Kaneko, Keiko

Conference Paper

Toward strong enforcement against improper marketing of personal information. New mission of the unsolicited marketing communication restriction in the era when security breach is inevitable

14th Asia-Pacific Regional Conference of the International Telecommunications Society (ITS): "Mapping ICT into Transformation for the Next Information Society", Kyoto, Japan, 24th-27th June, 2017

Provided in Cooperation with:

International Telecommunications Society (ITS)

Suggested Citation: Kaneko, Keiko (2017) : Toward strong enforcement against improper marketing of personal information. New mission of the unsolicited marketing communication restriction in the era when security breach is inevitable, 14th Asia-Pacific Regional Conference of the International Telecommunications Society (ITS): "Mapping ICT into Transformation for the Next Information Society", Kyoto, Japan, 24th-27th June, 2017, International Telecommunications Society (ITS), Calgary

This Version is available at:
https://hdl.handle.net/10419/168498

Toward strong enforcement against improper marketing of personal information
- New mission of the unsolicited marketing communication restriction in the era when security breach is inevitable-

Keiko Kaneko
Institute of Information Security

【abstract】
Due to the development of technology and threats, personal information leakage is getting inevitable. In Japan, societal criticism and possible a large amount of economic loss occur to the entity having leaked personal information, but not so much against data broker purchasing the leaked information or entity buying it from them. To strengthen the restriction against the latter, the 2015 amendment of Act on the Protection of Personal Information (APIP) introduced the traceability and the on-site inspection authority by the Personal Information Protection Committee(PPC), but the authority can not conduct without clue that the personal information is in circulation. In the United States, there are monitoring services for important personal information which may lead economic damage or identity theft to the information subject, but in countries like Japan, where even basic information is accountable, monitoring for wider range of personal information is desired. Meanwhile, in the Do Not Call system introduced in 18 countries around the world, consumers can simply delete their information from the call list of the telemarketer only by registering their phone number with the National Registration. This is useful as a system to control consumers' personal information without imposing a burden of actively pursue specific entities using it by consumers. Here, I would like to propose a "Do not hold" system to delete personal information illegally acquired by enabling the authority to investigate it by which it gets possible to identify the entity having the information of the data subject.

【keyword】personal information, data broaker, Do not call, the unsolicited marketing communication

1. preamble

The law for personal information protection was born in the 1970s to show how to protect privacy and human rights under computerization progresses. And, to date, it has developed coping with the development of technology and changes in society and business by it. With this background, the biggest role of the law has been to show guidance.

For this purpose, steady execution is not necessary. At the announcement of guidelines and other proposals, a rough direction is shown, and a decent entity would think about a method which does not become a problem. However, by nature, the guideline follows the development of technology and the

emergence of services. When a pioneering case without guidelines arises, it may be taken up also in the mass media, and the discussions arise reviewing the new business with respect to the privacy. Following it, the authority has hearing and issues guidelines. Even before the guideline is made, especially European authorities may also restrict it under some reasons. In Japan, steady execution is not necessary on decent business operators, as they are so nervous for critics by the media, which even has chilling effect. Since large US companies stand out, it is unnecessary to perform steady detection, but rather how to enforce effectively against a company with the thought that fine is just a part of cost may be a challenge.

However, what many consumers are concerned and in trouble is not a such advanced case, but a fundamental and primitive concern for the protection of personal information; concern that their personal information may be sold without their knowledge and nuisance by unfamiliar soliciting calls. Economic damage has also occurred to individuals or credit card companies due to leaks of credit card numbers. Enforcement against such illegal or improper distribution requires information gathering and steady detection, and effective execution has not been done much. Rather, emphasis is placed on social criticisms against entity having leaked their information and claims for damages against them.

This problem is not unrelated to the development of technology. Technology and attack methods to intentionally steal target information are rapidly developed, and a great deal of personal information is stolen without being noticed. Even in insider crime, the criminal exploits the blind spot where countermeasures have not caught up with the development of technology. In this way, it can be said that it is impossible to completely prevent the leakage.

In many countries breach notification is introduced to prevent the secondary damage by enabling the data subject to protect themselves with the notice. However, when the data was stolen without notice, by no means the entity can make breach notification.

Therefore, it is important to detect the illegal distribution of the personal information. Considering of national crime and the existence of the dark web, it’s impossible to completely eliminate illegal circulation of personal information. However, if the enforcement is not done against illegal circulation of ordinary brokers, the personal information protection law would be the norm that honesty doesn't pay.

In this paper, I first explain the situation of the personal information protection norm in Japan, compare it with the United States about the detection capability, and propose to use unsolicited marketing communication restriction for the purpose to detect the circulation of leaked or stolen personal information.

2. Situation of personal information protection in Japan

2.1. Personal information protection norm in Japan

In 1990s, when the law evolved to

adapt to the rapid development of digital and internet technology and the network society, Japan took the stance to minimize the regulation and execution to promote free development of technology and business, and leave the norm to the voluntary regulation and hand of market except for crime. In personal protection field, Privacy Mark Certification System started with similar thought. In 1999, the incident of Uji City, which defined the direction of Japanese personal information protection norm, occurred. There, personal information of 220 thousand citizens was stolen by a part time worker of the outsourced company. The leaked data was from basic resident register, which includes name, address, gender, date of birth, relation to the family head, and moved-in-date. No financial or account number was included. It was scooped from the claims or rumors of many citizens who received direct mail or phone calls from various stores including Kimono stores trying to sell Kimono for coming-of-age ceremony. In the litigation brought by 3 citizens claiming breach of privacy, the court approved damage of 10 thousand yen.

Because of the public opinion at this news and reciprocity requirement of the European directive, APIP was enacted in 2003.

In Japan, the strongest enforcement of the personal information protection norm is reputation risk. Even if a business entity seriously takes information security measures, once an incident occurs, it loses trust of customers and society, has to conduct breach notification to the data subject sometimes with small amount of coupon to show their apology, to the government and to the public, and sometimes is involved in the litigation.

On the other hand, reputation risk does not work to the data broker or entity using the stolen or leaked data, and law enforcement is not done much. The mechanism to detect such distribution and use is weak compared to the United States.

APIP prepares the way to promote the dispute resolution by the parties, between the data subject and the entity, because it is quicker and efficient, but it is not easy for a consumer to negotiate with the broker or user of the information, who the consumer can not be certain whether they can put trust. Under APIP, national and local governments are obliged to take measures (efforts) necessary for processing complaints that have arisen between the entity and the data subject, and National Consumer Affairs Center of Japan and Consumer Affairs Center by local government are conducting the mediation and reference.

In 2014, the number of complaints received by these institutions was 6,769, of which 3,016 cases (44.6% of the total) are for "improper acquisitions"[1]. That would be the claim where the consumer wonders why the calling entity has his/her personal information though they did not provide it to them.

[1] Consumer Affairs Agency ”report on enforcement of Personal Information Protection Act for 2014” May, 2015

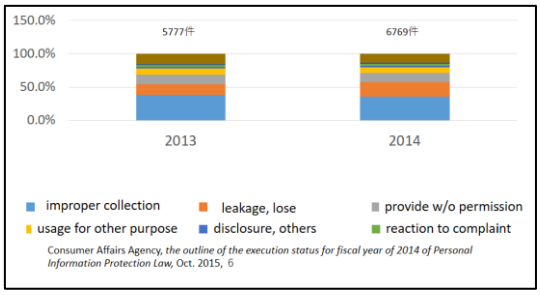

Fig. 1 claim reason

Consumer Affairs Agency "report on enforcement of Act on the Protection of Personal Information for 2014"

And the result of the processing of the claim is as follows. It's not certain that these claims connected to the enforcement.

processing results	claim	ratio
Advice (voluntary negotiation)	5,456	80.6%
Other providing of Information	913	13.5%
Mediation	138	2.0%
Introduction to other institutions	118	1.7%
No process required	101	1.5%
Inoperable	36	0.5%
Mediation failed	7	0.1%
total	6,769	100%

Table 1 result of process

APIP also prepares the legal enforcement. The competent minister (after May 30, 2017, PPC) exercises authority; request for report, advise, improvement recommendation, improvement order, and penalty if the improvement order is not be followed.

Although it is presumed that voluntary and informal reports based on the breach notification recommended in the guideline[2] were conducted, the number of official request for report under Article 32 of the Act has drastically declined around 2008 and the number of recommendations for improvement is small. (See Figure 1 - Number of exercising powers by the competent minister) All the eight recommendations issued by the year 2014 are to the entity having data breach, and six of them are to the entity voluntarily reported to the government. No detection is necessary for it, and this shows the enforcement action has not be conducted so much.

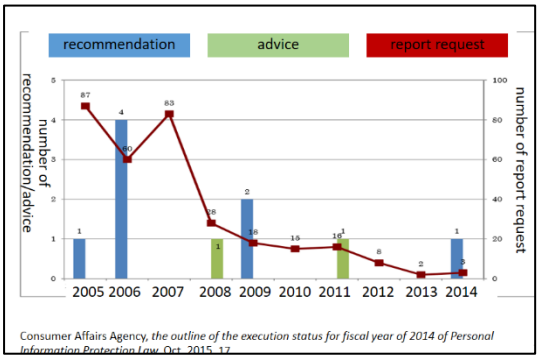

Fig.2 number of cases Competent Minister exercised its authority

2.2. Improper marketing of personal information in Japan and necessity to detect the circulation

As an improper distribution, what comes to mind immediately is data broker. APIP does not necessarily make data brokers illegal. It does not require the

[2] The guideline effective at this period was the guideline by Ministry of Economy, Trade and Industry (METI) on Act on the Protection of Personal Information, 2009. page 28

consent of data subject to acquire or provide the personal information. Regarding acquisition, Article 17 provide abstract requirement for proper acquisition, "Personal information should not be acquired by false or other improper means". Also, it is sufficient to publish or notice of the purpose of use for the personal individuals possessed. As for provision, according to Article 23 (2), it is possible to provide personal information to a third party if they prepare by opt-out procedure and publish it.

In March 2016, the Consumer Affairs Agency published "The Survey Report on the Provision of Personal Information by Data Brokers[3]". According to it, the data brokers acquire personal information from used paper collector, individual bringing in, and the fellow broker, and copy, process, and sell the data. Purchasers use it for promotion, and many of them are in the business for rich people, senior people, women, or new adults, or education services, and mail-order businesses. When acquiring, they do not confirm the acquisition route in particular, but some brokers gets "confirmation letter" that the data is of no problem from the seller.

Regarding the opt-out procedure, the brokers in the survey does not publish the information required by the law, so it does not meet the requirement of third-party provision by opt-out procedure. In other words, they were illegal.

If asked by the data subject, after confirming the identity, they delete his/her data from the database, and requests the seller broker to delete it.

However, it is becoming a hotbed of illegal distribution that trading without asking deeply to check the appropriateness at the time of acquisition. There are data brokers worse than those in the survey who deal with so called “kamo-list”, the list of people easy to be deceived, and complicit in criminal acts such as fraud, or nurture the consumer damage by inappropriate solicitation etc. It was pointed out as a social problem.

To react it, APIP was amended in 2015. It introduced traceability, and strengthens regulations on the provision to third parties by opt-out procedures.

The latter added "How to accept request to stop your data to be provide to a third party" to the notice publication matter, and oblige these information be notified to the PPC, which publishes it.

Regarding the traceability, the obligation to record the each provision/purchase of personal data to/from a third party to prevent the improper circulation and enable PPC to quickly grasp the acquisition route when problems such as data breach occurred. Concretely, especially at the time of acquisition, obligation to check the details of how the provider got the data was added.

In this way, the APIP prepares to deter the improper distribution and there will be some effect.

But you can’t find the broker or entity having your data by checking the web publication of PPC, and it is not practical to ask the entities on PPC’s web whether they

[3] http://www.caa.go.jp/policies/policy/consumer_system/other/ (last visited in Jan. 2017)

have your data. With this amendment, PPC has the authority of on-site inspection. We expect PPC to actively exercise this authority utilizing traceability to investigate. But it can't start investigation without clue. In other words, if you do not notice leakage or distribution, no investigation will be done.

3. System to detect the use or marketing of personal information

3.1. Monitoring service in US

Apart from leaks due to lost or stolen devices, it's often difficult to notice the breach by unauthorized access or internal crime, where the size of the leaked data tends to be rather large. Patterns in which such breach can be found are as follows;

(1) discovered by entity's monitoring and analyzing logs and abnormal signs are discovered

(2) discovered by being pointed out by external monitoring agencies such as JPCERT

(3) leaked data is posted on the web etc., and the fact spreads out by SNS etc.

(4) unauthorized use of leaked data has become a topic in SNS etc.

(5) leaked information is used, and the data subject makes inquiries to the business entity that he/she provides his/her information.

(6) leaked credit card number is used and credit card company notifies the entity

(7) at extortion, such as request to buy back the data.

Particularly with regard to (5), sometimes it's found because the customer controls or differentiates the information providing to each entity. Or at the increase the same type of inquiries from customers, the entity investigates the log etc and may find some sign of breach and sometimes who committed, but only by the entity keeping log properly. Also, in such cases, the criminal often delete the sign. Also when the possibility of breach is noticed, it is likely that time has passed since the breach occurred, so many businesses that have no logs left.

In the United States, there are identity theft monitoring services. Though it does not prevent leakage and identity theft of personal information, it is to find out that your information is used by someone at an early stage and stop spreading the damage. These services are for the data subject to purchase and pay. There are two kinds of monitoring, credit monitoring and identity theft monitoring.

The credit monitoring is to monitor the creation of loans and credit cards under their own name, mainly to avoid economic loss. The identity theft monitoring is to monitor that someone acts as you in the important process such as public process requiring the ID.

With these services, the discovery rate of unauthorized use of personal information is much higher in the United States than in Japan. In addition, the FTC operates the web site to report Identity Theft, a mechanism that consumers can easily report. Through accumulation of information collected in this manner, FTC or other authority can find the spot to investigate to enforce the law.

These monitoring systems monitor only important personal information because the use of account information and

identification information that are likely to lead substantial damage, such as the person himself or herself being economically damaged or suffering from social damage caused by identity theft. However, in Japan, more basic personal information is matters. In some case, the court approved the damage where the name, address, telephone number, email address, and Yahoo! ID was breached. This kind of information is traded by the broker and used for marketing. Is there a way to monitor the circulation or use of these information?

3.2. Proposal to utilize the unsolicited marketing communication restriction system

3.2.1. Outline of the unsolicited marketing communication restriction system[4]

The regulation to restrict the marketing of goods or services through visits, communication, etc., without consumers inviting, began with a viewpoint of consumer protection. There are regulation on visit, mail (paper direct mail), telephone (FAX, fixed phone, mobile phone) and e-mail. Especially regarding solicitations by telephone, it has already been introduced in 18 countries and is called the Do Not Call system. Telephone solicitation suddenly disturbs the peaceful privacy space/time of an individual's family, and it tends to impair consumers' proper self-determination's because of unexpectedness, anonymity, closed communication, compelling imperative, uncertainty, persistence of solicitation, convenience and cost effective for marketing entity[5].

This restriction began as a voluntary restriction of the Direct Marketing Association in the UK in 1996. In the United States National Registry for Do Not Call was introduced in 2003. There, the consumer who does not want to receive the telemarketing call register his/her phone number in the National Registry, and it is illegal to call the phone number for marketing purpose.

In many countries, like the United States, those who do not want solicitation take an opt-out method to register. In case of the United States, the FTC itself operates the Do Not Call system, but in many countries regulatory authorities outsource the operation to a telecommunications company or NPOs. In some countries it is outsourced to the association of telemarketing companies. This is due to the history of voluntary restrictions from increasing criticism of call solicitation before legal restriction took place.

In US, consumers need only register telephone numbers, but in some countries they have to also register the name and national id numbers to prevent spoofing

4 Regarding the law of unsolicited marketing communication restriction system in each country, Shinji Minai et al, *"know the unsolicited marketing communication restriction in the world", in Kokuminseikatsu*, June, 2015 – July 2016 http://www.kokusen.go.jp/wko/data/bn-kkisei.html (2017.2)

5 Masahiro Sato, et al, *"Handbook for Act on Specified Commercial Transactions"* Nihon Hyoronsya, 2014, 215

though the telemarketer can access only phone numbers. The telemarketers have an obligation to collate registration lists and their calling list once a month. Some countries impose this obligation indirectly by prohibiting making call to the numbers registered for more than one month. There are two types of method to make the registered number "available" to the telemarketer; "downloading the refusing list method" and "cleaning the call list method". In the former, the telemarketers can download the registration list and collate them with their call list. In the latter, the telemarketers upload/submit their call list to the agency and the agency delete or mark the refusing number and return it to the telemarketer. The latter is better because the additional phone number is not provided to the telemarketer. The country recently started the system tend to take the latter such as Australia, Singapore, Korea, Italy and France. In many countries, the telemarketer must be registered to the Do Not Call operating body and pay the fees for using the list, which is to cover the operating costs of the Do Not Call system.

In all countries, it is allowed to registered numbers if the person has given the explicit consent or has already business relationship. This takes balance between use and protection. Several countries also exclude the political parties and general newspapers.

In many countries prepare easy way for consumers to report the marketing phone call to the registered number to the authority etc. such as web site or ombudsman. In all countries, fines are set for violations, which is rather expensive.

3.2.2. The unsolicited marketing communication restriction system and personal information protection law

At the beginning, the law that provides the Do Not Call system was that on the telecommunication administrative law or consumer protection law. In the United States, first, in 1991, FCC, the telecommunication administration agent, based on the Telephone Consumer Protection Act, introduced entity specific Do Not Call. However, regarding the National Do not call System in 2003, the congress decided it as the mission of the FTC, which was responsible for consumer protection and was expanding its investigative authority to personal information protection as "deceptive transaction to consumers". Now, FTC seems to classify the Do Not Call in the same category as data protection. Do Not Call cases are reported in "the Privacy & Data Security Update (2016)[6]". In the "consumer information" site[7], it lists do not call, identity theft, online security, protecting kids online. This site has the link to web site report the identity theft, and Do Not Call site where consumers can register their number or report the claim.

In Europe, in 2002, unsolicited marketing communication restriction is

[6] https://www.ftc.gov/reports/privacy-data-security-update-2016 (last visited May 2017)

[7] https://www.consumer.ftc.gov/topics/privacy-identity-online-security(last visited May 2017)

obliged under "Directive on Personal Data Processing and Privacy Protection in the Telecommunications Field (2002/58 / EC)". The main purpose of this directive was telecommunication administration. It was made in response to the 1995 Data Protection Directive, and revisions are being processed in accordance with the General Data Protection Regulation.

In the UK, the Privacy and Electronic Communications Regulations 2003 was enacted in accordance with Data Protection Act 1998. The regulations are carried out by the Office of Communications but the enforcement is carried out by the Information Commissioners Office (ICO) in charge of Data Protection Act. Even in Italy the system itself is based on the Presidential Decree, but violators are sanctioned by the Data Protection Act.

The Do not call system has also spread to North America, South America and some Asia-Pacific countries. In Singapore, Do Not Call is based on one chapter of Personal Data Protection Act 2012 itself, and Personal Data Protection Commission operates Do not call.

Thus, the two systems are getting more closely related.

3.2.3. Proposal: utilizing the unsolicited marketing communication restriction system to detect the improper marketing of personal information

As mentioned in the previous chapter, in order to enforce unauthorized circulation of personal information, the clue of the circulation is necessary. Unauthorized use, such as telemarketing from entity to whom the consumer has not provide his/her information is more likely to be discovered than distribution itself.

With the “cleaning the call list method” Do Not Call System, it may be possible to identify the entity having many registered phone numbers, because the company submits the list, and this may be a good clue that the entity purchased the list. Even in the “downloading the refusing list method”, businesses with many complaints from consumers are suspected to have purchased the list, which may be the clue to lead the investigation of the improper distribution.

As mentioned earlier, the FTC has prepared web site for reporting identity theft and Do not call complaints from the same consumer site. Consumer claims are stored in a database and are shared with consumer related law enforcement agencies such as FTC, FCC and state prosecutors through the Consumer Sentinel database. If many claims are concentrated to an entity, that would be prioritized for investigation. Depending on size and content, suitable agency investigates the claim. Even as Do Not Call complaints rise a lot, it can be prosecuted as a case of general privacy case.

The Do not call execution cases reported in the annual report[8] of FTC are on fraudulent acts, so Do Not Call seems to be used as the clue to investigate complaints as the beginning. Since United States does not have comprehensive

8 see note 6

data protection legislation at federal level, there are big data brokers which is legal and has political power. This may be the background that the case started at Do Not Call claim clue is not on the improper circulation.

On the other hand, in the UK, in January 2017, though it is concerning e-mails, an order by ICO for penalty based on the Data Protection Act against a data broker was issued, for which ICO started investigation at the clue from the detection system for the unsolicited marketing communication restriction.

Mobile phone users can report the receipt of unsolicited marketing text messages to the GSMA's Spam Reporting Service by forwarding the message to 7726 (spelling out "SPAM"). Each law enforcement agency can access the database. ICO started the investigation at 174 complaints from 19th June to 21st September 2015 on email for pay day loan. As a result of investigation, it was found that the sender was The Data Supply Company (DSC), a data broker. It was found that 580,302 data were purchased and 21045 text messages were sent out. Although DSC claimed that it was acquired from multiple financial institutions and that they posted consent wording on Web sites. ICO reasoned that the general consent is not enough, and consent should be made recognizing the specific sender of the message based on the Electronic Communications Regulation 2003 in order to sell/purchase the data for the purpose of text e-mail, automated phones for marketing purposes. Further, it states that data controllers wanting to sell a marketing list for use in text, email or automated call campaigns must keep clear records showing when and how consent was obtained, by whom, and exactly what the individual was told (including copies of privacy notices), so that it can give proper assurances to buyers. ICO fined DSC under 55A of Data Protection Act1998.

In Japan, Do Not Call itself has not been introduced. Sine it has already been introduced in 18 countries, mainly developed countries, and it may be possible to be introduced in Japan.

If introduce, from the viewpoint of using also as a clue for effective enforcement of APIP, it should be conducted by an institute under PPC, and the Consumer Affairs Agency co-ordinates for enforcement, because Consumer Affairs Center by local government are conducting the part of enforcement of APIP, and main purpose of Do Not Call system is for consumer protection.

Since in Japan decent businesses have already shrunk by the reputations on personal information protection norm, from the perspective of balancing the use and protection of personal information, as like many countries, it should be the opt-out approach. In addition, in order to detect unauthorized use of personal information, "cleaning the call list method" is preferable like Singapore and South Korea. This is because if there is no contact from the business operator, consumers usually do not know which businesses have their own personal information, and in "cleaning the call list method", it is possible to find a business entity having his own information through the operator without imposing a

burden on the consumer.

In addition, although the information acquired by the written consent is not be deleted from the calling list, in order to realize this by "cleaning the call list method" the entity must have a separate database to add to the cleaned call list. This will be burdensome to the business operator, and an undelivered call list will remain. To solve that, the telemarketer can submit the call list with a mark to the phone number with consent.

It is meaningful to make the telemarketer not to have a registered phone number, but from the view point of enforcement of APIP, it's important to find the fact that the telemarketer has the registered telephone number. And it is important to improve the detecting ability by such as easy reporting system from consumers. As in the case of overseas, the it must be made illegal not to collate the call list, and with the reporting system the violation can be found. Of course, business operators should be given the opportunity to explain if they have the consent of telemarketing.

With the "cleaning the call list method", this may be used for the service the consumer can know the business entity having his/her information. Considering the monitoring service in the United States for a fee, this kind of service may be paid for with a small fee. There, you can know that the telemarketer asserts they have your information with your consent, and if it's not true, you can either report it to the authority or exercise your right based on Individual Participation Principle.

3.2.4. Develop to Do not hold

You can make the entity to delete your data from their calling list under the Do Not Call system, but it does not reach the other list. In Do not hold, when realizing it as an enforcement system of APIP, it is necessary to cover other information possessed and handled by a business other than the call list.

It is not realistic to let the business entity to submit all the list to Do Not Call system. However, with active enforcement at the clue that there are many complaints on the entity, PPC and the delegated institute can make them delete from other list. By the investigation, it is also possible to investigate the acquisition route of the list.

In some case, the telemarketer believed the list is purchased legally, but there may be problems upstream of that distribution. For such entity, voluntary reporting system should be available not to make the entity guilty and to encourage the information useful to find the improper circulation.

4. Conclusion

In this way, the consumer can delete his/her personal information without contacting the unknown entity only by registering, and the PCC can find businesses illegally marketing or acquiring personal data for effective enforcement.

In any case, it is important to keep effort to make the norm of personal information protection under which the protection and utilization balances without excessive burden on consumers and decent business entities, and the enforcement against the illegal data brokers lead the norm effective and fair.