying, often in unpredictable ways, as new technological innovations become available. Hence, it is difficult at present to firmly demarcate the boundaries of lifelog-monitoring services. For convenience in this report, we divided lifelog-monitoring services into services providing information matching consumer preferences and interests and services providing statistical information. While fully aware there are services that do not fit this categorization, this categorization was felt to be sufficient for our present analysis. Accordingly, the next sections develop a general view of these two types of services through examples.

A. Services providing information matching consumer preferences and interests

Services in this category acquire and accumulate consumer lifelogs, analyze them for preferences and interests, and either display relevant ads or provide relevant advice or information. The ads or advice provided by these services are more likely to correspond to the consumer's interests than ordinary ads or advice. The most common services found in this category today are behavioral advertising and location-based personalized assistance services. More advanced services are expected to arrive with sensor developments that can collect even more lifelog data. For example, services are being studied that will use microscopic sensors embedded in the body to acquire and analyze biometric data and provide pertinent health care and maintenance advice.

[3] Gordon Bell and Jim Gemmell, "Total Recall: How the E-Memory Revolution Will Change Everything". (Dutton Adult, 2009).

The next sections look at the two most common services: behavioral advertising and location-based personalized assistance services.

i. Behavioral advertising

Behavioral advertising[4] refers to services that predict consumers' preferences and interests from their accumulated Web behavioral history (such as viewing histories or purchasing histories on e-commerce sites), divides consumers into audience segments, and then delivers ads matching the attributes of each segment. It is interesting to note that these deliveries are called "advertisements" only when a Web site publisher sells space on its Web site to advertisers for compensation or consideration. When a publisher uses a space on its Website for its own promotional purposes, the deliveries are called "recommendations."[5] [6]

Whether advertisements or recommendations, there is little difference in the Web behavioral logs gathered and stored or how the logs are utilized. Logs are generally amassed by the following method. When a consumer first accesses via the Internet some site or media content with an advertisement, the advertisement assigns a unique ID number to the consumer's browser or mobile device using a cookie or similar technique.[7] After this, each time the consumer performs some action on that site or media, such as viewing a Web page or inputting information, a log of that action is stored along with the ID number. As the behavior log is accumulated, algorithms analyze the consumer's actions to find his or her preferences and interests, which are used to sort the consumer into a segment. The advertiser then delivers to the browser or mobile device ads and information targeted for the specific segment.

---

[4] While not behavioral advertising in the strictest sense, advertisements, such as Google AdWords, delivered according to search results and advertisements, such as Google AdSense, delivered according to Web site content are forms of targeted advertisements. There are also advertisements that combine elements of search advertisements and contextual advertisements in behavioral advertising.

[5] Most recommendations are contextual, displaying information relevant to the viewed page or the viewed page's products, although some do analyze and target an individual's preferences and interests.

[6] For example, most newspaper sites sell space on their sites to advertisers; therefore, "ads" are provided on their sites. Banners appearing on personal Web sites are also advertisements. But promotions of products on e-commerce sites are usually recommendations, because the spaces are not sold to advertisers. Still, the line between advertisements and recommendations is difficult to establish, since there are e-commerce aggregate sites that may sell spaces to advertisers.

[7] Cookies are generally not used with mobile phones. Instead, the phone is identified with the subscriber ID number.

The business that serves the targeted advertisements and the business providing the advertising space are usually different businesses. In these cases, the ad-serving business typically sets up an ad network serving ads to spaces on multiple partner Web sites. Third-party ad delivery scenarios like this are expected to expand for several reasons. First, because the ad-serving business can acquire visit logs from multiple Web sites,[8] it can obtain a more detailed picture of an individual's preferences and interests and thus deliver more appropriate and effective ads. Second, the media business is able to outsource the expense of lifelog analysis and ad delivery. On the other hand, the ability to finely deduce an individual's preferences and interests is considered by some as a privacy threat. As a result, there is ongoing debate in the United States and other countries about the privacy implications of third-party ad delivery.

ii. Personalized assistance services

Mobile telecoms are beginning to develop advanced personalized assistance services,[9] making use of the convenient fact that mobile users carry their mobile phone or device with them nearly all the time. Like behavioral advertising, personalized assistance services use algorithms to estimate a user's preferences and interests from stored behavioral logs and personal attributes and serve targeted information to the user's browser, mobile phone, or device. Where they differ is in a personalized assistance service's ability to deliver more timely information to consumers because it can access more immediate lifelog data from GPS and other sensors built into mobile devices and because it can utilize the mobile device that the user always carries with him or her as an interface.

Personalized assistance services using location information taken from GPS and other sensors are now reaching the commercial stage, but future advances in sensor technology may lead to the creation of services that use biometric and environmental data as well. And sensors are starting to appear in more than just mobile devices; they are being installed in car navigation systems and game

[8] Some ad-serving businesses collect visit logs on their own, and others purchase visit logs from other businesses.

[9] NTT DoCoMo's iConcier is one leading location-based personalized assistance service that is being deployed. At the testing stage is KDDI Laboratory's Keitai de Lifelog, part of the Ministry of Internal Affairs and Communications' Ubila R&D project into ubiquitous networking control and management technologies, and NTT DoCoMo's My Life Assist Service, part of the Ministry of Economy, Trade and Industry's Information Grand Voyage project.

consoles. For these reasons, many observers expect to see significant growth and development in the personalized assistance service market.

B. Services providing statistical information

Services in this category acquire lifelog data from individuals, tabulate and process the data statistically, and provide the resulting statistical information to their clients. In the past, these services created statistical information for marketing purposes from subscriber records and similar data. However, the applications of this statistical information were constrained by the limited amount and type of obtainable lifelogs.

But with the expanding volume and diversity of lifelogs that can be collected due to the emergence of large-scale lifelog aggregators, such as mobile telecoms and SNS businesses, and the inclusion of sensors on mobile devices, services can now create richer, more accurate statistical information with more efficiency.

Mobile telecoms, for instance, can construct accurate statistical models of people's behavior by pairing location information acquired from the GPS sensors on mobile phones with personal attributes like gender and age. Further sensor developments and installations will likely enable telecoms to efficiently create accurate statistics on weather conditions or traffic congestion.

In the same way, major SNS sites have the potential of becoming statistics providers by harnessing their large user bases.[10] Because SNS sites collect detailed information on preferences and interests[11] as well as age and address information, they can generate rich, high-quality statistical information.

[10] For example, among the major domestic SMS sites, Mixi has about 18.58 million users, Gree has about 16.73 million users, and DeNA's Mobage-town has about 15.81 million users. (All figures taken from respective IR reports and current as of December 2009.)

[11] Mixi, for example, requires users to give their interests at sign-up. Furthermore, users may also list their favorite movies, sports, music, and free-time pursuits.

3. State of Lifelog-Monitoring Services in Other Countries[12]

Endeavors are underway to actively collect and utilize lifelog data in other countries as well. In the United States, research is looking at advanced lifelog-monitoring services, such as the LifeLog Project[13] and MyLifeBits Project.[14] Nevertheless, much like Japan, the services with the greatest commercial interest at the current time are services providing information matching consumer preferences and interests: that is, online behavioral advertising and content recommendations ("behavioral advertising," hereafter). The following sections detail the current state of behavioral advertising in other countries.

(1) United States

The privacy implications of behavioral advertising have been under the spotlight since the DoubleClick controversy in 2000.[15] This incident prompted the Federal Trade Commission (FTC) to release in 2007 the *Online Behavioral Advertising Privacy Principles* draft of fundamental principles for businesses to follow when creating self-regulatory guidelines. These principles, after undergoing a public comment process and subsequent revisions, were released in 2009 as the *FTC Staff Report: Self-Regulatory Principles For Online Behavioral Advertising*. The key requirements under the principles were explicit statements that data was being collected and the ability of users to opt out of any data collection.

Several industry groups have created their own guidelines based on the FTC's

---

[12] This chapter is based on the March 2010 report by the Study Group on the Economic Benefits of Behavioral Advertising and User Protection, commissioned by the Ministry of Internal Affairs and Communications' Institute for Information and Communications Policy.

[13] Run by the Defense Advanced Research Projects Agency, an agency of the U.S. Department of Defense, the LifeLog Project was an ambitious attempt to create a database that would record everything a person says, sees, or does. It was canceled in 2004 after civil groups vehemently objected to the project on privacy grounds.

[14] The MyLifeBits Project, sponsored by Microsoft, is a pilot project to digitize and store a record of everything a person encounters in their life — Web pages, books, DVDs, CDs — and then create a system where all this information can be accessed at any time. http://research.microsoft.com/en-us/projects/mylifebits/default.aspx (last visited on April 2, 2010).

[15] The controversy centered on the privacy of online advertising agency DoubleClick's services. Legal action was launched against the company for embedding cookies on hard drives when Internet users accessed participating or partner Web sites, which was seen as a violation of the U.S. Electronic Communications Privacy Act. The incident developed into an FTC investigation, a class action suit in federal court by the user group Electronic Privacy Information Center (EPIC), and investigations by 10 state attorney-generals. All legal action was resolved in 2002.

principles.[16] Table 1 contrasts the FTC principles with these industry self-regulatory guidelines.

Since the second half of the 2000s, numerous controversies have erupted surrounding the privacy of targeted advertisements in the United States. Besides the DoubleClick incident, Facebook's services were at the center of a dispute in 2007[17] and behavioral advertising using deep packet inspection (DPI) technology deployed by NebuAd, AdZilla, and others has also been attacked.[18]

Table 1: Comparison of FTC principles and industry self-regulatory guidelines

	FTC	IAB	NAI	4A's
Applicable data	Data used to deliver advertising targeted to the individual consumer's interests. Exceptions provided for (1) data not passed into third-party hands, and (2) contextual advertising that does not store data.	Data utilized in interactive advertisements	Information for behavioral-targeting advertisements, multi-site advertising, and ad delivery and reporting (differentiation made between personally identifiable information and non-personally identifiable information)	Data associated with online behavioral advertisements. Exceptions provided for (1) data not passed into third-party hands, and (2) contextual advertising that does not store data.
Applicable businesses	• Web site publishers • Businesses that store data for behavioral	Interactive advertising businesses	Behavioral advertising businesses	• First Parties — Web site publishers • Third Parties — businesses that take data from Web

[16] Some examples: *Interactive Advertising Privacy Principles* from the Interactive Advertising Bureau (IAB); *The Network Advertising Initiative's Self-Regulatory Code of Conduct* from the Network Advertising Initiative (NAI); and *Self-Regulatory Principles for Online Behavioral Advertising* from the American Association of Advertising Agencies (4A's), which consists of the Association of National Advertisers (ANA), the Direct Marketing Association (DMA), the Council of Better Business Bureaus (CBBB) and IAB.

[17] Social network service operator Facebook was the target of user backlash when it launched Beacon, a function that shared behavioral data from external sites on Facebook. A class action lawsuit was filed against Facebook in the U.S. District Court for the Northern District of California. The lawsuit was settled in 2009.

[18] In this case, a class action lawsuit was filed in the U.S. District Court for the Northern District of California against NebuAd for its use of user Internet viewing behavior records for marketing purposes without user permission. The act was alleged to have violated the Electronic Communications Privacy Act, the Computer Fraud and Abuse Act, and various California laws. The lawsuit was suspended with NebuAd's bankruptcy in 2009. A lawsuit was launched against AdZilla and its parent corporation, Conductive Corporation, in 2009 for the same reasons as NebuAd.

	advertising			site publishers and deliver behavioral advertisements • Service Providers — providers of Internet access and providers of desktop application software such as Web browser "tool bars"
Principles				
Transparency and consumer control	• Requires Web site publishers to explicitly state that data is being collected and allow consumers to choose whether or not to have their information collected	• Requires explicit statements that data is being collected and that consumers can choose whether or not to have their information collected	Requires explicit notification that data is being collected and the provision of an opt in link or opt out link, depending on whether the information is personally identifiable	• Requires First Parties and Third Parties to abide by the transparency principle • Requires Third Parties to abide by the principle of consumer control
Reasonable data security and limited data retention of consumer data	• Requires any company that collects and/or stores consumer data for behavioral advertising to provide reasonable security for that data • Any company that collects and/or stores consumer data for behavioral advertising can retain data only as long as is necessary to fulfill a legitimate business or law enforcement need	Requires members to provide reasonable security for collected data relative to its sensitivity	• Requires members to provide reasonable security for collected data relative to its sensitivity • Members can retain data collected only as long as necessary to fulfill a legitimate business need, or as required by law	• Requires Service Providers to abide by the principle of data security
Affirmative express consent for material changes to existing privacy promises	Requires any company that collects and/or stores consumer data for behavioral advertising to obtain affirmative express consent from consumers for material changes to existing privacy	No applicable principle	Members shall obtain consumer consent through opt in or opt out means depending on whether personally identifiable information or non-personally identifiable	Requires all parties to abide by the principle of material changes to existing policies and practices

	promises		information is being handled	
Affirmative express consent to (or prohibition against) use of sensitive data	• Requires companies to collect sensitive data for behavioral advertising only after they obtain affirmative express consent from the consumer • Sensitive data has not been strictly defined and the FTC is continuing to solicit opinions on its definition	No applicable principle	• Requires reasonable data security be provided depending on the sensitivity of that data • Additionally requires parental consent to collect personal information on children	Requires all parties to abide by the principle of sensitive data • Additionally requires parental consent to the collection of personal information on children
Other principles not in the FTC principles		• Requires accountability to government bodies • Requires reasonable efforts to educate consumers (Education principle)	• Requires reasonable efforts to educate consumers (Transparency principle)	• Requires all parties to make efforts to educate consumers (Education principle) • Requires entities to revise and improve principles (Accountability principle)

Source: Taken from pages 110 and 111 of the March 2010 report by the Study Group on the Economic Benefits of Behavioral Advertising and User Protection, commissioned by the Ministry of Internal Affairs and Communications' Institute for Information and Communications Policy.

(2) Europe

As in the United States, attention is being paid in Europe to privacy concerns with lifelog-monitoring services and behavioral advertising. One manifestation of these concerns was the Telecoms Reform Package, adopted by the European Parliament, in November 2009, which obliged telecoms to provide clear, prior notification about the use of cookies and personal information.[19]

[19] The European Parliament's decision obliges EU member states to implement the package in domestic law within 18 months.

Within Europe, the United Kingdom has been at the center of behavioral advertising and privacy controversy. In one case, the European Commission opened infringement proceedings[20] against the U.K. firm Phorm in 2008 on suspicions its behavioral advertising services that relied on deep packet inspection breached the 1995 European Directive on Protection of Personal Data and the 2002 European Directive on Privacy and Electronic Communications, among other EU laws. The commission also pointed out several structural problems with U.K. law as well: namely (1) that UK does not have an independent national supervisory authority dealing with communication interceptions; (2) that under U.K. law interception is considered to be lawful when the interceptor has reasonable grounds for believing that consent to interception has been given; and (3) that only intentional interceptions are considered an offense.

The trade association Internet Advertising Bureau (IAB), also in the U.K., released *Good Practice Principles for Online Behavioural Advertising*. The guideline includes principles on notice of data collection, user choice, user education, and sensitive information segments.

[20] In this case, it was revealed that Phorm in 2008 provided behavioral advertising technology using deep packet inspection to leading ISPs in the United Kingdom, including BT, VirginMedia, and TalkTalk. Prior to this, the company had conducted trials of the technology with BT in 2006 and 2007.

4. Legal Concerns in Japan

As we saw in Chapter 2, advances in networked and mobile devices have enabled companies to actively monitor lifelogs and other online data for behavioral advertising, statistical analysis, and other applications. At the same time, such lifelog-monitoring services have triggered concerns about the protection of personal information and privacy. This chapter examines the legal issues lifelog-monitoring services face along these two lines.

It is important to revisit the point we made previously that lifelog-monitoring services are constantly transforming, developing, and diversifying, often in unpredictable ways, and as such it is difficult at present to firmly demarcate the boundaries of these services. For this reason we decided to look at legal concerns in Japan in the context of the most mainstream lifelog-monitoring services: behavioral advertising, content recommendation functions, and location-based personalized assistance services.

(1) Relationship with the Personal Information Protection Law

The Act Concerning Protection of Personal Information (the Personal Information Protection Law) imposes a number of obligations and requirements on “business operators handling personal information” with respect to the handling and treatment of “personal information,” “personal data,” and “retained personal data.” Where lifelog-monitoring businesses fall under the Law’s “business operators handling personal information” definition, they are subject to the obligations[21] stipulated in Article 15 and subsequent articles.

This section examines whether the obligations in the Personal Information Protection Law apply to providers of behavioral advertising and similar applications as “business operators handling personal information.” To be classed as a business operator handling personal information, a provider must be “using a

[21] The Law stipulates numerous obligations according to the type of information being handled. Article 15 — *Specification of the purpose of utilization*, Article 16 — *Restriction by the purpose of utilization*, Article 17 — *Proper acquisition*, and Article 18 — *Notice of the purpose of utilization at the time of acquisition* relate to the treatment of personal information. Article 19 — *Maintenance of the accuracy of data*, Article 20 — *Security control measures*, Article 21 — *Supervision of employees*, Article 22 — *Supervision of trustees*, and Article 23 — *Restriction of provision to a third party* relate to the treatment of personal data. Article 24 — *Public announcement of matters concerning retained personal data*, Article 25 — *Disclosure*, Article 26 — *Correction*, and Article 27 — *Discontinuance of the use* relate to the treatment of retained personal data.

personal information database, etc. for its business."[22] We first studied whether the information such providers deal with meets the definition of personal information to determine this. This led us to consider whether providers' business-use databases are "an assembly of information including personal information" and "an assembly of information systematically arranged in such a way that specific personal information can be retrieved by a computer" from the definition of a personal information database in Article 2-2.

A. Do providers of behavioral advertising and similar applications handle personal information?

i. What is personal information?

Article 2-1 defines "personal information" as "information about a living individual which can identify the specific individual by name, date of birth, or other description contained in such information (including such information as will allow easy reference to other information and will thereby enable the identification of the specific individual)." Thus, the state of being personally identifiable is a necessary condition of "personal information."

ii. Application to behavioral advertising and similar applications

Behavioral advertising and similar applications usually only require (a) logs of Web actions and habits (browsing, purchases, etc.) needed to predict consumer preferences and interests, (b) location information and (c) IDs generated with cookies needed to acquire action logs and serve advertisements, or (d) subscriber IDs to identify mobile devices. Except in special circumstances or situations, this information alone is not personally identifiable. Thus, providers of behavioral advertising and similar applications are normally not believed to be business operators handling personal information.[23]

Nevertheless, information types (a), (b), (c), and (d) can become personally

[22] However, entities with personal information databases for business purposes that have no more than 5,000 specific individuals identified by the personal information that makes up all or part of the personal information databases on any day in the last six months are excluded. (From Article 2-3 in the Personal Information Protection Law and Article 2 in the Cabinet Order for the Enforcement of the Act Concerning Protection of Personal Information.)

[23] It goes without saying that if a provider of behavioral advertising or similar applications maintains other personal information databases for business use other than behavioral advertising, the provider is considered a business operator handling personal information.

identifiable when retained information permits the identification of a specific individual through simple reference to other information. For instance, if it is an easy matter to link a database of (e) subscriber names and other subscriber information with type (a), (b), (c), or (d) information, then the information attains the state of being personally identifiable. (Table 2 summarizes the situations in which information handled by providers of behavior advertising and similar applications is recognized as being personally identifiable.) Furthermore, type (a), (b), (c), and (d) information is considered personal information even if acquired from a third party if the potential exists that specific individuals can be identified through simple pairing with relevant auxiliary data (so-called re-identification).[24]

Moreover, type (a) information on Web actions and habits (browsing, purchases, etc.) may acquire the state of being personally identifiable if collected in sufficient amounts over a sufficiently long period. Similarly, it is possible to infer who a specific individual is if type (b) location information is stored chronologically over a sufficiently long period.

[24] Whether information is personally identifiable or not is a relative decision based on individual businesses' circumstances. See Hisamichi Okamura, "Personal Information Protection Law". Revised Edition. (Shoji Homu, 2009), page 76.

Table 2: Information obtainable from consumers by providers of behavioral advertising and similar applications

	Information Type	Contained Information	Personally Identifiable
Information required for behavioral advertising and similar applications	(a) Logs of Web actions and habits (browsing, purchases, etc.)	Logs of a user's Web browsing habits, purchasing habits, search queries, and other actions	Under normal situations, not considered personally identifiable information (It may be possible, however, to surmise a specific individual in some situations if logs of Web actions and habits are accumulated in sufficient amounts over a sufficiently long period.)
	(b) Location information	Location information measured with a GPS sensor on a mobile device or car-navigation system	Under normal situations, not considered personally identifiable information (It may be possible, however, to surmise a specific individual in some situations if location information records are accumulated chronologically over a sufficiently long period.)
		Location registration information sent from a mobile device to a base station	
	(c) Cookie-generated IDs	Information that sites providing Net-based services, such as portal sites or CGM sites, use to identify users (strictly speaking, browsers) who do not log into the site	Not considered personally identifiable information
	(d) Subscriber IDs	Information sent to a Web site when a user views a Web site from a mobile device that identifies the browser or device[25]	Not considered personally identifiable information[26]

[25] The function and use of subscriber IDs varies among mobile phone carriers.

[26] It has been pointed out that since the same subscriber ID is sent to multiple content providers, it is a very easy task to collect and cross-reference the separate Web habit and location information records held by each content provider under the same ID. It has also been indicated that logs of Web habits and actions accumulated under the same subscriber ID could easily acquire the state of being personally identifiable because it is a simple matter for content providers to link subscriber IDs to subscriber records and other personal information.

Information not necessarily required for behavioral advertising and similar applications	(e) Name, address, and other subscriber information	Information the e-commerce operator or telecom obtains from the subscriber when signing up for e-commerce or telecom services. These records usually include name, gender, address, age, and telephone number as well as credit card details and other personal credit information.	Considered personally identifiable information
	(f) ID information used for logging in	Information used by sites providing Net-based services, such as portal sites, CGM sites, and e-commerce sites, to identify users at log in	Not considered personally identifiable information unless the user includes their name or other personally identifiable information in the ID proper

B. Do providers of behavioral advertising and similar applications collect an assembly of information systematically arranged in such a way that specific personal information can be retrieved by a computer?

Our investigation in Section (a) above found that, under normal conditions, the information acquired and used by providers of behavioral advertising and similar applications is not personal information. However, such providers do maintain personal information databases for business use in the previously mentioned exceptions where the information they handle is considered personal information.[27] The personal information database definition also applies when providers manage elemental information fields including type (e) information in such a way that they can be linked and retrieved by a computer.

C. Summary

Providers of behavioral advertising and similar applications are generally not thought to be business operators handling personal information, as legally defined, because the information they handle is, itself, not personal information. Nevertheless, there are exceptions to this conclusion where providers of behavioral advertising and similar applications do fall under the categorization of business operators handling personal information and, as such, are required to manage the information they handle according to the provisions of the Personal Information Protection Law. These exceptions occur when elemental information fields can be linked and retrieved by a computer, enabling the identification of specific individuals. Examples include cases where information types (a), (b), (c),

[27] Normally in these cases the database is also considered an assembly of information including personal information.

or (d) can be easily associated and used with databases of (e) names and other subscriber information and cases where (a) records of Web habits (browsing histories and purchasing histories) are amassed in sufficient number over a sufficient long period from which the identity of a specific individual can be inferred.

Reference: Anonymization

In our examination of services providing behavioral advertising and statistical information, we studied approaches by some businesses to anonymize[28] personally identifiable information because they do not necessarily need to identify individuals. By removing, or scrubbing, personal-related information from the data, it is felt that the data can be shared and utilized with a higher degree of confidence.

Personally identifiable information consists of information like (e) subscriber information that is, itself, personally identifiable information. Personally identifiable information can also be generated in some cases from consumers' (a) Web habits, such as browsing, purchasing, and search histories.

We studied various anonymization methods, including k-anonymization,[29] as approaches to avoid the risks associated with personally identifiable information. Because of issues raised with anonymization techniques and the difficulty in completely and objectively de-identifying information, there is no alternative but to make decisions about anonymization on a case-by-case basis.

---

[28] Strictly speaking, there are two methods of anonymizing information. The first, non-linkable anonymization, completely erases any personally identifiable fields, such as subscriber information, from the target information. The second, linkable anonymization, replaces personally identifiable fields with numbers or symbols. The first method scrubs the information of any personal traits and the output information is not considered personal information. The second method is not so cut and dried: the information output by the anonymization process may or may not be personal information. If specific individuals can be identified by pairing the replacement numbers or symbols with other data, the information is personal information. For a more in-depth discussion, see *Guidelines for the Protection of Personal Information for Business Operations Handling Personal Genetic Information* (Ministry of Economy, Trade and Industry, 2005).

[29] K-anonymization is the process of creating a state, known as k-anonymity, within a database in which every combination of values of quasi-identifiers — information that can be exploited to identify or restrict the uncertainty about an individual through linking with other data — can be indistinctly matched to at least k individuals. This is done by generalizing or making ambiguous a portion of the data records — e.g., the browsing history.

At the same time, we understand that business operators handling personal information do not need to identify anonymization as a “purpose of utilization” under the Personal Information Protection Law since the removal of personal traits from information through anonymization does not constitute a use of personal information.[30]

The intent of the specification of the purpose of utilization (Article 15)[31] provision in the Personal Information Protection Law is twofold: to restrict the unnecessary or unwarranted handling of personal information, and to form an environment that encourages transparency in the handling of personal information and that empowers individuals to take steps to protect themselves from infringements on their rights and interests.[32] Anonymization, however, poses very little risk of infringement on the rights and interests of individuals. If anything, not obliging companies to specify anonymization as a purpose of utilization is thought to be more in tune with the spirit of the law.

Because this point has not been clarified sufficiently, we seek a complete exposition in the commentary to the *Guidelines on Personal Information Protection for Telecommunication Business Operators* (Ministry of Internal Affairs and Communication Ordinance 695 of 2004).[33]

---

[30] Aside from Article 15 — *Specification of the purpose of utilization*, there are other obligations on business operators handling personal information with respect to purpose of utilization, including Article 16 — *Restriction by the purpose of utilization* and Article 18 — *Notice of the purpose of utilization at the time of acquisition*.

[31] Specification of the purpose of utilization is provided for in Article 5 of the *Guidelines on Personal Information Protection for Telecommunication Business Operators*.

[32] See “Commentary on the Personal Information Protection Law” (Gyosei, 2003) by Shizuo Fujiwara and the Study Group on Personal Information Protection Legislation, edited by Itsuo Sonobe.

[33] One guideline that determined that anonymizing processes do not need to be specified as a purpose of utilization is the *Guidelines for the Proper Handling of Personal Information in Business Enterprises Involved in Medical Treatment and Care* (Ministry of Health, Labour and Welfare, December 2004).

(2) Relationship to privacy issues

While Japan has no over-arching law that deals specifically with privacy, privacy has been recognized as a personal interest that should be legally protected through case law and legal precedents.

The landmark case dealing with privacy infringement was the *Utage no Ato* [After the Banquet] case, concerning the Yukio Mishima novel of the same name.[34] In its September 28, 1964, decision, the Tokyo District Court defined privacy rights as "the legal guarantee and right not to have one's private life revealed publically without warrant." The court decision also set three necessary conditions for the recognition of a privacy violation: "(1) the contents disclosed concern those which are the facts of his/her private life or seemingly so; (2) ordinary people will not expect such information to be disclosed if put in the plaintiff's situation; and (3) the facts are unknown to society at large and thereby the plaintiff experiences tangible unease or insecurity by their disclosure."

The three *Utage no Ato* tests for determining privacy infringement cases were employed in court decisions for many years after 1964. More recently, however, the scope has been enlarging of what information should be considered private. In the case[35] concerning Waseda University's disclosure to the police of information about people attending a controversial lecture, the Supreme Court ruled on September 12, 2003, that even though the names, addresses, telephone numbers, and other information disclosed were simple personally identifiable information, "it is natural that a principle would not want information to be disclosed to others whom the person would not inform otherwise, and because this expectation should be protected, the personal information involved in this case should deserve legal protection as the Appellants' private information." As this shows, the three privacy tests of the *Utage no Ato* case are no longer necessarily followed in current decisions.

A. Potential for privacy infringement and its extent

[34] A decision by the Tokyo District Court on September 28, 1964.
[35] A decision by the Second Petty Bench of the Supreme Court on September 12, 2003.

As discussed above, behavioral advertising and similar applications usually involve the collection and utilization of Web habits (browsing and purchasing histories), location information, and similar kinds of data.

Because the accumulation of a sufficiently thorough Web browsing and purchasing history about a person makes it possible to surmise that person's interests, preferences, views, and ideologies, records on Web habits are considered highly confidential information involving intimate personal matters.[36] Similarly, if location information can be linked chronologically over a sufficiently long period, it is quite possible to determine much about the person's lifestyle. It is natural, then, to suppose that the person in question would not like this information to be made known to others without a legitimate reason. Thus, records of Web habits and location information, depending on how they are handled, are potentially subject to the legal protection afforded to private information.

Some commentators have suggested that records of Web habits and location information cannot infringe upon a specific individual's privacy because such information is, generally, not personally identifiable information.[37] Certainly, when a person's preferences, interests, and lifestyle are revealed only to a limited degree and it is impossible for another person to determine whose information it is, then we agree that infringement of a specific individual's privacy is very unlikely. Nevertheless, despite records of Web habits not being personally identifiable information, it is possible to identify a person if a sufficient number of records are amassed and such records may become personally identifiable if they are circulated broadly. Therefore, it is not correct to think that because a certain data set is not currently personally identifiable, the need for privacy protection is completely relinquished.

---

[36] The First Petty Court of the Supreme Court, in its March 6, 2008, ruling on the Juki Net residency registry network case, dealt tangentially with the question of whether the information managed and used on the registry "should be regarded as highly confidential information involving intimate personal matters." The court made the level of protection a decision factor. See Hisamichi Okamura, "Personal Information Protection Law". Revised Edition. (Shoji Homu, 2009), page 35.

[37] The Niigata District Court referred to a link between privacy and information being personally identifiable in its May 11, 2006, opinion on the Defense Agency list case: "In order to conclude that the plaintiffs' privacy has been violated, it is necessary that the personal information on the plaintiffs contained in the list be personally identifiable."

Although a comprehensive analysis of how the lifelogs are treated is needed to determine the possibility and extent of privacy infringements, there is considerable variety in the handling of lifelogs for the provision of behavioral advertising and similar applications. Therefore, the only alternative is to make decisions on a case-by-case basis. Studies of the most common scenarios — for example, the accumulation of Web viewing behaviors or location information over a sufficiently long period to enable detailed analysis of a specific individual's preferences or lifestyle — indicate the potential for privacy infringements. Furthermore, the sharing of Web browsing habits or location information with third parties without the consumer's permission or the release of that information on the Internet also invites the possibility of privacy infringements.[38]

In light of these considerations, businesses should make reasonable efforts to reduce the risk of privacy infringement, such as ensuring transparency in the treatment of Web browsing histories or location information and providing consumers with the means to stop the use or collection of their information.[39]

B. Consumer concerns

Even if, hypothetically, certain information is not personally identifiable and does not constitute any sort of privacy infringement or violation, the fact that the consumer does not know how the information is being handled or the fact that the consumer cannot control how the information is handled can cause concerns when, for the consumer in question, the information — such as information

[38] One privacy-related issue is violations of the right to control the usage of one's likeness, or so-called "portrait rights." The First Petty Bench of the Supreme Court wrote in November 10, 2005: "Any person has a legally protected personal interest not to have his/her face or appearance photographed without good reason, and whether or not an act of photographing a person's face or appearance without consent should be deemed to be a tort should be determined by examining whether or not the photographed person's personal interest has been injured beyond the tolerable limit in social life, while taking various factors into consideration such as the photographed person's social status, the photographed activity, the place, purpose, manner, and necessity of photographing." This opinion set out criteria for judgments including conditions for exemptions from illegality.

[39] The Tokyo District Court, in its February 20, 2004, ruling on the question and extent of privacy violations by the construction of a multistory apartment building on adjacent residents, noted that the defendant (the building administrator) had changed the building's handrails and window glass and installed blinds in response to demands by the plaintiffs (the adjacent residents) and wrote that "the Court recognizes that the company took reasonable concern and effort to protect [the adjacent residents'] privacy and, therefore, does not recognize that the plaintiffs' privacy has been injured beyond a tolerable limit."

identifying a handset, device, or browser — is self-evidently his or hers. Even the simple collection of Web browsing habits can invite concern if the consumer cannot participate in the data handling process or if the business does not ensure the data handling process is transparent.

For this reason again, businesses should make reasonable efforts to reduce consumer concerns and promote the smooth development of their services, such as improving the transparency in their treatment of Web action records and location information and provide consumers with the means to stop the use or collection of their information.

C. Summary

This section has shown that lifelog-monitoring services, depending on their circumstances, can violate privacy rights or provoke consumer concerns. But if a business takes reasonable steps to preserve privacy, it can limit the likelihood of infringing upon privacy rights and significantly reduce consumer concerns. Accordingly, we call on businesses to account for these concerns in their handling of lifelogs in order to promote the provision of services that consumers can trust.

This chapter has focused mainly on behavioral advertising and similar applications. The next chapter examines general considerations for services that collect and use lifelog data.

5. Creating More Trustworthy Services (proposal of consumer-centric principles)

As our discussion to this point has shown, lifelog-monitoring services, depending on their circumstances, can violate privacy rights and provoke consumer concerns. Consequently, it is preferable that businesses collecting, storing, and utilizing lifelogs take consumers into consideration and that they devise strategies and practices that account for consumers in order to provide better, more trustworthy services.

One possible means of affecting this is to have administrative bodies draw up guidelines and procedures on the practices businesses should follow. This idea was rejected, however, because lifelog-monitoring services are in their infancy and it is not wise to place excessive burdens on businesses that will hamper their growth. Instead, it is better to encourage businesses to draft their own self-regulatory guidelines instead of applying administrative guidelines that strongly resemble regulations. The Study Group decided, then, to establish a set of informal, consumer-centric principles to serve as a roadmap for businesses to formulate their own guidelines. We expect businesses[40] to draw up their own guidelines in reference to our consumer-centric principles while adding provisions tailored to their own business circumstances and needs.[41]

These consumer-centric principles will have to be revised periodically, since lifelog-monitoring services are expected to develop rapidly in the coming years in tandem with technological innovations and since international harmonization will become necessary due to the borderless nature of these services. To encourage efforts by businesses in this area, the Ministry of Internal Affairs and Communications must periodically review initiatives by businesses based on these principles and announce the findings.

(1) Scope

---

[40] Some specific businesses envisioned at the present time are advertisers that serve targeted advertisements, e-commerce sites that operate recommendation functions, Internet service providers that serve targeted advertisements using deep-packet-inspection technologies, and mobile phone companies that offer personalized assistance services.

[41] The FTC used the same approach as our consumer-centric principles in its *FTC Staff Report: Self-Regulatory Principles For Online Behavioral Advertising*, a document of fundamental principles for businesses to refer to when creating their own guidelines.

A. Applicable information

The consumer-centric principles apply to information that can identify a specific terminal, device, or browser (“device,” hereafter). The principles apply to such information regardless of whether the information is considered personal information under the Personal Information Protection Law.

For example, the principles apply to the following types of information: IDs generated by cookies or similar techniques, subscriber IDs associated with mobile phone handsets, login IDs that identify users, device serial numbers, and other ID data such as MAC addresses or IC tags. The scope also includes any information — such as browsing histories, search histories, and purchasing histories — that can be bound to IDs identifying devices.

We have shown that much of the information handled in the provision of lifelog-monitoring services is not personally identifiable. It is true that handling non-personally identifiable information poses relatively little risk of violating the privacy of specific individuals, but this is not equivalent to believing such use is completely free of privacy concerns. For example, information, by being broadly circulated over the Internet, may become personally identifiable. Furthermore, it may be possible to infer the identity of a specific individual if enough information is amassed. And even if the information is not personally identifiable from the standpoint of the business handling the applicable information, for the person in question the information may be self-evidently his or hers. Therefore, not being able to participate in or control the handling of this information invites concerns.

On the other hand, it is felt that information which cannot be used to identify specific devices poses virtually no risk of becoming personally identifiable or violating privacy even if it is linked with other information or if large volumes are accumulated. Moreover, there is very little possibility of sparking consumer concerns because consumers are not going to recognize information this general as their own.

It goes without saying that businesses must in addition abide by the Personal Information Protection Law and related guidelines if the applicable information is classed as personal information under the law.

B. Applicable businesses
The consumer-centric principles apply to businesses that utilize applicable information for business purposes (excluding business uses where applicable information is not stored or accumulated in any way).

Here, “business” refers not only to similar acts performed iteratively or repetitively to achieve a given objective but also to acts that are commonly recognized by society as being business activities. For example, individuals who publish their own Web sites or blogs may collect, store, and utilize applicable information, but ordinarily this act is not considered a business activity unless the individual is running an e-commerce site or other business. Therefore, such individuals are not included in the businesses that the consumer-centric principles apply to.[42]

The consumer-centric principles should not apply to services that do not store or accumulate applicable information since it is highly unlikely they could violate individuals’ privacy or cause consumer concerns. The ability of such services to identify consumer preferences or interests is very limited and the applicable information is not stored.[43]

(2) Consumer-centric principles
There are six specific consumer-centric principles.

A. Publicity, promotion, and education activities
B. Assurance of transparency
C. Assurance of opportunities for consumer participation
D. Assurance of data collection by appropriate means
E. Assurance of adequate security controls
F. Assurance of frameworks to address complaints and inquiries

[42] It is conceivable that private individuals, who are not in business, may collect, store, and utilize large amounts of applicable information. Although such individuals are not included in the scope of applicable businesses, it is preferable that they also establish their own privacy policies based on the consumer-centric principles.

[43] Search contextual advertising is held to be an example of a service that does not accumulate applicable information. (Search keywords are usually not stored in contextual advertising linked to search queries.)

The following sections go into more detail about the specific provisions of each principle.

A. Publicity, promotion, and education activities

> Applicable businesses and related entities shall endeavor to take part in publicity and other education activities about the operation of their services that utilize applicable information and about initiatives based on the consumer-centric principles in order to help raise consumer literacy and dispel consumer concerns and anxieties.

This principle calls for businesses that handle applicable information and their related entities to participate in publicity, promotion, and education efforts. This principle can be divided into two main parts: publicity, promotion, and education activities directed at consumers and publicity, promotion, and education activities directed at lifelog-monitoring businesses. Pursuing these two publicity streams in tandem is expected to help raise consumer literacy and dispel consumer concerns. Groups considered related entities in this context include consumer groups, public-service organizations, and central and local government bodies.

The purpose of consumer-directed publicity activities is to more effectively achieve the objectives of the second principle, transparency. Businesses operating lifelog-monitoring services rely on lifelog data gathered from consumers. In the interest of privacy and personal information protection, however, the decision whether lifelog data is collected or not should be left to each consumer. At the same time, service operations should be made sufficiently transparent so consumers have a firm basis on which to make their decision. Therefore, the Study Group decided to encourage businesses to disclose the nature of their services to consumers in order to ensure transparency. (See B. Assurance of transparency below.)

The principle of publicity was included because it was felt consumer awareness of lifelog collection is low. To avoid businesses and related entities settling for only passive service transparency, we decided to call on them to participate in actively publicizing, promoting, and educating consumers about their service operations.

The second part of this principle — publicity, promotion, and education activities directed at lifelog-monitoring businesses — was established because the majority of lifelog-monitoring businesses do not adequately account for consumers when collecting, storing, and utilizing lifelog data. It is hoped that if businesses and related entities that already have guidelines consistent with the consumer-centric principles in place will publicize, promote, and educate about the principles to businesses with an inadequate consumer focus, it will result in more businesses drawing up guidelines consistent with these principles and consequently serve to alleviate consumer concerns about the industry in general.

B. Assurance of transparency

> Applicable businesses and related entities shall endeavor to inform consumers or otherwise put into a knowable state for consumers ("disclosures," hereafter) about the details of applicable information collection, storage, and utilization and of the means of consumer participation. Applicable businesses and related entities shall endeavor to make disclosures clear and understandable to consumers.

We have already stated that the decision about whether to provide lifelog data to a business should rest with the consumer. To enable consumers to make informed decisions, businesses should ensure that their service operations, including means of consumer participation, are transparent. The Study Group decided to call on businesses to disclose their service operations to consumers to ensure a suitable level of transparency. This principle — together with the assurance of opportunities for consumer participation, the third principle — encourages businesses to properly handle applicable information and forms the core of the six principles.

After surveying domestic and foreign guidelines[44] on online behavioral advertising and recommendations and the current practices by industry leaders, we believe[45] businesses should, as a minimum, disclose to consumers or

[44] Specifically, from Japan, *Behavioral Advertising Guidelines* (Japan Internet Advertising Association, June 2009), and from the United States, *Self-Regulatory Principles for Online Behavioral Advertising* (American Association of Advertising Agencies et al., July 2009).

[45] Some Study Group members indicated that businesses should make it possible for consumers to readily recognize which advertisements are targeted advertisements utilizing applicable information.

otherwise put into a knowable state for consumers: i. the fact that data is being collected; ii. the name of the business or organization collecting the applicable information; iii. the type or category of data collected; iv. the method of collection; v. the fact that collected data will be shared with third parties; vi. the scope of entities that will be provided with collected data; vii. the type or category of data provided to third parties; viii. the purpose of use; ix. the storage period;[46] and x. the means of consumer participation.

The intent of this principle, that transparency be ensured, is not satisfied if a business does disclose its applicable information collection, storage, and utilization and the means of consumer participation but in a manner that is confusing or difficult to recognize. Consequently, businesses should make disclosures easy for consumers to recognize and understand.

As for the actual presentation of disclosures that are easy for consumers to recognize and understand, businesses should aim to state the facts relating to the data collection briefly and conspicuously, such as them on the collector's privacy policy page.

Third-party collection of applicable information or third-party advertisement or Web beacon delivery creates a problem for behavioral advertising services. When the advertisement publisher, applicable information collector, and advertisement server are all separate businesses, transparency is not ensured by simply disclosing the data collection on the Web sites of the applicable information collector or advertisement server because it is difficult for consumers to find the disclosure. In such cases, the advertisement publisher should disclose on its Web site that third parties collect applicable information and serve advertisements. The advertisement publisher should also provide a link to a page listing the name of the collecting business and details about the data collection.[47]

C. Assurance of opportunities for consumer participation

---

[46] There are two storage periods: the period of ongoing device identification and the period collected applicable information is retained.

[47] The Study Group received opinions that applicable information collection and advertisement serving by third parties tend to have greater privacy implications and, therefore, collectors of applicable information should disclose the Web sites from which they collect data.

Applicable businesses shall endeavor to provide consumers with the means to stop the collection or use of applicable information, or otherwise participate in the handling of their information, according to the characteristics of their business.

This principle calls on businesses to provide consumers, who are in the position of having the most knowledge about applicable information relating to them, with the means to participate in the handling of information in the interest of preventing and correcting privacy violations or improper handling of personal information caused by erroneous handling of applicable information. This principle assumes that the transparency principle has been properly implemented.

Provision of the means to stop[48] the serving of targeted advertisements is currently gaining traction in the industry. Normally, an opt-out cookie is issued that indicates the browser has refused delivery of targeted advertisements. The problem with this method is that the opt-out indication is deleted when cookies are cleared from the browser. Similarly the opt-out cookie must be reissued if the consumer uses a different browser, replaces his or her handset, or reinstalls the operating system. We ask that businesses explain to consumers the limitations of opt-out cookies.

One alternative means of providing consumer control that has been seen occasionally is rejecting or clearing cookies associated with behavioral advertising. Explanations about this have been found in privacy policies and other similar pages, and there are Web sites detailing methods of blocking or clearing certain cookies. Because rejecting or clearing cookies makes it impossible to identify the browser, collected information cannot be accumulated in the way applicable information can. Businesses considering this approach, however, must factor in the difficulty to reject individual cookies with normal browser settings.[49]

In the area of mobile phone Internet, Web sites have been seen explaining how to hide one's mobile phone subscriber ID. Hiding the subscriber ID makes it impossible to identify the browser and thus collected information cannot be

[48] Normally, non-targeted advertisements are delivered in place of targeted advertisements.

[49] Windows Internet Explorer 8 is standard equipped with a function to block individual cookies. Mozilla Firefox Version 3.x and Google Chrome 4.0.249.89 can block individual cookies with add-ons.

accumulated in the way applicable information can. The problem here, again, is businesses must consider that many sites and services cannot be used if the subscriber ID is hidden.

In light of the argument above, we ask that businesses provide comprehensive means, according to the characteristics of their business, for consumers to participate in the handling of their information. This includes providing the means to cancel the delivery of targeted advertisements as well as cookie rejection and deletion. The provision “according to the characteristics of their business” was included because there is much diversity among lifelog-monitoring businesses, and thus the means for consumer participation should also be provided flexibly.

Businesses should provide means so that consumers can readily check the handling of their applicable information and stop its collection and usage.[50]

D. Assurance of data collection by appropriate means

Applicable businesses shall endeavor to collect applicable information by appropriate means.

Examples of inappropriate collection means include falsifying the collector or the scope of collected information (including collecting information from a much wider scope than the ordinary person would expect) and collecting information without the consumer’s knowledge. Such inappropriate collection means only serve to heighten consumer concerns about data collection in general. In the face of such incidents, it is imperative that integrity be assured from the collection stage, which is the starting point of data handling, in the interest of reducing concerns and gaining consumer confidence in the appropriate handling of applicable information. Therefore, this principle proposes that businesses collect applicable information through appropriate means only.

Since decisions on what appropriate means are are not universal, we leave them to the relevant laws and ordinances and to commonly accepted ideas.

[50] Some Study Group members were of the opinion that what was needed was the development of technical means so that consumers can readily check the handling of their applicable information and stop its collection and usage.

E. Assurance of adequate security controls

> Applicable businesses shall endeavor to take necessary and appropriate measures to prevent disclosures, destruction, and losses of applicable information they handle and to otherwise ensure the security and control of applicable information.

It is conceivable that entities obtaining applicable information illegally may provide it for questionable uses or cause massive privacy violations. For this reason, this principle calls on businesses that handle applicable information to exercise care and consideration to keep the applicable information from being disclosed, destroyed, or lost or coming to other harm.

F. Assurance of frameworks to address complaints and inquiries

> Applicable businesses shall endeavor to handle appropriately and promptly complaints and inquiries about the handling of applicable information.

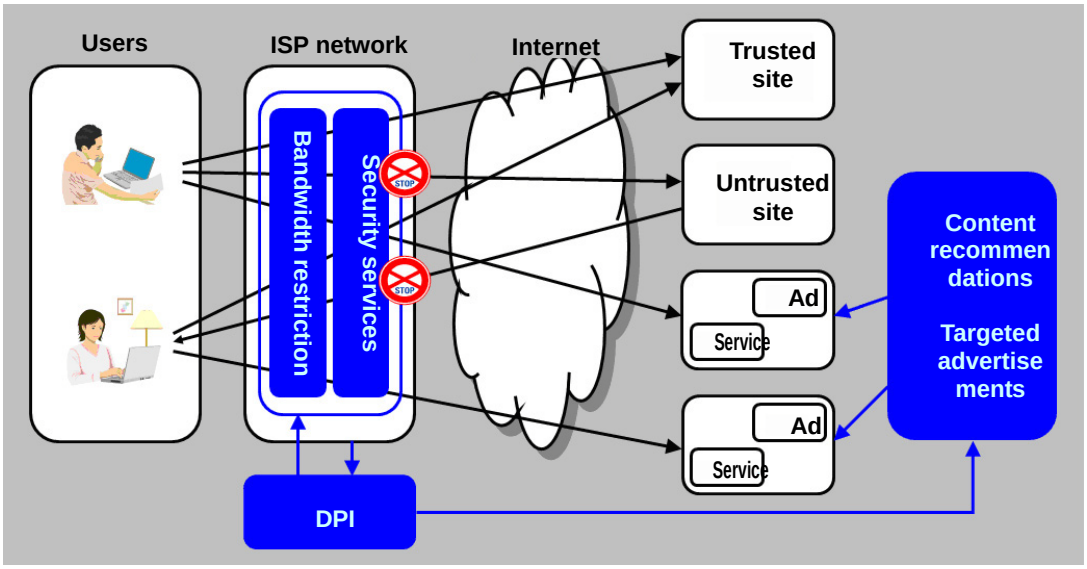
Problems or complications surrounding the handling of applicable information are essentially issues between individuals and, thus, businesses should attempt to resolve them promptly through discussions between the parties. For this reason, this principle calls on businesses to set up a contact point for questions and complaints about the handling of applicable information and to exercise care and consideration so that claims are processed quickly and appropriately.

6. Behavioral Advertising Using Deep Packet Inspection Technology

(1) Behavioral advertising using deep packet inspection technology

Behavioral advertising using deep packet inspection (DPI) technology is an advertising modality in which an Internet service provider (ISP) intercepts and inspects packets passing over its networks to predict customers' preferences and interests — information that is then used to deliver targeted advertisements to customers.[51] DPI usually refers to the technology that parses the headers and payloads of packets passing over a network and screens them for certain communication characteristics and behaviors. DPI has conventionally been used as an elemental technology for bandwidth restriction. But companies are now studying its use in advanced applications as an elemental technology in protection schemes against Internet threats that cannot be contained by firewalls and as an elemental technology for more refined behavioral advertising. DPI technology is expected to continue to grow and develop over the coming years.

Figure 1: Schematic of behavioral advertising using DPI



[51] Current DPI-based online behavioral advertising predicts preferences and interests based on information extracted from packets associated with HTTP requests and responses (access URLs or search queries from search engines) and delivers advertisements that match the predicted preferences and interests. The browser or device is identified with an ID generated from the IP address or similar fixed information.

(2) Legal issues

Because DPI-based behavioral advertising involves ISPs inspecting packets passing over their networks, it necessitates an examination of not only its relationship to the Personal Information Protection Law and privacy protection, which we looked at in Chapter 4, but also its relationship with protection of communication confidentiality. The sections below sort out DPI-based behavioral advertising's relationship with the confidentiality of communications, but clearly operators of DPI-based behavioral advertising must also take the Personal Information Protection Law and privacy protection into account as well.

A. Confidentiality of communications

The confidentiality of communications is enshrined as a fundamental human right in Article 21-2 of the Japanese Constitution because communications safeguard the freedom of individual's private lives and protect privacy, which guarantees the well-being of individual lives, and because communications are essential to human social activities.

> The Constitution of Japan
> Article 21-2
> No censorship shall be maintained, nor shall the secrecy of any means of communication be violated.

The Telecommunications Business Act, following the provisions of Article 21-2 in the Constitution, also safeguards the confidentiality of communications that are handled by a telecommunications carrier (Article 4-1). The Act sets out penal provisions for violating the confidentiality of communications (Article 179). Furthermore, the Minister for Internal Affairs and Communications can order a telecommunications carrier to improve its business operations if the carrier is found to be hindering the assurance of communication confidentiality (Article 29-1(i)). Together these provisions rigorously protect the confidentiality of communications.

> Telecommunications Business Act (Act No. 86 of 1984)
> Article 4
> (1) The secrecy of communications being handled by a

telecommunications carrier shall not be violated.
(2) Any person who is engaged in a telecommunications business shall not disclose secrets obtained, while in office, with respect to communications being handled by a telecommunications carrier. The same shall apply even after he/she has left the office.

Article 29
(1) Where the Minister for Internal Affairs and Communications finds that the business activities of a telecommunications carrier fall under any of the following items, the Minister may order the telecommunications carrier to improve the methods of conducting its business activities or take other measures within the limits necessary for ensuring the interests of users or the public interest:
(i) If there is hindrance in ensuring secrecy of communications with respect to the telecommunications carrier's methods of conducting its business activities

Article 179
(1) Any person who has violated the secrecy of communications being handled by a telecommunications carrier (including communications set forth in Article 164 paragraph (2)) shall be punished by imprisonment with work of not more than two years or a fine of not more than one million yen.
(2) Any person engaging in a telecommunications business who has committed the act set forth in the preceding paragraph shall be punished by imprisonment with work of not more than three years or a fine of not more than two million yen.
(3) An attempt at the offenses set forth in the preceding two paragraphs shall be punished.

In the above provisions, “being handled by a telecommunications carrier” refers to the state of being under the control and management of the telecommunications carrier from the time the sender issues the communication until the time the receiver receives the communication.

“Secrecy of communications” includes not only the content of the communication but also all particulars (constituent elements of a communication) — such as the time, date, and location of the communication, the name, address, location, phone

number, and other identifying information about the communication parties, the number of communications, etc. — from which the meaning or intent of the communication could be surmised. Entities engaging in a telecommunications business are obliged to protect the confidentiality of the communication itself and of personal information about the subscriber collected at the time of the service agreement and any information that could be used to surmise the meaning of the communication, even though this information is not a constituent element of a particular communication.[52]

Violations of the confidentiality of communications include “make knowable” — in which a third party who is not a party to the communication intentionally and willfully puts the confidential communications in a knowable state — “disclosure” — in which a third party places captured confidential communications in a knowable state for others — and “unauthorized use” — in which confidential communications are used for one’s own or another’s interest against the wishes of the sender or receiver. These are independently considered confidentiality violations.

B. Consent of communication parties

When consent of the communication parties is obtained, use of their communications for behavioral advertising is not in violation of the communication parties’ wishes and, thus, is not a violation of the confidentiality of communications. What is at issue is whether consent is fully informed, and therefore effective, consent since confidentiality of communications is a serious matter. Effective consent of communication parties is generally regarded as needing “separate” and “explicit” consent. For instance, Web site notices or provisions contained in a contract agreement are not considered sufficient for effective consent. Effective consent requires a method of explicit confirmation, such as including a separate provision in contracts for new users to consent to the collection of communicated information with DPI technology for use in behavioral advertising.

C. Does DPI-based behavioral advertising violate confidentiality of

[52] It should be noted that the penal provisions are limited to violations of the secrecy of communications (Article 179, Telecommunications Business Act).

communications?
ISPs use DPI-based behavioral advertising to inspect all packets associated with a consumer's HTTP requests and responses, estimate the consumer's preferences and interests, and serve the consumer with advertisements that match the estimated preferences and interests.

To check whether DPI-based behavioral advertising violates confidentiality of communications, we must first establish whether the inspected packets are being handled by a telecommunications carrier. ISPs inspect packets associated with communications between the sender — the consumer — and the receiver — the Web server (in responses, communications between the sender, or Web server, and the receiver, or consumer). These communications are under the control and management of the telecommunications carrier — the ISP. Consequently, the inspected packets are packets associated with communications being handled by a telecommunications carrier.

Next, we must establish whether the information monitored by DPI-based behavioral advertising includes constituent elements of a communication or its actual content. DPI-based behavioral advertising extracts and inspects URLs of Web pages the consumer accesses and search queries the consumer enters in search engines from all packets associated with the consumer's HTTP requests and responses. Clearly, this information includes constituent elements of a communication and the communication itself and therefore the confidentiality of this information is granted protection under confidentiality of communications legislation.

DPI-based behavioral advertising inspects packets and uses the results to serve targeted advertisements. The act of inspecting packets falls under "making known," and the act of using inspection results in serving advertisements falls under "unauthorized use." Hence, DPI-based behavioral advertising violates confidentiality of communications in two ways.

D. Is DPI-based behavioral advertising a justifiable act exempt from illegality?
The argument in the previous section shows that DPI-based behavioral advertising does constitute a violation of the confidentiality of communications where consumer consent is not obtained. In exceptional cases, however, where

specific reasons are recognized — such as justifiable acts (Article 35, Penal Code), self-defense (Article 36, Penal Code), and averting present danger (Article 37, Penal Code) — violations of the confidentiality of communications are exempt from illegality and are permissible. Reasons such as self-defense and averting present danger are hard to apply to DPI-based behavioral advertising, so we looked at justifiable acts as an argument for recognizing an exemption from illegality. Acts that conform with laws and regulations and acts in the performance of lawful business are not punishable as justifiable acts. Since DPI-based behavioral advertising is part of a private business's operations, it is not an act founded on any law or regulation. Therefore, the problem becomes whether it can be called an act in the performance of lawful business.

> Penal Code
> Article 35
> An act performed in accordance with laws and regulations or in the pursuit of lawful business is not punishable.

We looked for a common reasoning when violations of the confidentiality of communications by telecommunications carriers are considered acts in the performance of lawful business by examining a number of business operation cases. Cases of where confidentiality violations have been recognized as acts in the performance of lawful business include (i) acts whereby communication carriers use customer communication records for billing and invoicing purposes; (ii) acts required to maintain and sustain a communication business, such as an ISP using communication headers at a router to control routing; and (iii) acts (such as bandwidth restrictions on large-volume communications) that are measures needed for the stable operation of networks that are recognized as being appropriate in terms of the legitimacy of the purpose, the necessity of the act, and the appropriateness of the means. The fundamental rationale behind these exemptions was that the measures were deemed appropriate and necessary in view of providing telecommunication services smoothly to consumers — that is, nearly all citizens — taking into account the nature of communication services, which are a public key infrastructure shared by all citizens. Hence, these violations were recognized as acts in the performance of

lawful business.

In light of this reasoning, it is hard to conclude that the purpose of DPI-based behavioral advertising by ISPs — serving more relevant advertising and ascertaining consumers' interests to do so — is absolutely appropriate and necessary for their telecommunications services (which are, after all, the connecting of consumers to the Internet with telecommunication facilities). Thus, it is very unlikely that DPI-based behavioral advertising constitutes an act in the performance of lawful business.[53] [54]

E. Establishment of operating standards

As the argument above shows, DPI-based behavioral advertising is not permitted to violate the confidentiality of communications without consumer consent. In section B. we saw that consumer consent must be explicit and separate. Businesses engaged in DPI-based behavioral advertising should make their service mechanisms and operations sufficiently transparent to consumers so that consumers can make effective, informed consent. Accordingly, businesses should establish and apply operating standards or similar guidelines to ensure

---

[53] This point was touched on earlier in Footnote 10. One case, which centered on whether telecommunications carriers were obliged to stop threatening transmissions, provides a judicial precedent related to this matter. In the original sentence (a July 7, 2004, decision by the Osaka District Court), the written decision on the act of telecommunications carriers ascertaining and blocking threatening transmissions observed: (a) this is an act not only inappropriate to request communication carriers to carry out but also prohibitively illegal in view of the nature of a public communications carrier's duties; (b) the services expected to be provided by a telecommunications carrier are nothing more than the unaltered conveyance of communications from senders to receivers by physical communication media and means; (c) to ascertain whether a given transmission contains criminal intent, all transmissions would have to be inspected, which would mean an overwhelming number of consumers would have the confidentiality of their communications violated and would have an immeasurably adverse impact on the public; and (d) scrutinizing each transmission would cause contractions in the telecommunications industry and inhibit freedom of expression activities and the circulation of information. Although this decision did not judge whether the interception and ascertainment of transmitted content by a telecommunications carrier was an act in the pursuit of lawful business, to the extent we can extrapolate from the decision's reasoning, it is difficult to interpret the act of inspecting the content of transmissions as being an act in the pursuit of lawful business. Incidentally, the plaintiff's appeal was rejected in an appeals court decision (Osaka High Court, June 3, 2005).

[54] There are opinions that Article 35 of the Penal Code recognizes a general justifiable cause for noncompliance with the law, in addition to acts based on laws and regulations and acts in the pursuit of lawful business. Even if we were to agree with this opinion, referring to the previous footnote's decision on intercepting threatening transmissions, it is difficult to conclude that DPI-based behavioral advertising that involves the inspection of transmission content can be exempt of illegality on the grounds of a general justifiable cause for noncompliance with the law.

transparency. Some points businesses should follow in this regard are as follows:
i. Establish operating standards based on the consumer-centric principles and apply these to services, even for tests and trials.
ii. Notify consumers or otherwise put into a knowable state for consumers in a manner that consumers can easily recognize and understand at the very least items (i) to (x) from the transparency principle in the consumer-centric principles as a way of obtaining informed consent from consumers.
iii. Provide consumers with opportunities to easily opt out.

7. Conclusion

This Study Group believes it is necessary for businesses and other entities to address consumer privacy issues and consumer concerns in order to promote the further growth of lifelog-monitoring services. To this end, we presented consumer-consideration principles as an indication of how this can be accomplished. We are cognizant that this will be insufficient on its own to promote development in the lifelog-monitoring service field. Advancement of lifelog utilization will also be necessary.

We call on the Ministry of Internal Affairs and Communications to move ahead with further studies to advance lifelog utilization and to promote the further growth of lifelog-monitoring services.

June 3, 2010

Japan Internet Advertising Association (JIAA)

Behavioral Advertising Guidelines

First published in 2009

Revised in 2010

Chapter 1: General Provisions

Article 1 *Objective*

In connection to behavioral advertising that consists of the collection of data associated with Web behaviors by Internet users (“users,” hereafter) and the serving of targeted advertisements based on predictions made from the collected data, the Guideline’s objective is to establish an environment in which the usefulness of behavioral advertising can be demonstrated and in which secure Internet advertising can be deployed with the correct understanding of users and advertising sponsors by defining basic matters that Japan Internet Advertising Association (“JIAA,” hereafter) Members should follow in their behavioral advertising practices.

Article 2 *Scope and application*

(1) The Guideline shall apply to JIAA Members that utilize Web behavior data on users for business purposes.

(2) The Guideline shall apply to the serving of advertisements and shall not apply to the transmission or delivery of non-advertising content.

(3) The Guideline does not deal with “personal information” as defined in legal statutes concerning the protection of personal information. JIAA Members are to follow the Personal Information Protection Law and privacy guidelines in the handling of “personal information.”

Article 3 *Definitions*

The following terms where used in the Guideline shall take the respective definitions as given below.

(i) “Web behavior data”

The term “Web behavior data” shall mean Web viewing logs, e-commerce site purchasing records, and other data that when accumulated can be utilized to predict the preferences and interests of a user. Web behavior data does not necessarily have to be sufficiently comprehensive to identify a specific individual.

(ii) “Behavioral advertising”

The term “behavioral advertising” shall mean a service that, in tandem with accumulating Web behavior data,

predicts the preferences and interests of a user from Web behavior data and classifies each user in an audience segment, and serves Internet advertisements to each segment based on their relevance to that segment.

(iii) “ad publishing entity”

The term “ad publishing entity” shall mean a Member that owns a Web site on which targeted advertisements are published.

(iv) “Reporting entity”

The term “reporting entity” shall mean a Member that owns a Web site and provides Web behavior data collected from that Web site to an ad delivery business.

(v) “Ad delivery business”

The term “ad delivery business” shall mean a Member that receives Web behavior data from Web site publishers and serves targeted advertisements based on that data.

(vi) “Ad serving business”

The term “ad serving business” shall be a collective term for ad publishing entities, reporting entities, and ad delivery businesses.

Chapter 2: Principles on the Handling of Web Behavior Data

Article 4 *Assurance of transparency*

(1) Ad delivery businesses and ad publishing entities shall notify users or otherwise put into a knowable state for users the following matters (items (i) to (xiii) are required and item (xiv) is recommended; items (i) to (xiv) are referred to as “notification matters” hereafter) by some method, such as displaying the notification matters in a manner that users can easily recognize and understand in their privacy policy or other conspicuous location on their Web site.

(i) the fact of collection

(ii) name of the business collecting the applicable data

(iii) the types of data being collected

(iv) the collection method or methods

(v) the fact that data is supplied to third parties

(vi) the scope of data-receiving entities

(vii) the types of data being supplied

(viii) the purpose of use

(ix) the length of time the data will be retained

(x) the means of user participation

(xi) a statement that the data used is not personally identifiable

(xii) the policy on handling personal information (or a link to the policy)
(xiii) a statement of Guideline compliance as a participating company
(xiv) descriptions of each Member's respective user care and consideration efforts

(2) Ad publishing entities, in addition to the provisions of the previous paragraph, shall state that Web behavior data is being used for behavioral advertising in their privacy policy or other conspicuous location on their Web site.

(3) Ad publishing entities, in addition to the provisions of the previous two paragraphs, shall endeavor to notify users or otherwise put into a knowable state for users the notification matters by placing a link near spaces where targeted advertisements are posted that points to a page describing the notification matters (either a page on their Web site or a page on the relevant ad delivery business's Web site).

(4) Reporting entities shall state that Web behavior data is being used for behavioral advertising in their privacy policy or other conspicuous location on their Web site. Furthermore, reporting entities shall notify users or otherwise put into a knowable state for users the notification matters by some method, such as displaying the notification matters on their site in a manner that users can easily recognize and understand or placing a link in a conspicuous location on their Web site to a page on the relevant ad delivery business's Web site that describes the notification matters.

(5) When a substantive change occurs to the notification matters, ad serving businesses must notify users or otherwise put into a knowable state for users about the change and the details of the change prior to the change taking effect by some method, such as displaying the change and the details of the change in a conspicuous location on their Web site in a manner that users can easily recognize and understand. This limitation shall not apply, however, in connection to changes that reduce the collection or usage of Web behavior data.

Article 5 *Assurance of opportunities for user participation*
Ad serving businesses shall provide users in a space that is easily accessed from conspicuous locations on their Web site with some means of easily selecting whether to allow the ad serving business to collect their Web behavior data and whether to allow the ad serving business to use their Web behavior data.

Article 6 *Assurance of collection by legitimate means*
Ad serving businesses shall collect Web behavior data through legitimate means only.

Article 7 *Assurance of proper safety controls*

(1) Ad serving businesses must erect and maintain proper safeguard measures in their management practices to protect Web behavior data.

(2) Web behavior data shall be retained only as long as necessary to fulfill a legitimate business need or as required by law.

(3) Ad serving businesses shall disclose that Web behavior data are not personally identifiable information in notifications to users concerning privacy.

(4) Ad serving businesses that provide Web behavior data to third parties shall implement the following measures to prevent disclosure, loss, or damage to Web behavior data and to otherwise safeguard the security of Web behavior data. The third parties that receive Web behavior data and subsequent purchasers that receive provisions from third parties shall be limited to those entities disclosed in notification matter (vi), the scope of data-receiving entities.
(i) Ad serving businesses shall not divulge or make known algorithms or other mechanisms for encrypting Web behavior data even when providing Web behavior data to third parties.
(ii) Ad serving businesses shall provide Web behavior data to third parties under the conditions that the third party shall not engage in any act that contravenes the Personal Information Protection Law and that the third party uses the Web behavior data only within the scope disclosed in notification matter (viii), the purpose of use.
(iii) Where a third party provides Web behavior data to another party, ad serving businesses shall oblige the third party to provide the Web behavior data under the conditions given in the previous item.

Article 8 *Education*
(1) Ad serving businesses shall participate in efforts to educate individuals and businesses about behavioral advertising.

(2) Ad serving businesses shall make all efforts to display the notification matters in order to provide users with factual information about behavioral advertising and make all efforts to provide users with the means to exercise their selection rights given in Article 5.

(3) Ad publishing entities shall cooperate, including using ad spaces on their own Web site, in efforts to guide users to pages on the JIAA Web site created to provide information on behavioral advertising and publicize behavioral advertising.

Article 9 *Assurance of frameworks to address complaints and inquiries*

Ad serving businesses shall endeavor to set up a contact point for questions and complaints about the handling of Web behavior data and strive to process claims quickly and appropriately.

Chapter 3: Other Provisions

Article 10 *Reporting*

(1) Ad serving business shall submit reports to JIAA on the state of their compliance with the Guideline as requested by JIAA.

(2) JIAA may issue a request for corrections to any ad serving business found to be in violation of the Guideline.

Article 11 *Revisions to the Guideline*

The Guideline shall be revised and updated as necessary in light of changes in the surrounding environment, including but not limited to changes in social circumstances, changes in the consciousness of citizens, and changes in technological development.