A Comparative Legal Study on Data Breaches in Japan, the U.S., and the U.K.

Kaori Ishii, Taro Komukai

▶ **To cite this version:**

Kaori Ishii, Taro Komukai. A Comparative Legal Study on Data Breaches in Japan, the U.S., and the U.K.. 12th IFIP International Conference on Human Choice and Computers (HCC), Sep 2016, Salford, United Kingdom. pp.86-105, 10.1007/978-3-319-44805-3_8 . hal-01449452

HAL Id: hal-01449452
https://inria.hal.science/hal-01449452

Submitted on 30 Jan 2017

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution 4.0 International License

A Comparative Legal Study on Data Breaches in Japan, the U.S., and the U.K.

Kaori Ishii[1] and Taro Komukai[2]

[1] Faculty of Library, Information and Media Science, University of Tsukuba, Tsukuba, Japan
kaoriish@slis.tsukuba.ac.jp
[2] College of Risk Management, Nihon University, Tokyo, Japan
komukai.taro@nihon-u.ac.jp

Abstract. This paper focuses on the liability and duties of data controllers regarding data leaks and compares the relevant legal schemes of Japan, the U.S., and the U.K. There are three primary approaches to reducing or redressing damages caused by data leaks: 1) providing remedies for data leaks; 2) data security obligations; and 3) notification obligations in the event of a data breach. The aim of this article is to compare the measures on data breaches from the above viewpoints and highlight the relevant issues in order to reach an appropriate solution.

To address the issues related to data breaches, legal rules among countries should be common to all due to the worldwide circulation of personal data. Nonetheless, different features are recognizable through the analysis in each chapter.

Companies in Japan have thus far eagerly abided by data security obligations even if they are ineffective for data protection. Conducting PIAs is another option to prevent security incidents. If data breach notification rules are introduced, the subject matters to be publicized must be identified and followed by enforcement actions. Also, such rules should contribute to the avoidance of secondary harm.

In the U.S., while compensations for data leakage and security breach notification rules have apparently been effectively managed, it is needed to reduce serious harm arising from massive data breach. Obliging companies to maintain data traceability might serve this.

In the U.K., data breach notification rules imposed as part of the General Data Protection Regulation need to connect with other effective enforcements and contributions to avoiding secondary harm, so as not to become meaningless.

We must harmonize the above differences and make ongoing efforts to improve the effectiveness of rules.

Keywords: data breach notification· tort liability on data leaks· data security obligations· ID theft criminal uses of leaked data.

1. Introduction

This paper focuses on the liability and duties of data controllers regarding data leaks and compares the relevant legal schemes of Japan, the U.S., and the U.K. Because data leakage is currently a hot topic, issues such as determining how to prevent data leaks, reducing the associated damages at a time when massive amounts of data are processed and circulated all over the world, and protecting data from illegal or improper breaches is becoming increasingly important.

Outlined below are the three primary approaches to reducing or redressing damages caused by data leaks: 1) providing remedies for data leaks; 2) data security obligations; and 3) notification obligations in the event of a data breach.

1. Remedies for data leaks
   Data leaks can result in tort liability in Japan and the U.S., while in the U.K., the Data Protection Act 1998 (DPA) provides rules for compensation. These approaches are to redress the damage resulting from data leaks.
2. Data security obligations
   Data controllers are accountable for the security of the data they process. Legal frameworks for data protection generally include the data controller's obligation to keep personal data secure—an approach designed to prevent data leaks in advance.
3. Notification obligations in the event of a data breach
   Many states in the U.S. have rules for notifying victims of data breaches, and the EU's General Data Protection Regulation (GDPR) proposes similar rules. The use of notification rules for data breaches is an approach to prevent further damage and ensure the law enforcements.

The aim of this article is to compare the measures on data breaches from the above viewpoints and highlight the relevant issues in order to reach an appropriate solution. The reasons for comparing conditions in Japan, the U.S., and the U.K. are as follows.

First, it is indisputable that the concept of the right to privacy was created in the U.S. and that the E.U. is proud of its advanced data protection capabilities. A recent massive data leakage case has now prompted Japan to address the issue of data breaches. One measure the government has taken in this regard is the introduction of penal sanctions on illegal transactions involving personal databases, in an amendment to the Act on the Protection of Personal Information (APPI) in September 2015. While we referred to the criminal provision of the DPA during the amendment process, the effectiveness of the provision is still unclear. The data breach notification rule, which the U.S. first made into law, should also be considered. Japan has partially introduced this rule in the relevant act, although this might not be sufficient to address data breaches.

Second, in the U.S., massive data leakages have resulted in huge amounts of pecuniary damage. The Federal Trade Commission (FTC) has enforced penalties in those cases where security measures were violated. The U.S. has developed data breach notification rules as a legal obligation. The situation in the U.S. carries vital lessons for other countries.

Third, Europe has long been held up as the most advanced region when it comes to the field of data protection. The E.U. adopted the GDPR on the April 14th, 2016, which includes a data breach notification rule inspired by similar efforts in the U.S. Of the various European countries, the U.K. has exercised enforcement actions regarding violations of the DPA and stipulates criminal sanctions against unlawful obtaining or disclosing of personal data. We need to research the situation in the U.K. to evaluate the effectiveness of this provision.

Once a data breach occurs, the leaked data can instantly be circulated all over the world. Establishing common rules among countries is therefore the ideal; however, there are many differences in the surrounding circumstances of particular data breaches and the legal approaches employed to address them. We must conduct a comparative study, taking the above difficulties into account.

In Sections 2 to 4 we present our research on the facts on data breaches and the three legal measures of compensation, data security obligations, and data breach notification rules in the three countries. In Section 5, we analyze the common features of and differences among the said countries, and consider the effectiveness of possible data flow and legal schemes for addressing data breaches. In Section 6, we discuss the issues and available solutions, followed by the advantages and drawbacks of the said legal measures in order to establish a common rule for the future.

2. Legal remedies for data leakage in Japan

2.1 Tort law and data leakage

Claiming damages for data leakage in Japan is based on tort law from the Civil Code. Article 709 stipulates that “a person who has intentionally or negligently infringed any right of others, or legally protected interest of others, shall be liable to compensate any damages resulting in consequence.” When the injured party incurs mental or psychological harm, he/she can make a claim for compensation under Article 710. In addition, Article 715 rules that a person who employs others for a certain business shall be liable for damages inflicted on a third party by his/her employees with respect to the execution of that business. However, one challenge is that even if an injured party files suit against a perpetrator, the plaintiff is often awarded only a small amount in pecuniary damages.

The first court case involved the city of Uji. The city negligently leaked approximately 220,000 personal records from the resident registration system. In 2001, the

Kyoto District Court awarded damages of 10,000 yen for each plaintiff.[1] The Osaka High Court and the Supreme Court both dismissed Uji city's appeals.[2]

A case involving Waseda University was heard before the Supreme Court. The university invited Mr. Jiang Zemin, the former President of China, to lecture in front of a large audience. It provided a list of 1,400 student participants to the Tokyo Metropolitan Police Department for security purposes, but the participants did not consent to the provision of this information. Some students brought actions against the university. Although the Tokyo District Court and the Tokyo High Court dismissed the students' claims, the Supreme Court reversed the decision of the High Court and awarded consolation damages of 5,000 yen to each student.[3]

In the Yahoo! BB case, subscribers of Yahoo! BB brought an action against the Yahoo Japan Corporation and BB Technology Ltd. for leaking their data. The leakage was caused by a former employee and an acquaintance of his, who stole approximately 10 million records by illegally accessing the server. The Osaka District Court granted the plaintiffs' claim, which was upheld by the Osaka High Court.[4]

Another case concerns so-called "sensitive data." A large aesthetic service provider, Tokyo Beauty Center (TBC), negligently released customers' online questionnaire results, which led to the disclosure of their bust-waist-hip measurements and interest in epilation services, in addition to their names, ages, addresses, phone numbers, and e-mail addresses. The Tokyo District Court granted damages of 35,000 yen to several plaintiffs and 22,000 yen to one plaintiff.[5] The Tokyo High Court upheld the decision.[6]

2.2 Recent massive data leaks

Data leaks occur nearly every day. One noteworthy case involved the Benesse Corporation in 2014. A giant education company, Benesse, leaked approximately 29 million pieces of customer data, including dates of birth, the gender of children, and the names, addresses, and telephone numbers of parents and children [1]. One of the employees of the subcontractor allegedly copied the data list from the firm's database and sold it to three data brokers. The data brokers re-sold the data to other brokers; then, finally, competitors of Benesse bought the data. Benesse sent tradable coupons worth 500 yen to each victim, which did not sufficiently compensate the victims for their damages. As of December 4, 2015, over 10,000 people have sued Benesse, claiming damages of 55,000 yen each.

As a result of the Benesse case, the APPI was amended. When a business operator handling personal information (business operator) discloses personal information

[1] Kyoto Chiho Saibansho [Kyoto Dist. Ct.], Feb. 23, 2001, 265 Hanrei Chihoujichi 11 (Japan).

[2] Osaka Koto Saibansho [Osaka High. Ct.], Dec. 25, 2001, 265 Hanrei Chihoujichi 11 (Japan). Saiko Saibansho [Sup. Ct.], Jul. 11, 2002, 265 Hanrei Chihoujichi 11 (Japan).

[3] *See also* Ishini Oyogu Sakana Case [Sup. Ct.], Sep. 24, 2002, 207 Shumin 289 (Japan).

[4] Osaka Chiho Saibansho [Osaka Dist. Ct.], May 19, 2006, 1948 Hanji 122 (Japan), Osaka Koto Saibansho [Osaka High. Ct.], Jun. 21, 2007, Unpublished (Japan).

[5] Tokyo Chiho Saibansho [Tokyo Dist. Ct.], Feb. 8, 2007, 1964 Hanji 113 (Japan),

[6] Tokyo Koto Saibansho [Tokyo High. Ct.], Aug. 28, 2007, Unpublished (Japan).

from a database to a third party, both parties must keep a transaction record for traceability (Article 25 of the amended Act). Additionally, the third party must confirm the name of the disclosing business operator and the background of such operator's obtaining the data (Article 26 of the amended Act). As for criminal sanctions, if a business operator, an employee, or a former employee discloses or misappropriates personal information from a database concerning the business to others for the purpose of unlawfully benefitting themselves or third parties, he/she shall be punished by imprisonment with work for not more than one year or with a fine of not more than 500,000 yen (Article 83 of the amended Act) [2].

The Japanese data protection scheme has not been effective in reducing the trade in illegally obtained data. Thus, in recent reforms of the Japanese data protection scheme have introduced new rules for tracking data transactions and imposing criminal sanctions.

2.3 Legal obligations for security and data breach notifications

The APPI requires data security (Article 20). Business operators shall appropriately supervise employees and subcontractors (Articles 20 and 21). Failure to comply with the Act may result in administrative penalties. The competent minister may issue a recommendation or order. In recent reforms of the APPI, the Personal Information Protection Commission was established as an independent regulatory authority for data protection and in 2018 will gain the power to issue a recommendation or order.

Table 1 shows the number of regulatory actions by competent ministers in recent years.

Table 1. The number of regulatory actions by competent ministers from 2005–2014

Fiscal year	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014
Reports requiring (Article 32)	87	60	83	28	18	15	16	8	2	3
Advice (Article 33)	0	0	1	0	0	0	1	1	0	0
Recommendations (Article 34)	1	4	0	0	2	0	0	0	0	1

Source: Consumer Affairs Agency, Government of Japan, "Regulatory actions based on the Act on the Protection of Personal Information," 2005-2014, http://www.ppc.go.jp/personal/information/

If a business operator does not comply with an order, the person responsible for the breach of such order may be accused of a criminal offense (imprisonment for up to six months or a fine of not more than 300,000 Japanese yen). Also, the entity itself

could be held criminally liable. Thus far, however, there has been no case in which a person or entity was held criminally responsible.

In Japanese culture, companies confront severe condemnation regarding their leaks from the general public and mass media. They lose customer trust and it lowers the value of their brands, which could lead to a big financial loss. For instance, Softbank, the parent company of Yahoo Corporation and BB Technology Ltd., announced a net loss of 107 billion yen after the 2004 data leakage incident [3]. The Benesse Corporation lost 940,000 customers from its main service after its massive data leak [4]. The company also made public a sales decline of 1.07 million yen in May 2015 [5]. For fear of losing consumers' trust, companies are usually eager to maintain security measures, regardless of the existence of legal obligations.

There is no provision that requires data breach notifications in the APPI. The "Policies Concerning the Protection of Personal Information" (partially revised in April 2008) put forth by the Japanese Cabinet in 2004 "in accordance with" the APPI states "in the case of incidents such as data leakage, it is important for business operators handling personal information to disclose information about the incident as far as possible in order to prevent secondary damage or similar cases."

Many business operators disclose information regarding data leaks in accordance with the policy. The number of published data leaks in 2014 was 338, and approximately 66 percent were small cases involving no more than 500 records. Employees brought 67.5 percent of the cases, and most were caused by carelessness on the part of workers. Parties outside the company brought 26.6 percent of the cases, over 90 percent of which were committed intentionally.

Table 2. The number of published data leaks under the Policies Concerning the Protection of Personal Information

Fiscal year	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014
Number of cases	1,556	893	848	538	490	413	420	319	366	338

Source: Consumer Affairs Agency, Government of Japan, "Regulatory actions based on the Act on the Protection of Personal Information," 2014, http://www.ppc.go.jp/personal/information/

The Ministry of Economy, Trade, and Industry (METI) provides guidelines pertaining to the APPI that target the business sector [6]. The guidelines recommend contacting the person(s) potentially affected and reporting to the competent minister or the authorized personal information protection organizations. The METI has received 3,146 reports directly or through authorized organizations, most of which are minor cases caused by negligence. There are 15 cases of data leaks involving over 50,000 records; 11 of these cases were caused by malware or unlawful computer access [7].

One of the relevant acts of the APPI is the so-called National ID Act (formally named the Act on the Use of Numbers to Identify a Specific Individual in the Administrative Procedure), which covers handling personal data related to individual num-

bers. Individual numbers are allocated to each person and processed for administrative procedures in the field of Social Security, Tax and Disaster Response. Article 29-4 of the act obliges on relevant institutions (mainly governmental agencies) to report data breaches to Personal Information Protection Commission.

3. Legal remedies for data leakage in the United States

3.1 Litigation involving massive data leaks

In the United States, individuals who disclose personal data are subject to tort liability[7]. Notably, hacking often leads to massive data breaches. Table 3 below summarizes the cases involving massive data leaks caused by hacking in the last five years.

Table 3. Cases involving massive data leaks caused by hacking from 2011-2015[8]

Date of Breach	Name	Entity	Data that could have been compromised	Amount of data
April 27, 2011	Sony PlayStation Network (PSN), Sony Online Entertainment (SOE)	Businesses - Retail/ Merchant	Names, addresses, gender, email addresses, dates of birth, login names and associated passwords, phone numbers, online IDs, users' purchase history, billing addresses, passwords security questions, user credit card accounts, and bank accounts	101.6 million (12 million unencrypted credit card numbers)
October 4, 2013	Adobe, PR Newswire, National White-Collar Crime Center	Businesses - Retail/ Merchant	Customer IDs, encrypted passwords, names, encrypted credit or debit card numbers, expiration dates, and other information related to customer orders	2.9 million (38 million user emails and passwords exposed)
December 13, 2013	Target	Businesses - Retail/ Merchant	Customer names, credit or debit card numbers, card expiration dates, and card security codes	40 million (reportedly up to 110 million)
May 21, 2014	eBay	Businesses - Other	Email addresses, encrypted passwords, birth dates, mailing addresses (no financial data or	145 million

[7] Restatement (Second) of Torts § 652D; W. Page Keeton, Dan B Dobbs, Robert E. Keeton., David G. Owen: Prosser & Keeton on Torts 856-63 (5th 8 Supp.).

[8] The source of the chart is primarily the Chronology of Data Breaches Security Breaches 2005 – Present, from the Privacy Rights Clearinghouse, https://www.privacyrights.org/data-breach.

			PayPal databases were compromised)	
August 28, 2014	JP Morgan Chase	Businesses - Financial and Insurance Services	Names, addresses, phone numbers, and email addresses (no financial or bank account information was accessed)	76 million
September 2, 2014	The Home Depot	Businesses - Retail/ Merchant	Information on credit and debit cards, e-mail addresses	56 million
February 5, 2015	Anthem	Businesses - Financial and Insurance Services	Names, birth dates, medical IDs, Social Security Numbers, street addresses, e-mail addresses, employment and income information	80 million
June 4, 2015	OPM (The Office of Personnel Management)	Government	Employee job assignments, performance and training information, SSNs, fingerprints	21.5 million

Class actions have been brought against the above companies, and many cases have been resolved by consent judgments. In the Target case, the United States District Court for the District of Minnesota granted the plaintiffs' motion for approval of settlement but payments for claims can only be made after any appeals are resolved and after claims are finalized in 20159. In the Adobe case, the District Court Judge granted the plaintiffs' motion for approval of attorney fees in 201510. The company had already paid an undisclosed amount to settle customer claims [8]. Home Depot was also hit with a class action lawsuit in September 5, 2014 [9].

Though such companies are liable for invasions of privacy, plaintiffs face many challenges to be authorized that they have standing to be considered their merit in the actions. In the e-Bay class action, the District Court judge dismissed the plaintiffs' claim for lack of standing[11]. The judge held that the plaintiffs had failed to allege a cognizable injury-in-fact, and therefore lacked Article III standing to pursue the case in Federal Court. This case raised the issue of whether an increased risk of future identity theft or identity fraud posed by a data security breach confers Article III standing on individuals whose information has been compromised by a data breach but has not yet been misused[12].

[9] In re Target Corporation Customer Data Security Breach Litigation, MDL No.14-2522 (PAM/JJK) (D. Minn. 2015), http://www.mnd.uscourts.gov/MDL-Target/Orders/2015/2015-1117-14MDL2522-M&O.pdf.

[10] Adobe Systems Inc. Privacy Litigation, No. 5:13-cv-05226-LHK (N.D. CA. 2015).

[11] Collin Green v. eBay Inc., No. 2:14-cv-01688 (E.D. LA. 2015).

[12] Clapper v. Amnesty International USA, 133 S. Ct. 1138 (2013).

Neiman Marcus uncovered 1.1 million pieces of disclosed customer data, which led to a class action. The U.S. Court of Appeals for the Seventh Circuit held that data breach victims satisfied the Article III standing requirements and plaintiffs could make a claim in court against companies that failed to protect their personal data13.

3.2 The FTC's role in maintaining security

While many cases have been brought against companies, the Federal Trade Commission (FTC) has also played an important role in data breach cases. Article 5(a) of the FTC Act (15 U.S.C. § 45(a)) stipulates that "unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful." The FTC has the authority to investigate and initiate an enforcement action against a company in violation of the FTC Act, and recently has actively exercised enforcement actions against data breach cases[14].

Under Section 5(b) of the FTC Act (15 U.S.C. § 45(b)), the FTC may challenge "unfair or deceptive acts or practices" (or violations of other consumer protection statutes) through maintenance of an administrative adjudication. When there is **"**reason to believe" that a violation has occurred, the FTC may issue a complaint setting forth its allegations. If the respondent elects to settle the case, it may sign a consent agreement (without admitting liability), consent to the entry of a final order, and waive all rights to judicial review. If the FTC accepts such a proposed consent agreement, it places the order on the record for thirty days of public comment (or for such other period as the FTC may specify) before determining whether to issue a final order [10].

However, when it comes to data security, the authority for initiating an enforcement action becomes an issue under the terms of Article 5 of the FTC Act. In the case of Wyndham Worldwide Corp., the U.S. Court of Appeals for the Third Circuit affirmed the FTC's authority to bring actions in data security cases[15]. There are other cases where the FTC has approved final orders setting charges against companies lacking security[16]. However, the FTC bears the burden of proving that the allegedly unreasonable conduct caused or is likely to cause substantial injury to consumers. If the FTC fails to meet this burden, the complaint is dismissed [11].

In addition, the FTC values the importance of Privacy Impact Assessments (PIAs) and Privacy by Design (PbD). PIAs involve an analysis of how personally identifiable information is collected, used, shared, and maintained [12]. One of the advantages of a PIA is that it allows entities to discover security risks in the lifecycle of personal data, which can support data security management. PbD is a framework that was de-

[13] Helary Remijas v. Neiman Marcus Group LLC, No. 14-3122 (7th Cir. Dec. 20, 2015).

[14] Wyndham case in September 2015, cases of GMR Transcription Services, Fandango and Credit Karma in August 2014, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises.

[15] FTC v. Wyndham Worldwide Corporation, et al., No. 14-35414, (3rd Cir. Aug. 24, 2015).

[16] Final order cases on Cbr Systems, Inc. in 2013, HTC America in 2013, TRENDnet in 2014, Fandango, LLC and Credit Karma in 2014, and GMR Transcription Services, Inc. in 2014 under the tab News and Events on the FTC website, https://www.ftc.gov/news-events.

veloped by the former Information and Privacy Commissioner of Ontario in Canada, Dr. Ann Cavoukian. According to the definition, PbD advances the view that the future of privacy cannot be assured solely by complying with legislation and regulatory frameworks; rather, privacy assurance must become an organization's default mode of operation. PbD has seven basic principles: 1. proactive not reactive; 2. preventative not remedial; 3. privacy as the default setting (privacy embedded into design); 4. full functionality (positive-sum, not zero-sum); 5. end-to-end security (full lifecycle protection); 6. visibility and transparency (keep it open); and 7. respect for user privacy (keep it user-centric), which have been widely accepted in many countries [13]. The FTC strongly supported PbD in its Privacy Report of 2012 [14]. PIAs contain the essential aspects of PbD, playing an important role in satisfying the above principles [15].

3.3 Security breach notifications

There are more security breach issues in the U.S. than any other country in the world. Most states in the U.S. have legislation setting forth obligations for data breach notifications, but the specific rules vary from state to state. The U.S. also has Federal laws governing data breach notifications such as the Health Insurance Portability and Accountability Act (HIPAA) (42 U.S.A. § 17932), the Gramm-Leach-Bliley Act (GLB Act) (15 U.S.C. § 6801), and so on.

The first state to pass legislation requiring data breach notifications was California. The California Security Breach Notification Act requires a business or state agency to notify any California resident whose unencrypted personal information, as defined in the act, was acquired, or is reasonably believed to have been acquired, by an unauthorized person (California Civil Code s. 1798.29(a) and California Civ. Code s. 1798.82(a)). Any person or business that is required to issue a security breach notification to more than 500 California residents as a result of a single breach of a security system shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General (California Civil Code s. 1798.29(e) and California Civ. Code s. 1798.82(f)). ChoicePoint's data breach, disclosing more than 163,000 pieces of consumer data, is a well-known case to which the California Data Breach Act was applied. The case is said to have motivated other states to enact their own data breach notification laws because the company did not send notices to people who were affected in other states. The FTC eventually ordered the company to pay $10 million in civil penalties and $5 million for consumer redress purposes [16].

According to the California Data Breach Report of 2014 [17], reports of 167 data breaches affecting more than 500 California residents were submitted. The number of reported data breaches increased by 28 percent and the number of records affected increased by over 600 percent from the previous year. The latter increase was primarily due to two massive retailer breaches, Target and LivingSocial, which together involve over 15 million records of California residents. As for the type of breach, malware and hacking comprised the majority (53 percent) of all breaches reported. Nearly

half of the data breaches reported in 2013 involved Social Security numbers (56 percent), followed by payment card data (38 percent).

The report suggests that recent technological advances offer means to devalue payment card data, making it an unattractive target for hackers and thieves, and emphasizes the importance of improving retailer responses to breaches of payment card data. In California, as well as in most other states in the U.S., a data breach is discussed in the context of a criminal offense for using or targeting the compromised data, such as ID theft or fraud [18].

4. Legal remedies for data leakage in the United Kingdom

4.1 Data Protection Act 1998

4.1.1 Legal foundation

Article 13 of the DPA provides data subjects with the right to receive compensation for any contravention by a data controller. It seems to be less common to bring class actions in the U.K. and other European countries. However, in the Vidal Hall v. Google case, the U.K. Court of Appeal raised two issues. The claimants insisted that Google had collected their data using cookies without their consent. The first issue was whether the cause of action for misuse of private information is a tort; the second was the meaning of damage in section 13 of the DPA, particularly whether there can be a claim for compensation without pecuniary loss17. On March 27, 2015, the court ruled in the claimants' favor on both issues.

In addition to Article 13, the Information Commissioner has used other sections of the DPA against data controllers in many security breach incidents. Schedule 1 of the DPA prescribes seven data protection principles that data controllers must follow.

The first principle of the DPA in the U.K. is that "personal data shall be processed fairly and lawfully" and "whether personal data are processed fairly, regard is to be had to the method by which they are obtained, including in particular whether any person from whom they are obtained is deceived or misled as to the purpose or purposes for which they are to be processed" (Schedule 1, Part II, 1(1) of the DPA). The seventh principle requires that appropriate technical and organizational measures be taken against unauthorized or unlawful processing of personal data and against the accidental loss of, destruction of, or damage to personal data.

Concerning enforcement, Article 55A of the DPA authorizes the imposition of monetary penalties by the Commissioner. Additionally, Section 4(4) states that the data controller must comply with the data protection principles in relation to all personal data with respect to which he or she is the data controller.

Under the above conditions, the Commissioner may serve a monetary penalty notice on a data controller, requiring the data controller to pay a penalty of an amount determined by the Commissioner and specified in the notice, not exceeding £500,000 (Data Protection (Monetary Penalties) (Maximum Penalty and Notices) Regulations 2010, S.I. 2010, No. 31).

[17] Vidal Hall v. Google, [2015] EWCA Civ. 311.

In addition to the provisions referenced above, the DPA has a unique article that prohibits unlawful obtaining etc., of personal data. Pursuant to Section 1 of Article 55, a person must not knowingly or recklessly, without the consent of the data controller, obtain or disclose personal data or information contained in the personal data or permit the disclosure to a third party of any information contained in the personal data. Any violation of this provision is subject to criminal sanctions.

4.1.2 Recent data security trends and major incidents

The Information Commissioner Office (ICO), the office for the independent supervisory authority for the DPA, announced recent data breach trends. Based on the ICO's information, the graphs below show trends regarding incidents under the ICO consideration in relation to data security from April to June of 2015. Information regarding security incidents comes from a variety of sources, including self-reports from data controllers, media reports, whistleblowers, and reports from data subjects. The ICO reports that the health sector continues to account for most data security incidents. This was due to the combination of the National Health Service (NHS) making it mandatory to report incidents, the size of the health sector, and the sensitive nature of the data processed [19].

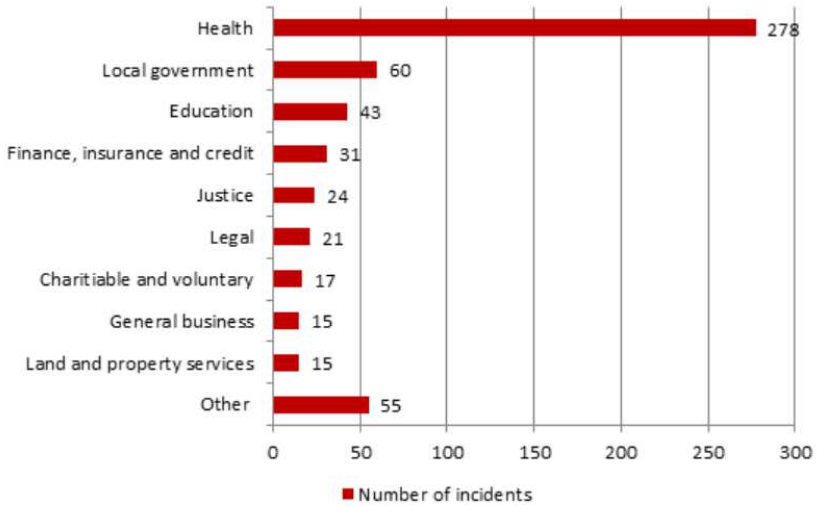

Fig. 1. Data security incident by sector

Source: ICO, *Data security incident trends*, https://ico.org.uk/action-weve-taken/data-security-incident-trends/

The table below summarizes the main data leakage cases that occurred in the U.K. between 2007 and 2015. Though the scale of the leakage is not as large as that of the U.S., the Commissioner imposed penalties on the perpetrators in some cases.

Table 4. Primary data leak cases, 2007–2015[18][20]

Date	Name	Entity	Data that could have been compromised	Cause	Amount of data
2007	HM Revenue & Customs	Government	Child benefit records	Loss of two CDs	25 million
March 2008	Brighton and Sussex University Hospitals NHS Trust	NHS Trust	Patient data	Loss of hard drives	79,000
December 2008	T-Mobile	Telecommunication Company	Customer records	Sales staff sold the data to data brokers	Millions of records
2011	Sony Computer Entertainment Europe Limited	Entertainment company	Names, addresses, email addresses, dates of birth and account passwords, customer payment card details	Hacking	Up to 3 million Britons[21]
December 24, 2012	Think W3 Limited	Online holiday firm	Credit and debit card records	Hacking (SQL injection attack)	1,163,996
2014	Mumsnet	Parenting Network	User accounts	Hacking	1.5 million
2014	Staffordshire University	University	Data on students and applicants	A computer stolen from a car	125,000
2014	Morrison's Supermarket	Retailor	Workforce database	Insider attack	100,000
October 22, 2015	Talk Talk	Telecommunication provider	Bank account numbers and sort codes, credit and debit card numbers	Hacking	156,959 (as of October 30, 2015)
Jan. 2015	Moonpig	Online retailer	Customer registration details	Hacking	3 million

4.2 Enforcement actions

Regarding the cases discussed in Section 4.1.2, the Commissioner imposed pecuniary sanctions on some companies. Fines were imposed on Think W3 (£150,000),

[18] This chart was made with information from the case list of the ICO, `https://ico.org.uk/action-weve-taken/enforcement/`.

Sony Computer Entertainment (£250,000), and Brighton and Sussex University Hospitals and the NHS Trust (£325,000). Two employees of T-Mobile, penalized under Article 55 of the DPA, were issued confiscation orders and were ordered by the court to pay £73,400 in fines in June 2011. In addition to those cases, a number of entities have been ordered to improve their data protection practices or to pay penalties.

PbD and PIAs are also valued by the ICO. The ICO has made the PbD webpage public [22], and the foundational principles of PbD are relevant to U.K. data controllers, as can be seen in the document entitled "Conducting Privacy Impact Assessments Code of Practice" [23] . PIAs are definitely important to ensure compliance with the seventh data principle.

4.3 Data breach notifications

Though the current laws and their enforcement results have been summarized above, the U.K. DPA will be dramatically altered by the EU GDPR which was finalized on the April 14th, 2016 [24]. PbD, PIAs, and data breach notifications is introduced in the GDPR. We should keep an eye on the changes that occur with the implementation of the GDPR.

The ICO enforces not only the DPA but also the Privacy and Electronic Communications Regulations of 2003 (an EC Directive). Service providers (e.g., telecom providers or Internet service providers) are required to notify the ICO if a "personal data breach" occurs. They must report to the ICO within 24 hours of becoming aware of the essential facts of the breach. They must also keep a log and notify customers if the breach is likely to adversely affect customers' privacy [25]. The ICO uses significant human resources to investigate inappropriate data transactions. Additionally, an expert at the ICO says that the introduction of a rule for data breach notifications in all sectors would make data flow clearer and would provide greater opportunities for enforcement.[19]

There is one more provision to ensure the transparency of data circulation in DPA. The first principle of the DPA in the U.K. is that "personal data shall be processed fairly and lawfully" and "whether personal data are processed fairly, regard is to be had to the method by which they are obtained, including in particular whether any person from whom they are obtained is deceived or misled as to the purpose or purposes for which they are to be processed" (Schedule 1, Part II, 1(1) of the DPA).

5. Consideration

Data leaks can cause two types of concerning issues. One is the privacy risk caused by the wide circulation of personal data and the other is the risk of economic damage. As mentioned in the introduction, there are three approaches for reducing the two types of risk; 1) providing remedies for data leaks; 2) data security obligations; and 3) notification obligations in the event of a data breach.

[19] According to the interview with the ICO in September 2015.

Table 5 shows the outlines of the regulatory schemes concerning these approaches in Japan, the U.S., and the U.K.

Table 5. Outlines of the regulatory schemes in Japan, the U.S., and the U.K.

Approach	Japan	U.S.	U.K.
1. compensation for data leaks	Tort liability: Articles 709, 710, and 715 of the Civil Code.	Tort liability: Common Law.	Right to receive compensation: Article 13 of DPA.
2. data security obligation	Obligation of business operator: Article 20 of APPI.	Prohibition of unfair or deceptive acts or practices: Article 5 of the FTC Act.	Appropriate technical and Organizational measures: 7th Principle.
3. Data breach notification	Recommendation for data breach disclosure: Policies by Cabinet.	Obligation to notify Notification to Attorney General and disclosure: Californian Act.	Notification to Supervisory Authority and Communication to Data Subjects: EU Data Protection Regulation.

The common feature of the three countries is that they all have basic legal or quasi-legal measures for compensation, data security obligations, and data breach notifications. However, the surroundings of data breaches, approaches toward harm arising from leakages, and issues among each country are different.

First, the compensation for data leaks is to provide remedy for damages caused by an actual data leak. While privacy infringement by wide circulation could be the reason for damages as well as economic harm, economic damages seem to easily go higher in terms of the amount of compensation than the damages arising from wide circulation of personal data itself.

In Japan, most data leaks are made by employees or subcontractors who disclose a small number of records. Business operators have had to pay compensation in relatively insignificant amounts thus far, even if they were ordered to pay damages to victims. Although compensation is higher when sensitive data is disclosed, an entity's obligatory compensation is still low. Therefore, tort liability for compensatory damages seems to be ineffective for compensating privacy victims. Nevertheless, as the number of plaintiffs in the Benesse case is growing, the monetary damages that are awarded might have some impact on the company, depending on the end results of all of the lawsuits.

Secondary harm such as identity theft and fraud have been outside the scope of consideration by courts because of differences in the causes of action. If such harm actually occurs, business entities are forced to face additional litigation.

In the U.S., hacking and malware issues are common causes of data leaks and economic damages are crucial in this issue. There are many class actions seeking compensation for data leaks, and the compensatory amounts are generally high. While

many cases have been solved by consent agreements, proving the standing of plaintiffs is still the issue.

In the U.K., there are not as many leaks as in the U.S., and few cases seem to lead to the economic damages that result from fraudulently using credit card information. Although class actions against data leaks seem to be rare, there are cases in which the interpretations of Article 13 of the DPA were disputed. Rather than claiming compensation by individuals, such cases have been dealt with enforcements by the ICO.

Second, the data security obligation imposes an obligation on data controllers and is intended to reduce the risk of both wide circulations of personal data and economic damage. In Japan, for fear of losing consumers' trust, companies tend to eagerly maintain security measures, regardless of the existence of legal obligations. While it might be sufficient to protect personal data in our culture, the APPI's data security obligation seems to be insufficient, and the introduction of PIA would be another option to ensure the sufficient level of security. In this case, we need to be careful of a drawback of PIA that might become a dead letter due to focusing on procedures. As for the new criminal sanction against illegal provisions of personal database, we need to keep an eye on their effectiveness in the U.K.

In the U.S., the FTC exercised enforcement actions against perpetrators based on "unfair acts or practices" provided by Article 5 of the FTC Act in the case of a data breach. The FTC's role in this regard has been effective, except for the issue of proving that the allegedly unreasonable conduct caused or is likely to cause substantial injury to consumers. The FTC also values the importance of PIA and PbD as proactive measures.

In the U.K., the ICO has exercised enforcement actions against violations of the seventh data protection principle. Although there have been no massive data leakages on the scale of those in the U.S., the ICO has compiled a list of enforcement cases. The ICO also views PIAs and PbD as important. In addition, the DPA stipulates criminal sanctions against the unlawful obtaining of personal data. Along with the sanctions, confiscation orders seem to be effective in reducing illegal data transactions. Currently, making use of breached data for a criminal offense in Japan and the U.K. does not seem to be as pressing as in the U.S.

Third, data breach notifications were originally introduced in almost all the states and sector-based federal statutes in the U.S., where they were essential to reduce the damages resulting from the criminal use of leaked data. Apparently, they have proven effective in requiring security breach notifications from entities as soon as possible in order to effectively respond to the unlawful use of breached data.

In Japan, the APPI does not provide the obligation to notify victims of data breaches. The amendment of the National ID Act has partially introduced the rule, although the legal system might be insufficient to implement it. However, companies tend to follow the breach notification rule even if it is just a recommendation by the Cabinet. As a result, a lot of reports have been submitted to competent ministers, including small cases. Given our tendency to keep security in a diligent manner, legal obligations might be burdensome for some entities.

In the U.K., the rule was introduced as a sector-based rule in the Privacy and Electronic Communications Regulations of 2003. As the GDPR is formally adopted, the scope of the rule will be expanded generally. The ICO views this positively, as it is expected that the introduction of a general data breach notification rule in the U.K. will improve the transparency of data circulation.

However, it is questionable that data breach notifications will also be effective in improving the transparency of data circulation, because notification will never reduce the data circulation by itself; it only alerts victims to the situation. In fact, the practice of data breach notification in Japan seems to lose substance in this regard.

It will be necessary to review whether the data breach notification rule is not only effective for addressing the criminal use of breached data, but also increases the transparency of data circulation and reduces inadequate data flows.

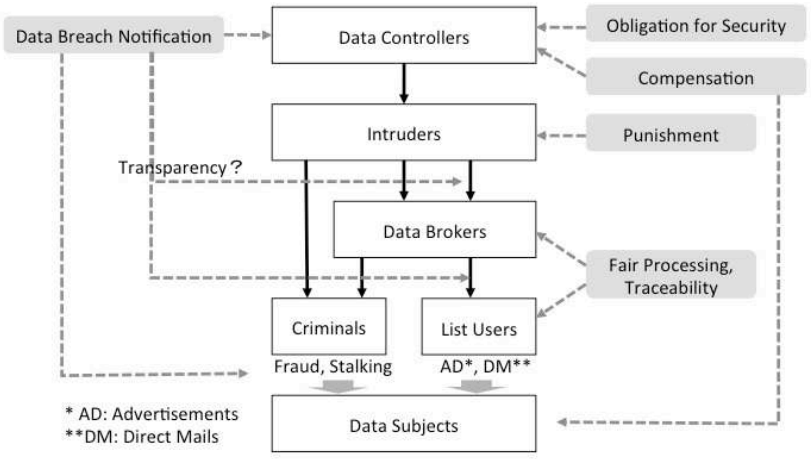

Fig. 2. Possible data flow and legal schemes for addressing data breaches

According to the above analysis, Figure 2 shows the possible data flow and legal schemes for addressing data breaches. The compensation for data leaks is to make data controllers pay data subjects for damage due to an actual data leak. While harm caused by the wide circulation of personal data could be compensated, as well as economic damages, the latter seems to easily lead to a higher amount of compensation than the damage done by the wide circulation of personal data. The data security obligation is designed to make data controllers keep personal data secure. The obligation is expected to reduce the risk of both wide circulations of personal data and economic damage. Data breach notifications, intended to make data controllers report and disclose data leaks, were originally introduced in the U.S., where it is essential to

reduce the damage resulting from the criminal use of leaked data. Although it is clearly effective in preventing the unlawful use of breached data, it is questionable that data breach notification is effective in improving the transparency of data circulation, because notifications will never reduce data circulation by itself—it only alerts others of the data circulation.

6. Conclusion

To address the issues related to data breaches, legal rules among countries should be common to all due to the worldwide circulation of personal data. Nonetheless, different features are recognizable through the analysis presented in the preceding chapter. According to this analysis, the following statements are the issues and measures that should be addressed and taken in each country.

Companies in Japan have thus far eagerly abided by data security obligations, although these seem to be not necessarily effective for data protection. There is another option, in which entities handling personal data conduct PIAs to prevent security incidents. In that case, it would be necessary to avoid bureaucratic procedures, and such action would entail the risk of data breach notification rules being a mere façade. If such notification rules are introduced, the subject matters to be publicized must be identified and followed by enforcement actions. Also, such rules should contribute to the avoidance of secondary harm. Newly introduced obligations on data traceability should be managed in a manner that harmonizes with effective enforcements.

In the U.S., compensations for data leakage and security breach notification rules have apparently been effectively managed. This comes from a background in which data breaches and the secondary harm arising there from are extremely serious compared to similar events in the other two countries. To reduce this threat, there is an option to oblige companies to maintain data traceability.

In the U.K., data breach notification rules imposed as part of the GDPR need to connect with other effective enforcements and contributions to avoiding secondary harm, so as not to become meaningless. The purpose of notification should be clear, which might avert wide circulation of personal data or the risk of economic damage.

We must harmonize the above differences and make ongoing efforts to improve the effectiveness of rules.

This work was supported by JSPS KAKENHI (C) Grant Number 15K03237.

References

1. Nikkei Asian Review.: Customer data leak deals blow to Benesse (in Japanese), Jul. 10, 2014(2014).
2. Japan Times.: 1.25 Million Affected by Japan Pension Service Hack (in Japanese), http://www.japantimes.co.jp/news/2015/06/01/national/crime-legal/japan-pension-system-hacked-1-25-million-cases-personal-data-leaked/#.VmBcY79RJ2I.
3. IT Media News.: Softbank losses 107 billion yen in the Current Term affected by the Influence of Data Leakage (in Japanese),

http://www.itmedia.co.jp/news/articles/0405/10/news071.html.
4. Nikkei Business.: Competitors take advantage of the leakage of Benesse Corporation (in Japanese), http://business.nikkeibp.co.jp/atcl/report/15/110879/080300059/?P=3.
5. IT Media Business.: Benesse Corporation declined its sales profit of 1.07 million yen (in Japanese), http://bizmakoto.jp/makoto/articles/1505/01/news115.html.
6. METI.: Guidelines Targeting Economic and Industrial Sectors Pertaining to the Act on the Protection of Personal Information (in Japanese), http://www.meti.go.jp/policy/it_policy/privacy/0910english.pdf/.
7. METI.: Outline and Enforcement of the METI Guidelines," December 2014 (in Japanese), https://www.ipa.go.jp/files/000041265.pdf/.
8. Darren Pauli.: Adobe pays US $1.2M plus settlements to end 2013 breach class action, http://www.theregister.co.uk/2015/08/17/adobe_settles_claims_for_data_breach/.
9. Jeffery Roman.: Home Depot already faces breach lawsuit, data breach today, http://www.databreachtoday.com/home-depot-already-faces-breach-lawsuit-a-7282.
10. FTC.: A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority, https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority.
11. FTC.: Administrative Law Judge Dismisses FTC Data Security Complaint Against Medical Testing Laboratory LabMD, Inc. (Nov. 19, 2015), https://www.ftc.gov/news-events/press-releases/2015/11/administrative-law-judge-dismisses-ftc-data-security-complaint.
12. FTC.: Privacy Impact Assessments, https://www.ftc.gov/site-information/privacy-policy/privacy-impact-assessments.
13. Information and Privacy Commissioner of Ontario.: Privacy by Design, https://www.privacybydesign.ca/index.php/about-pbd/.
14. FTC.: Protecting Consumer Privacy in an Era of Rapid Change, Recommendations for Businesses and Policymakers (Mar. 26, 2012), http://ftc.gov/os/2012/03/120326privacyreport.pdf.
15. Pat Jeselon.: A Foundational Framework for a PbD – PIA, https://www.privacybydesign.ca/content/uploads/2011/11/PbD-PIA-Foundational-Framework.pdf.
16. FTC.: ChoicePoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress (Jan. 26, 2006), https://www.ftc.gov/news-events/press-releases/2006/01/choicepoint-settles-data-security-breach-charges-pay-10-million.
17. Kamala D. Harris.: California Data Breach Report 2014, https://oag.ca.gov/ecrime/databreach/reporting/.
18. Sasha Romanosky., Rahul Telang., and Alessandro Acquisti.: Do Data Breach Disclosure Laws Reduce Identity Theft?, Journal of Policy Analysis and Management, Vol. 30, No. 2, pp. 256-286, 2011.

19. ICO.: Data security incident trends, https://ico.org.uk/action-weve-taken/data-security-incident-trends/.
20. John E. Dunn.: The UK's 11 most infamous data breaches 2015, http://www.techworld.com/security/uks-11-most-infamous-data-breaches-2015-3604586/3/.
21. ICO.: Data Protection Act Monetary Penalty Notice (Jul. 21, 2014), https://ico.org.uk/action-weve-taken/enforcement/think-w3-limited/.
22. ICO.: Privacy by design, https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/.
23. ICO.: Conducting privacy impact assessments code of practice (Feb. 2014), https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf.
24. European Commission.: Protection of personal data, http://ec.europa.eu/justice/data-protection/.
25. ICO.: Security breaches, https://ico.org.uk/for-organisations/guide-to-pecr/communications-networks-and-services/security-breaches/.
26. Ann Cavoukian.: Privacy by Design: The 7 Foundational Principles. https://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf.
27. Daniel J. Solove., Woodrow Hartzog.: The FTC and the New Common Law of Privacy. 114 Cal. L. Rev. 583 (2014).
28. Kamala D. Harris.: California Data Breach Report 2014. https://oag.ca.gov/ecrime/databreach/reporting/.
29. Kaori Ishii.: The Doctrine and Current Issues of Laws on the Protection of Personal Data: From the Historical Development and International Viewpoints. Keiso Publishing, Tokyo(2008).
30. Kaori Ishii.: The Present and the Future of Laws on the Protection of Personal Data: The World Surroundings and the Future Prospect in Japan. Keiso Publishing, Tokyo (2014).
31. Lisa Thomas.: Thomas on Data Breach: A Practical Guide to Handling Data Breach Notifications Worldwide. Legal Works (2015).
32. Masao Horibe., et al.: Analysis on the Legal Issues of Information and Communications. Shojihomu Publishing, Tokyo (2015).
33. Sasha Romanosky., Rahul Telang., Alessandro Acquisti.: Do Data Breach Disclosure Laws Reduce Identity Theft?. Journal of Policy Analysis and Management, Vol. 30, No. 2, 256-286(2011).
34. Taro Komukai.: Introduction to Informational Law; Law on Digital Network. NTT Publishing, 3rd ed., Tokyo (2015).