Journal of Korean Law | Vol. 15, 191-235, December 2015

Litigating Personal Data Disclosures against Information and Telecommunication Service Providers: A Korea-US Comparison*

*Joe Phillips** and Se-In Lee****

Abstract

Millions of Korean and US consumers have sought remedies for the unauthorized disclosure of personal information by Internet-based information and telecommunication service providers (ITSPs). Courts and legislatures in Korea and the United States are fashioning legal claims and remedies to address these disclosures. We contribute to this evolution with a unique comparative analysis of the law in Korea and the United States, across three areas: (1) the definition of 'personal information;' (2) possible causes of action; and (3) available remedies. We compare and contrast the two countries' legal approaches to disclosures, enriching our understanding of both jurisdictions. This article will help scholars, courts, and practitioners in Korea and the United States find an appropriate balance between consumer protection and commercial freedom. We conclude our paper by suggesting ways to improve the law's effectiveness and efficiency in addressing the exponential technological developments in information communication.

Key Words: Personal information disclosures, Identity theft, Protection of personal information, Claims for personal information disclosures, Damages for personal information disclosures

Manuscript received: Oct. 19, 2015; review completed: Nov. 25, 2015; accepted: Dec. 15, 2015.

* This work was supported by a 2-Year Research Grant of Pusan National University.

** Associate Professor, Pusan National University, Department of Global Studies

*** Professor, Pusan National University, School of Law (Corresponding author). Contact: silee@pusan.ac.kr.

I. The Rise of Personal Information Disclosures

Millions of Korean consumers have suffered the unauthorized release of personal information by Korean Internet-based information and telecommunication service providers (**ITSPs**). Some incidents have resulted in lawsuits, with varying results. Suits against Kookmin Bank led to damage awards for the consumers' mental suffering, which the Seoul High Court affirmed in 2007. Litigation against SK Communications resulted in conflicting decisions, with some lower courts finding the defendant liable and others acquitting it. So far, one appellate court has affirmed SK Comm's liability, while another court determined that the company was not liable. Both decisions are pending in the Supreme Court. In 2014, the Supreme Court rejected claims by LG U Plus members for personal information leaks. Suits against Ebay Korea (Auction) ended in February 2015 when the Supreme Court ruled that the company was not legally responsible for personal information disclosures.

United States' courts, legislatures, and administrative agencies have also struggled to address the legal issues surrounding ITSPs' failure to protect consumers' personal information.[1] In 2014, there were 1,164 incidents of unauthorized information disclosure in the United States, accounting for 72% of the worldwide total.[2] The average information breach in the United States costs approximately $5.4 million, and $159 per record disclosed (2013).[3] High-profile cases have made clear the need for legal remedies.

In 2013, computer systems at US retailer, Target Corp., were hacked,

---

1) *See* Matthew Moriarty, *Thy Brother Came with Subtlety: How a Cause of Action against Companies who Leak Data can Increase Security in the Digital Age*, 62 Univ. of Kan. L. Rev. 813 (2014) [hereinafter Moriarty].

2) Gemalto & Safenet, Year of Mega Breaches & Identity Theft (2014), http://breachlevelindex.com/pdf/Breach-Level-Index-Annual-Report-2014.pdf.

3) Robert Hamilton, *Mistakes are Costing Companies Millions from Avoidable Data Breaches*, Symantec, June 5, 2013, http://www.symantec.com/connect/blogs/mistakes-are-costing-companies-millions-avoidable-data-breaches. *See also* Verizon, Data Breach Investigations Report (2015), www.verizonenterprise.com/DBIR/2015/; Bill Hardekopf, *The Big Data Breaches of 2014*, Forbes, Jan. 13, 2015, www.forbes.com/sites/moneybuilder/2015/01/13/the-big-data-breaches-of-2014/.

compromising approximately forty-million credit cards. The claims were settled, reportedly for as much as sixty-seven million dollars.[4] A class action lawsuit was filed against Excellus BlueCross BlueShield, after a cyber-attack possibly exposed the data of approximately 10.5 million persons.[5] The US Office of Personnel Management was sued because the personal information of 4.2 million current and former federal employees was hacked.[6] Retailer Neiman Marcus faces a class action over a data breach which exposed consumers' credit card information.[7] One industry news site lists dozens more class actions, alleging unauthorized disclosures of personal information.[8]

These cases present new legal issues for Korea and the United States. What are the legal rights of consumers who *voluntarily* provide personal information to ITSPs? Can plaintiffs rely on existing legal claims or must new ones be created? What is the standard of care that ITSPs must follow? What damages can the plaintiff recover? The two jurisdictions can learn from each other in answering these questions and finding an appropriate balance between consumer protection and commercial freedom. US jurisprudence has dealt with disclosure claims longer and produced a larger, although still evolving, body of law. Korean law, on the other hand, is clearer, more uniform, and more accommodating to disclosure claims.

To tap these experiences, we describe and compare Korean and US law across three areas: (1) the definition of 'personal information;' (2) possible

---

4) James Eng, *Target Reaches Settlement with Visa over 2013 Data Breach*, Associated Press, Aug. 18, 2015, http://www.nbcnews.com/tech/security/target-reaches-settlement-visa-over-2013-data-breach-n412071.

5) Marianne Kolbasuk McGee, *Excellus Faces Breach-Related Lawsuit*, Data Breach Today, Sept. 21, 2015, http://www.databreachtoday.com/excellus-faces-breach-related-lawsuit-a-8539.

6) Schwartz Mathew J., *OPM Sued Again*, Data Breach Today, Aug. 18, 2015, http://www.databreachtoday.com/opm-sued-again-this-time-by-judge-a-8482.

7) Tracy Kitten, *Is Neiman Marcus Case a Game-Changer?*, Data Breach Today, Aug. 10, 2015, http://www.databreachtoday.com/neiman-marcus-case-game-changer-a-8462.

8) Data Breach Today, http://www.databreachtoday.com/litigation-c-320 (accessed Dec. 5, 2015). Not surprisingly, Supreme Court Chief Justice John Roberts has stated that the law's application to technology is one of the biggest challenges facing the Court. Mike Tolson, *Chief Justice Roberts: Technology among Top Issues for Court*, Chron, Oct. 17, 2012, http://www.chron.com/news/houston-texas/houston/article/Chief-Justice-Roberts-Technology-among-top-3957626.php.

causes of action; and (3) available legal remedies for a breach. We then suggest ways to improve the law's effectiveness and efficiency. In making our comparison, we focus on private, consumer claims against ITSPs. Article 2 of Korea's Information and Telecommunication Network Use Promotion and Information Act (**Network Act**),[9] defines an ITSP as (1) "any person or entity who engages in the business of transferring others' telecommunications through its electric telecommunication system or provides such an electric telecommunication system for the telecommunication of others" and (2) "anyone who, for the purpose of gaining profit, supplies information or promotes the supply of information through electric communication services provided by an ITSP."[10]

II. The Benefits of a Korea-US Comparison

A comparison between Korean and US jurisprudence is widely relevant. The US provides a large amount of global online commercial services; many Korean residents use US online services; and Korean ITSPs operate within the US, and US ITSPs operate in Korea. US jurisprudence has extensively dealt with legal issues surrounding the duty of ITSPs to protect personal information, and the US' extensive federal system provides a rich source of relevant statutes, regulations, and case law. Despite some differences between the Korean and US legal systems, both countries have similar principles and public policies protecting personal information. They have applied negligence and contract law to online information breaches. They approach causes of action, damages, and notice requirements through a combination of statutes, regulations, and cases.

Differences between Korean civil law and US common law jurisprudence do not undermine this comparison. Indeed, we find some convergence in the two countries' approaches to personal information disclosures. Korea's

9) Jeongbotongsinmang iyongchogjin mit jeongboboho deunge gwanhan beoblyul [Information and Telecommunication Network Use Promotion and Information Protection Act (**Network Act**)], Act No. 13344, Jun. 22, 2015 (S. Kor.) [hereinafter Network Act].

10) The first category of ITSPs overlaps the definition of an 'Electric Communication Enterprise,' which is set out in Jeongitongsinsaeobbeob [Electric Communication Business Act], Act No. 13011, Jan. 20, 2015 (S. Kor.).

recent adoption of penalty damages for data disclosure the Personal Information Protection Act, which will take effect in July of 2016, is similar to the US concept of punitive damages. Korean courts seem to be joining US courts in withholding compensatory damages unless the plaintiff can show actual damages from the disclosure. Attempts are ongoing in the US to pass a comprehensive federal statute, like Korea's Network Act and Personal Information Protection Act. Where these two jurisdictions differ, they provide insights for developing each country's laws. Although we have not located an extensive comparison of Korean-US approaches to the information protection duties of ITSPs, we did locate relevant articles in Korean[11] and US[12] journals, generally dealing with the legal protection of personal information.

III. What is 'Personal' Information?

Before considering the possible causes of action and remedies, the concept of 'personal information,' and more broadly, 'privacy,' should be

---

11) We did locate several articles explaining the development of Korea's legal regime for protecting personal information, including some articles dealing directly with ITSP liability, which appear in later citations in this article. The articles on development of Korea's legal regime include Yoon Jongsoo, *Gaeinjeongbobohobeobjeui Gaegwan* [*The Overview of Personal Information Protection Legislation*], 13(1) JEONGBOBEOBHAG [JOURNAL OF KOREA INFORMATION LAW] 179 (2011); and Yi Jaekyeong, Gaeinjeongbo yuchule ttaleun jeongsinjeog sonhaewa wijalyoui injeongganeungseong [*A Study on the Possibility of Psychological Damage and Consolation Money for the Leakage of Personal Information*], 20 DONGBUGABEOBYEONGU [NORTHEAST ASIAN LAW JOURNAL] 525 (2015).

12) US law journals have published articles chronicling the difficulty consumers have had holding ITSPs in US courts, but cross-country comparative analyses are less common. *See, e.g.,* Moriarty, *supra* note 1; Rachel Peters, *So You've Been Notified, Now What?*, 56 ARIZ. L. REV. 1171, 1171 (2014) [hereinafter Peters]; Peter Sloan, *The Reasonable Information Security Program*, 21 RICH. J.L. & TECH. 2 (2014) [hereinafter Sloan]; Eric T. Glynn, *The Credit Industry and Identity Theft*, 61 BUFF. L. REV. 215 (2013) [hereinafter Glynn]; Andrea M. Matwyshyn, Symposium: Data Devolution, 84 CHI-KENT L.REV. 713 (2010) [hereinafter Matwyshyn]; Jacqueline Klosek, et al., *Information Services, Technology and Data Protection*, 43 INT'L LAW. 677 (2009). For an interesting analysis on how competition/antitrust law can be used to protect personal information, see Maureen K. Ohlhausen & Alexander P. Okuliar, *Competition, Consumer Protection, and The Right [Approach] to Privacy*, 80 ANTITRUST LAW JOURNAL 121 (2015) [hereinafter Ohlhausen & Okuliar].

addressed. Privacy expectations have long roots in Korean and Anglo-American law. In 2005, the Korean Constitutional Court declared that the "individual's decision regarding personal information" is a basic right. The case involved several citizens challenging the procedure for registering ten-fingerprints upon issuance of a resident card.[13] The plaintiffs claimed that their individual right to control their personal information was being infringed. The Court held that an individual has the right to decide how and when personal information is used. Although this right is not expressly stated in the Constitution, the Court rooted it in, among other sources, constitutional Article 10,[14] which addresses dignity and the pursuit of happiness, and Article 17[15] which directly addresses privacy protection. Principles of democracy and sovereignty of the people are also relevant, according to the Court.

Although the Korean Constitution was initially applied to the relationship between the government and citizens, the current interpretation extends constitutional rights to private relationships. This is seen in court judgments regarding personal information disclosures. The Seoul Central District Court, in a lawsuit against Kookmin Bank,[16] explained that the Network Act was enacted to protect individual rights provided in the Constitution. The Seoul High Court, in *LG Electronics*,[17] also held that constitutional principles apply to private relationships through statutes like the Network Act or general principles of civil law. The most notable case is *GS Caltex*,[18] where the plaintiffs directly relied on the Constitution to sue an ITSP for breach of individual rights.

Building on these constitutional principles, the Korean Personal

---

13) Constitutional Court [Const. Ct.], 99Hun-ma513& 2004Hun-ma190, May 26, 2005 (S. Kor.). The Constitutional Court decided that the procedure for registering ten-fingerprints did not violate the individual's rights regarding personal information. Three justices dissented.

14) "All citizens shall be assured of human worth and dignity and have the right to pursue happiness. It shall be the duty of the State to confirm and guarantee the fundamental and inviolable human rights of individuals."

15) "The privacy of no citizen shall be infringed."

16) Seoul Central District Court [Seoul Cent. Dist. Ct.], 2006Gahab33062, 53332, Feb. 8, 2007 (S. Kor.).

17) Seoul High Court [Seoul High Ct.], 2008Na25888, Nov. 25, 2008 (S. Kor.).

18) Supreme Court [S. Ct.], 2011Da59834, 59858, 59841, Dec. 26, 2012 (S. Kor.).

Information Protection Act (**PIPA**) broadly defines 'personal information' as information regarding a living person, such as the person's name, resident number, or a video clip that can be used to identify the individual.[19] Even when a piece of information alone cannot identify the individual, it is considered 'personal' if identification can be accomplished by easily combining other information. The Seoul Central District Court has interpreted "easy combination" to mean that the relevant information can be joined with other information without any difficulty.[20] Accordingly, the court found that a mobile phone's international mobile equipment identity number and USIM registration number are personal information. The Network Act provides the same basic definition but adds that personal information can take various forms, such as a sign, a character, the voice, music, or a video clip (Article 2).

In Anglo-American jurisprudence, privacy protections can be found in early common law which provided remedies for eavesdropping. Prohibitions against unreasonable government intrusions were incorporated into the US Constitution with the Bill of Rights.[21] Federal and state laws, along with court decisions, typically protect against the unauthorized disclosure of (1) government identification numbers, such as numbers for driver's licenses, Social Security, passports, and military identification; (2) financial identification numbers, including numbers for accounts and credit/debit cards; (3) passwords or other security codes, when included with financial account numbers; and (4) a person's given name (or initial) and family name when included with these other pieces of identifying information.[22] Thus, as in Korea, combined information can constitute 'personal' information even when, individually, the information is not 'personal.' California's state law, for example, defines 'personal

19) Gaeinjeongbobohobeob [Personal Information Protection Act (**PIPA**)], Act No. 13423, Jul. 24, 2015, art. 2 (S. Kor.).

20) Seoul Central District Court [Seoul Cent. Dist. Ct.], 2010Godan5343, Dec. 23, 2011 (S. Kor.).

21) *See* Daniel J. Solove, *A Brief History of Information Privacy Law*, *in* Proskauer on Privacy § 1:3.1[B] (Practicing Law Institute, 2006), http://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2076&context=faculty_publications.

22) *See, e.g.*, Alaska Stat. Ann. § 45.48.090; Ariz. Rev. Stat. Ann. § 44-7501; Md. Code Ann., Com. Law § 14-3501.

information' as a first name or initial combined with the person's family name and his or her Social Security number, driver's license number, account number, medical information, or health insurance information.[23)]

Protected information can also include medical records and biometric information, like fingerprints.[24)] Encrypted information might not be considered personal if the encryption renders the information "unusable, unreadable, or indecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information security."[25)] More generally, the US Supreme Court has stated that information may be classified as 'private' when it is "intended for or restricted to the use of a particular person or group or class of persons: not freely available to the public."[26)]

Despite the two countries' common history of protecting personal information, jurisprudence in Korea and the United States has struggled to accommodate modern technology's intrusions into privacy. Voluntary disclosure platforms, along with national and demographic differences over what remains 'private,' makes "craft[ing] a universal definition of privacy … notoriously contentious and, likely, impossible."[27)] Nonetheless, societies generally agree that consumers want to protect personal identification information, especially information that can be used to access their finances. While consumers can take some steps to protect privacy when using the Internet, including programs which block and detect spyware, they must primarily rely on ITSPs to maintain security. When these service providers fail, victims look to civil litigation to compensate them and better secure their personal information.

---

23) Cal. Civ. Code Ann. § 1798.29(g)(1).

24) *See, e.g.,* Iowa Code Ann. § 715C.1; *See, generally,* Moriarty, *supra* note 1, at 820-21, 826.

25) Cal. Civ. Code Ann. § 1798.29(g)(F)(4).

26) U.S. Dept. of Justice v. Reporters Committee for Freedom of Press, 489 U.S. 749, 763-64 (1989) (quoting Webster's).

27) Ohlhausen & Okuliar, *supra* note 12, at 150.

IV. Cause of Action

The increasing complexity of digital transmission and storage of personal information means that civil litigation will play a role in compensating victims and regulating companies. The jurisprudence, however, has not settled on accepted, well-defined causes of action. The result in Korea and the United States is that plaintiffs, courts, legislatures, and administrative agencies are experimenting with existing legal theories and new ones.[28] We address the role that civil litigation is playing in this evolution, considering the most common causes of action, which are based on torts and contracts.

1. Liability - Korea

1) The Duty and Standard of Care

Various statutes in Korea contain provisions protecting personal information, but the overarching statute is the Personal Information Protection Act (**PIPA**) which protects personal information in the public and private sectors.[29] PIPA allows provisions for personal information protection found in other statutes to be applied before PIPA.[30] Other provisions include those in the Network Act governing ITSPs. The Network Act's broad definition of ITSPs includes companies like SK Communications (SK Comm), Ebay Korea, and any bank who supplies services through a telecommunication network and the Internet.

Most plaintiffs have based their claims on Article 28 of the Network Act (Protection Measures for Personal Information), which requires that ITSPs

---

28) *See* Peters, *supra* note 12, at 1171 ("There is no clear-cut state or federal civil cause of action for consumers to bring, and existing causes of action have had limited success.").

29) Before the passage of PIPA, the public sector was governed by Gonggonggigwanui gaeinjeongbobohoe gwanhan beoblyul [Personal Information Protection of Public Organization Act], Act No. 10465, Mar. 29, 2011, but, with the passage of PIPA, the Personal Information Protection of Public Organization Act was repealed.

30) Personal Information Protection Act, art. 6 (Relationship with Other Statutes) "Unless other statutes have special provisions for the protection of personal information, the provisions in this statute will be applied."

provide technological and managerial measures to prevent loss, theft, leakage, and alteration of personal information. Article 32 permits a user, who incurs damage due to an ITSP's violation of the Network Act's personal information protection provisions, to claim damages. To avoid liability, the ITSP must establish that the disclosure was unintentional and without negligence. Also applicable is Article 750 of the Korean Civil Act[31] which provides the general definition of torts: "Any person who causes losses or inflicts injuries on another person by an unlawful act, willfully or negligently, shall be bound to compensate the person for damages arising therefrom." Contract claims are available under Article 390 of the Korean Civil Act (Non-performance of Obligations and Compensation for Damages), which provides that "If an obligor fails perform its obligation, the obligee may claim damages as compensation. Provided that, this shall not apply to cases where performance has become impossible without the obligor's intention or negligence."

Article 28 of the Network Act also provides general guidance on the measures necessary to avoid liability. The enumerated protective measures are (1) an internal policy for personal information protection; (2) a trespass block to prevent illegal access to personal information; (3) measures to prevent forging or falsifying an access record; (4) security measures using encryption technology to safely store and transmit personal information; (5) preventive measures against a computer virus, such as anti-virus software; and (6) any necessary measures to secure personal information.

Article 15 of the Network Regulation,[32] promulgated under the Network Act, provides more detailed mandates for these categories. For example, to comply with the trespass block requirement, an ITSP must (1) establish a standard for granting, changing, and canceling authority to access a personal information database; (2) install and operate a trespass block and detection system to prevent illegal access to personal information; (3) establish and operate a standard for creating and changing

31) Minbeop [Civil Act], Act No. 12777, Oct. 15, 2014 (S. Kor.).

32) Jeongbotongsinmang iyongchogjin mit jeongboboho deunge gwanhan beoblyul sihaengnyeong [Enforcement Decree of the Information and Telecommunication Network Use Promotion and Information Protection Act], Presidential Decree No. 26757, Dec. 22, 2015 (S. Kor.) [hereinafter Network Regulation].

pin numbers; and (4) implement other measures necessary to restrict access to personal information. Also, to satisfy the Act's encryption requirement, the regulation mandates that the ITSP encrypt passwords, bio-information, resident numbers, and financial information.

Article 28 initially had only a general statement requiring technological and managerial measures to prevent loss, theft, leakage, and alteration of personal information. It did not enumerate the six measures until the 2008 amendment. The six specific measures were originally provided in the Network Regulation (Article 15). However, with a June 2008 amendment (effective December 2008), the six specific measures were added to Article 28 of the Act. Additionally, Article 15 of the Network Regulation was amended to provide more detailed requirements. Although there is no published source on the legislative intent of these amendments, they were probably enacted because of several personal information disclosure cases, some of which we discuss.

PIPA has a provision similar to Article 28 of the Network Act.[33] The difference is that PIPA's Article 29 lays out a general statement requiring technological and managerial measures to prevent loss, theft, leakage, and alteration of personal information, but does not enumerate technological requirements, as does the Network Act. Thus, it resembles the previous version of Article 28 of the Network Act (before the 2008 amendment). Although the relevant regulation under PIPA provides that technological requirements be installed, the regulation enforcing the Network Act provides more detailed technological requirements. It is the Network Act and its Regulation, along with contract and negligence principles, that have played the major role in resolving Korea's personal information disclosure cases against ITSPs.

P v. Ebay Korea (Assignee of Ebay Auction)

In the *Ebay Korea* case,[34] the plaintiffs had provided their personal information to Auction (Ebay Korea), including their names, resident numbers, mobile phone numbers, and e-mail addresses, in order to use the

33) Article 29 of the Personal Information Protection Act.

34) Supreme Court [S. Ct.], 2013Da43994, Feb. 12, 2015 (S. Kor.).

company's online market services. Hackers accessed one of Auction's servers, gaining the database manager's ID and password. Approximately four leaks of personal information occurred between 4 and 8 January 2008. The plaintiffs alleged that the defendant breached its duty to provide the necessary technological and managerial measures to protect personal information, as mandated by Article 28 of the Network Act. The plaintiffs also argued that the defendant breached its contractual duty to provide necessary protective measures to secure their personal information.

In a groundbreaking ruling, the Supreme Court accepted that a company, which has collected consumers' personal information, has tort and contract duties to protect the information from unauthorized disclosures, but it concluded that Auction did not breach these duties. To reach that conclusion, the Court set out the standard of liability to determine whether the ITSP provided reasonably expected security as mandated by Article 28 or the parties' privacy protection contract.

The Court did not apply a strict liability standard: The fact that Auction did not detect the hacking did not automatically mean that Auction acted unreasonably. Rather, the Court explained that the standard of care is based on various factors, including (1) the firm's business type and size; (2) the firm's overall security measures; (3) the level of security technology widely available at the time of the information breach; (4) the cost and effectiveness of the available technology; (5) the type of technology used by the hackers and the possibility of prevention; (6) the contents of personal information gathered by the firm; and (7) the damage to users due to the leakage of personal information. The Court considered these same factors in defining the standard of care under both Article 28 of the Network Act and the plaintiffs' contractual right to privacy protection.

In applying these standards, the Court appeared to adopt a cost-benefit analysis, considering (1) Auction's situation; (2) the steps taken by the company to prevent the information breach; (3) the detectability of the information breach; and (4) the predictability of the information breach. Auction's hundreds of web servers and databases made it difficult to individually monitor them, so Auction used an automated scanner to check the servers for breaches and employed a widely-used anti-virus program. The Court considered these measures reasonable, even though they failed to detect a deficiency in the server's ID and pin number or immediately

detect a breach. The Court reasoned that the hackers' program, Webshell, was technologically difficult to spot, and the amount of data queries and data transmissions by the hacker was not considered abnormal. The Court also concluded that Auction took reasonable counter-measures after it detected the breach, including providing notice to customers.

The plaintiffs argued that the standard of care required a particular type of firewall in the server, but the Court noted that the defendant had several security measures and the suggested firewall was optional under the Network Act and Regulation. The plaintiffs also argued that Auction should have encrypted the resident numbers for safe storage. The Court pointed out that, although encryption codification of resident numbers is required under the amended Regulation, it was not required at the time of the information breach (January 2008), particularly given the level of available technology.

P v. LG UPlus

In *LG U Plus*,[35] the breach originated from an employee testing the system to determine whether the server could work well with another connected server. During the testing, the employee used an ID and password but did not properly erase them after the testing. Consequently, if someone inputted a phone number in the connected server, the person could receive the associated resident number from the company. Some of the LG U Plus members learned this fact, and brought tort and contract claims, seeking five hundred thousand won per each person for mental suffering.

The Seoul Central District Court decided that the defendant breached its duty of care mandated by both Article 28 of the Network Act and the personal information protection contract with its members. The court concluded that the defendant had long maintained a very vulnerable

35) Supreme Court [S. Ct.], 2011Da24555, 24562, May 16, 2014 (S. Kor.); Seoul High Court [Seoul High Ct.] 2009Na11931 & 2009Na119148, Feb. 10, 2011 (S. Kor.); Seoul Central District Court [Seoul Cent. Dist. Ct.], 2008Gahap75268 & 2009Gahap91281, Nov. 6, 2009 (S. Kor.).The plaintiffs in both the *Auction* and *LG U Plus* cases brought tort and contract claims, but, under Korea's selective claim system, the court usually selects only one claim to resolve the plaintiff's case.

security system, allowing connections to other servers through a simple ID and password, without any IP certification. The court further decided that the plaintiffs had experienced mental suffering due to the disclosure of their personal information. According to the court, a condition where third parties can see the contents of the personal information means leakage of personal information. The trial court awarded fifty thousand won to each plaintiff.

However, the Seoul High Court reversed the lower court's decision, holding that the mere fact that conditions allowed personal information to be transmitted through the connected server did not mean that personal information was leaked to third parties. The appellate court did not conduct any analysis to decide whether the defendant breached its duty in tort or contract. Rather, court simply stated that, even if the defendant breached its duty, this does not automatically mean that the plaintiffs' personal information was leaked. Because there was no evidence that personal information was disclosed or that the plaintiffs experienced mental suffering from the defendant's breach of duty, there was no liability. The Supreme Court, applying the same reasoning, affirmed the appellate court.

Two additional lower court cases – *SK Comm* and *Kookmin Bank* – shed further light on claims available to Korean plaintiffs. The *SK Comm* case is pending before the Supreme Court.

Ps v. SK Communication

Between 26 and 27 July 2011, the server for the ITSPs, Nate and Cyword (SK Comm), was hacked, disclosing the personal information of 34,954,887 members.[36] The leaked information included customers' names, resident numbers, IDs, passwords, e-mail addresses, physical addresses, and phone numbers. SK Comm reported the incident the next day to the police and the relevant Korean administrative agency (the Broadcasting and Telecommunications Agency). The hacker accessed the server and information base through the free anti-virus program, Alzip, used by SK

36) The hacking incident is well described in the judgment of the Daegu District Court [Daegu Dist. Ct.], 2012Na9865, Feb. 13, 2014 (S. Kor.).

Comm employees. Downloading the free Alzip program connected the individual computer to the Alzip server, which the hackers used to access SK Comm's server. The hacking resulted in several lawsuits by individuals and groups of individuals, with conflicting results. Some judges declared that SK Comm had breached its duty under the Network Act and its contract with the users; other judges found no breach.

In a Daegu District Gumi City Court case,[37] the plaintiff sought three million won for mental suffering, claiming that SK Comm did not fulfill its duty to provide the technological and managerial measures required by Article 28 and its privacy contract with the plaintiff. The plaintiff alleged that SK Comm (1) violated its duty to collect the minimum necessary personal information; (2) failed to ensure that employees used the business version of Alzip; (3) used an inadequate anti-hacking technology which could not detect the transmission of personal information for approximately 3.5 million members; (4) used FTP (File Transfer Protocol) in its Gateway and DB server, even though industry standards opposed using FTP for databases because it allowed easy transmission of large information; (5) allowed the hacker to access the ID and password of the server's manager; (6) did not reasonably limit access rights to certain IP addresses or otherwise prevent unauthorized access, which allowed the hacker to reach the server through an employee's computer; (7) used the MD5 method to encrypt the password, even though MD5 was known to weakly protect personal information; and (8) did not use an automatic logout system for employees, which works as a blocking tool.

SK Comm countered that it had fulfilled tort and contractual duties to provide reasonable technological and managerial protections. Moreover, there was no causal link between the company's use of the free version of Alzip and the plaintiff's damages because the hacker could have gained access even if the business version had been utilized. Finally, the mere fact that the plaintiff's personal information was leaked did not mean that he suffered actual damages.

The trial court found the defendant liable and awarded the plaintiff one million won in damages. The plaintiff, who had sought three million won,

37) Daegu District Court Kimcheon Division [Daegu Dist. Ct. Kimcheon Div.], 2011Gaso17384, Apr. 26, 2012 (S. Kor.).

appealed; SK Comm also appealed, challenging any finding of liability. The appellate court (Daegu District Court) affirmed that the company had not properly supervised its employees' decision to use the more vulnerable version of Alzip and had failed to use industry-standard technology.[38] The technology failures were not using anti-hacking programs which could detect large information transmissions, using FTP technology which allows for easy transmission of large information, and using the MD5 method to weakly encrypt passwords. Consequently, SK Comm was liable for damages under the Network Act and the member's contract. The case has been appealed and is now pending before the Supreme Court.

Additional cases against SK Comm, filed in the Seoul Western District Court and the Seoul Central District Court, produced conflicting decisions. The Seoul Western District Court found SK Comm liable, applying reasoning similar to that used by the Gumi City Court, and awarded two hundred thousand won to each plaintiff for mental suffering.[39] However, the Seoul Central District Court stated that SK Comm did not breach its tort and contractual duties and agreed that there was no causal link between the use of the free version of Alzip and the plaintiff's damages. This court also found that the collection of resident numbers, phone numbers, addresses, and blood types did not violate the duty to collect minimum personal information. The court further held that Article 28 does not require real-time monitoring of the server; relevant security companies, like Ahn Laboratories, had certified SK Comm's protection systems; the company had anti-virus software installed in its server and personal computers; and there was an internal policy, which the company carried out for protecting personal information.[40]

---

38) Daegu District Court [Daegu Dist. Ct.], 2012Na9865, Feb. 13, 2014 (S. Kor.).

39) Seoul Western District Court [Seoul We. Dist. Ct.], 2011Gahab11733, 2011Gahab13234, 2011Gahab14138, 2012Gahap1122, Feb. 15, 2013 (S. Kor.).

40) Seoul Central District Court [Seoul Cent. Dist. Ct.], 2011Gahab129394, 2011Gahab129400, 2011Gahab105718, 2011Gahab90267, 2012Gahab46342, Nov. 23, 2012 (S. Kor.). The authors were able to obtain one written judgment, 2011Gahab90267, and described the general reasoning of all four cases by referring to Choi Ho-Jin, *Haekinge uihan gaeinjeongboyuchulgwa jeongbotongsinseobiseujegongjae daehan sonhaebaesangchaegime gwanhan gochal* [*A Study on Civil liability for Damages of the Keeper Caused by Personal Information that Leaks or is Exposed by Hacking*] 689 BUPJO 123, 126-129 (2014) [hereinafter Choi].

On 20 March 2015, the Seoul High Court reversed the decisions by the Seoul Western District Court and held the defendant not liable, applying the duty standard laid out by the Supreme Court in the *Auction* case.[41] The appellate court stated that, considering the relevant factors in total, it cannot be concluded that the hacking occurred due to the defendant's breach of its statutory and contractual duties to provide technological and managerial measures. The court declared that none of the plaintiffs' negligence claims were valid, including complaints that SK Comm had not used a real-time monitoring system and had used FTP. The court focused on establishing that the technological and managerial measures, which plaintiffs said were required, were actually not required under the Network Act and the Regulation.

We, thus, currently have two diverging appellate court decisions arising from the SK Comm information breach. The Daegu District Court held the defendant liable and Seoul High Court held the defendant not liable. These cases are now pending in the Supreme Court.

Ps v. Kookmin Bank

In the *Kookmin Bank* case,[42] the plaintiffs had contracted with the defendant bank to open an "internet lottery account," so that, when the plaintiffs maintained a certain amount in the account, the bank would purchase a lottery ticket and provide the account holders any prize money. On 15 March 2006, one of the bank's employees distributed an e-mail to 32,277 members of the internet lottery service, who had not used the service during the prior three months. The employee accidentally attached a text file containing all the members' names, resident numbers, e-mail addresses, and recent service use dates.

After realizing that the file was attached, the employee blocked the e-mail transmission, but the e-mail and attachment already had been delivered to 3,723 members. The bank was able to cancel all but 641 of these

41) Seoul High Court [Seoul High Ct.], 2013Na20047, 2013Na20054, 2013Na 20061, 2013Na20078, Mar. 20, 2015 (S. Kor.).

42) Seoul High Court [Seoul High Ct.], 2007Na33059, 33066, Nov. 17, 2007 (S. Kor.); Seoul Central District Court [Seoul Cent. Dist. Ct.], 2006Gahab33062, 53332, Feb. 8, 2007 (S. Kor.).

messages by contacting the portal site which manages the members' e-mail accounts. The bank also sent apology e-mails to those 32,277 members whose personal information was contained in the attached file; it called the 641 members who opened the e-mail message, asking them to erase the message and attached file; and it established a website help center. The bank argued that it was not negligent because the mail server system was slow and the e-mail message did not initially show that a file had been uploaded.

The court stated that uploading the file and distributing the e-mail were plainly breaches of the duty mandated by the Network Act and the members' contracts. It rejected the bank's technological defense because the evidence did not show that the server was necessarily working slowly, and, even if it was slow, that did not defeat a negligence claim. The trial court awarded compensation for the plaintiff's mental suffering. The appellate court raised the compensation amount, and its decision is now final, without an appeal.

2) The New Notice Requirement

There was no notice requirement in the Network Act until the Act's amendment which took effect on 18 August 2012. A requirement was inserted as a part of the government's overall attempt to strengthen the protection of personal information, and it mandates that ITSPs send a notice of personal information loss, theft, or leakage to the users and relevant government authority, without any delay (Article 27-3). However, after several major cases involving personal information leaks, the notice provision was once again strengthened to require that ITSPs notify the users and authorities within *twenty-four hours* of learning about the incident, unless there is "just reason" for a delay. This latest amendment took effect on 29 November 2014. The defendants, in the four cases described above, were not subject to either the 2012 or 2014 notice requirement, since the relevant incidents occurred before 2012. However, whether the ITSPs responded properly to the incident was still a factor to consider in determining their liability. Future plaintiffs can now base their tort claims against ITSPs on the new twenty-four hour notice requirement.

2. *Liability - The United States*

1) The Duty and Standard of Care

Plaintiffs in the United States, like those in Korea, have relied on a combination of tort, contract, and statutory claims, along with theories of warranty, fraud/misrepresentation, unjust enrichment, and implied-in-law contracts, when suing ITSPs for disclosure of their personal information. US courts, like those in Korea, have produced conflicting decisions on claims, standards, and notice requirements.

Duty of Care

'Negligence' is a controversial claim in disclosure cases. Negligence standards require society's members to behave 'reasonably' in a given situation, but they do not normally require one party to take affirmative action to protect another party from a third-party's negligence or otherwise aid the other party. When the ITSP has disclosed personal information because of equipment failure or an employee's mistake, then the ITSP has breached its duty of care to the information owner. However, when a third-party has hacked the ITSP or otherwise stolen the information, the ITSP might successfully argue that it had no affirmative tort duty to protect the information owner against the third-party's misbehavior, particularly when that misbehavior is criminal. US plaintiffs have attempted to avoid this defense, and impose an affirmative duty to protect identity information.

One approach is treating the ITSP like a common carrier, which has an affirmative duty to protect passengers, and an innkeeper which has an affirmative duty to protect guests. Plaintiffs have also cast ITSPs as fiduciaries, with a heightened duty to identity owners. Another tactic relies on Section 323 of the RESTATEMENT (SECOND) TORTS which legally imposes a reasonable duty of care on parties who voluntarily assume that duty; ITSPs arguably have assumed a duty to protect personal information that they have collected and stored. Some plaintiffs have attempted to establish a new claim of 'negligent enablement of identity theft,' based on the ITSP's failure to provide reasonable security protection which then enabled the

theft of personal information.[43] These and similar legal experiments can draw on a history of cases, some of which do not directly involve ITSPs but do address the duty of care owed by holders of personal information to the owners of that information.

A 2005 decision by a Michigan state appeals court held that a union owed a duty to protect members' personal identity information.[44] The daughter of the union's treasurer stole personal information, including Social Security and driver's license numbers, and was convicted for the crime; the members then sued the union for negligence. The union argued that it owed no duty to protect the plaintiffs' personal information against a third-party's criminal acts. The appeals court disagreed, explaining that a special duty arises when the plaintiff "entrusted himself to the control and protection of the defendant, with a consequent loss of control to protect himself." In deciding whether this test has been met, a court should consider

> (1) the societal interests involved, (2) the severity of the risk, (3) the burden on the defendant, (4) the likelihood of occurrence of the risk, and (5) the relationship between the parties. Other factors to consider are the foreseeability of the harm, the defendant's ability to comply with the duty, the victim's inability to protect himself, the cost of providing protection, and whether the victim bestowed any economic benefit on the defendant.

Considering these factors, including the special relationship between a union and its members, the appeals court concluded that the union had a duty to safeguard its members' private information. Notably, the court appeared to treat the union as a fiduciary and analogized its duty of care to that owed by "any financial institution [to] its clients," indicating that the court would impose the same affirmative duty in some financial relationships. However, the court made clear that it was not creating a new tort of 'identity theft negligence' and each case would turn on its particular

---

43) *See* Moriarty, *supra* note 1, at 829-33, 837-40; Glynn, *supra* note 12, at 233-36.

44) Bell v. Michigan Council 25, No. 246684, 2005 WL 356306, at *2-6 (Mich. App. February 15, 2005).

facts.

Other courts have permitted similar claims under various scenarios. A federal court in Minnesota allowed banks issuing credit cards to sue a retailer for breaching the general duty of reasonable care. The retailer allegedly disabled certain security features for debit and credit card transactions and failed to heed warning signs that its system was being hacked.[45] In a California federal court case, a job applicant could proceed with his negligence and statutory-based privacy claims against a prospective employer, after laptop computers, containing applicants' unencrypted personal information, was stolen from the employer's agent.[46]

Expressed and implied contract claims have sometimes survived dismissal motions. In *Andersen v. Hannaford Brothers Co.*, the federal appeals court for the First Circuit permitted customers to sue a grocery store for breach of an implied contract (and negligence), after their electronic payment information was allegedly stolen.[47] The court explained:

> When a customer uses a credit card in a commercial transaction, she intends to provide that information to the merchant only. Ordinarily, a customer does not expect—and certainly does not intend—the merchant to allow unauthorized third-parties to access that information. A jury could reasonably conclude, therefore, that an implicit agreement to safeguard the information is necessary to effectuate the contract.[48]

Similarly, a New York appeals court reasoned that an insurance company had an "implied covenant of trust and confidence," essentially a fiduciary duty, to protect insureds' confidential personal information from access by unauthorized employees.[49]

---

45) In re Target Corp. Customer Data Security Breach Litigation, 64 F. Supp. 3d 1304, 1310-11 (D. Minn. 2014) (applying Minnesota law).

46) Ruiz v. Gap, Inc., 540 F. Supp. 2d 1121, 1126, 1228 (N.D. Cal. 2008) (applying California law).

47) Anderson, 659 F.3d 151, 157-59 (1st Cir. 2011).

48) *Id.* at 159.

49) Daly v. Metropolitan Life Ins. Co., 782 N.Y.S.2d 530, 534-36 (2004) (possibly relevant was that the insurance company had issued a privacy notice to the plaintiff, stating that the

Victims of identity disclosures might also have statutory claims under state consumer protection laws which allow private causes of action for deceptive and unfair actions. For example, a North Carolina trial court allowed union members to proceed with a statutory deceptive trade practices claim against their union for posting personal information, including Social Security numbers, on a bulletin board.[50]

Plaintiffs have often failed in their attempts to craft negligence and contract claims for unauthorized information disclosures. In a Massachusetts case, the plaintiff sued her credit card company which had allowed fraudulent charges after notification that a hacker had obtained the plaintiff's credit card information from a merchant's website server. The credit card company's privacy notice and customer agreement stated that it "can protect you from identity theft, fraud, and unauthorized access to personal information." Nonetheless, the trial court rejected the plaintiffs' negligence, fiduciary duty, contract, and deceptive trade practices claims. The court ruled that the language "merely suggests" that the credit card company is in a better position to protect the customer, but there was no "guarantee." Nor did the language establish a fiduciary duty, rather the parties had an ordinary debtor-creditor relationship.[51]

A federal district court in New York dismissed a claim against a credit reporting agency for breaching a fiduciary duty by selling the plaintiff's Social Security number and other sensitive identifying information without the plaintiff's consent. The plaintiff had furnished the information to obtain a credit report; the court concluded that this transaction, alone, did not create a fiduciary relationship.[52] In *Anderson v. Hannaford Brothers Co*, the same First Circuit decision that had allowed an implied contract cause of action rejected a fiduciary duty claim against the defendant grocery store

---

company took great care to protect personal information).

50) Fisher v. Communication Workers of America, No. 08 CVS 3154, 2008 WL 4754850, at *6 (N.C. Super. Ct. October 30, 2008). State laws sometimes allow victims to directly sue the hacker. *See* ALA. CODE §§ 13A-8-191, 13A-8-199 (victim may recover the greater of $5,000 or three times the actual damages).

51) Kuhn v. Capital One Financial Corp., No. CA015177, 2004 WL 3090707, at *3-7 (Mass. Super. November 30, 2004).

52) Menton v. Experian Corp., No. 02 Civ. 4687, 2003 WL 941388, at *4-5 (S.D. N.Y. March 6, 2003).

because there was no evidence of special trust, disparity of bargaining power, or the store's abuse of trust.[53]

Standard of Care

Once US plaintiffs are allowed to proceed with their claims, they, like plaintiffs in Korea, must establish that the defendant violated the standard of care, and, as in Korea, that standard is still developing. Courts have found several factors important: (1) the sensitivity of the personal information; (2) the risk of an information breach; (3) the defendant's awareness or the foreseeability of a breach; (4) whether concerns over security previously had been raised within the defendant organization; (5) whether the defendant heeded warning signs of a hacker's attack; (6) whether the defendant had procedures to protect against breaches; (7) the availability of reasonable and cost-effective security measures; (8) industry practices; and (9) whether the defendant represented its system as secure.[54] This list is not exhaustive, and courts are evolving standards as new fact patterns are litigated.

One reference point for constructing the standard is the patchwork of federal statutes and regulations protecting private information.[55] Describing, even listing, these numerous statutes is beyond this article's scope, but they include the following. The Financial Services Modernization Act (1999) requires financial institutions to have safeguards protecting customer information.[56] The Health Insurance Portability and Accountability Act (1996) prohibits use of a patient's medical data other than for the purposes for which the patient provided the information.[57] The Children's Online Privacy Protection Act (1998) requires websites that target children younger

53) Anderson, 659 F.3d at 157-58.

54) *See* In re Target Corp., 64 F.Supp.3d at 1310-12; Wolfe v. MBNA America Bank, 485 F.Supp.2d 874, 881-82 (W.D. Tenn. 2007); Bell, 2005 WL 356306 at *4-5; Daly, 782 N.Y.S.2d at 535-36. Courts can also draw on the 'state-of-the-art' defense used in product liability cases to assess whether available scientific knowledge could have prevented the disclosure. *See* Anderson v. Owens-Corning Fiberglas Corp., 810 P.2d 549, 551 (Cal. 1991).

55) *See* Sloan, *supra* note 12.

56) Gramm-Leach-Bililey Act, 15 U.S. Code §§ 6801-03.

57) HIPPA, 45 U.S.C. §§ 164.502 et seq.

than thirteen, or that knowingly collect information from children, to post privacy policies, obtain parental consent before collecting information, offer an opt-out before collection, and allow parents to decide how the information is used.[58] The Driver's Privacy Protection Act (1994) prohibits states from disclosing or selling a driver's personal information.[59] The Tax Reform Act (1976) established a general rule of confidentiality for tax records, subject to congressional exceptions.[60] The Family Education Rights and Privacy Act (1974) gives parents control over the disclosure of their children's educational records and, absent a legal exception, requires an adult student's consent before disclosure.[61]The Federal Trade Commission Act (1914) prohibits "deceptive" and "unfair" trade practices,[62] and the Federal Trade Commission has applied the act to companies' data protection practices.[63]

'Red Flag Rules,' issued pursuant to the Fair and Accurate Credit Transactions Act (2003), require financial institutions and some creditors to establish reasonable policies and procedures to identify "suspicious patterns or practices, or specific activities that indicate the possibility of identity theft." An example would be a person's attempt to open a financial account with suspicious identification. The policies and procedures must also set out appropriate reactions to the flags, such as changing passwords and other security codes, and a mechanism for updating the monitoring system.[64]

Unlike the Korean Network Act and Personal Information Protection Act, these US statutes and regulations do not provide private causes of action, but could function as models for the duty requirement and standard of care.[65] Unfortunately, these acts tend to be vague. For example, the

---

58) COPPA, 15 U.S.C. §§ 6501-6503.

59) DPPA, 18 U.S.C. §§ 2721-25.

60) TRA, 26 U.S.C. § 6103.

61) FERPA (Buckley Amendment), 20 U.S.C. § 1232g.

62) FTCA, 15 U.S.C. § 45.

63) *See, e.g.,* Complaint, Geocities, FTC Docket No. C-3850 (Feb. 5, 1999), https://www.ftc.gov/enforcement/cases-proceedings/982-3015/geocities.

64) Red Flag Rules, 16 U.S.C. § 681.1. *See* Fact Sheet 6a, Privacy Rights Clearinghouse, https://www.privacyrights.org/fs/fs6a-facta.htm (last visited Dec. 5, 2015).

65) Glynn, *supra* note 12, at 231-36. For example, The Federal Deceptive Trade Practices Act does not provide a private cause of action similar to that found in state DTPAs. Holloway

Financial Services Modernization Act simply provides that a financial institution "shall not disclose, other than to a consumer reporting agency, an account number or similar form of access number or access code for a credit card account, deposit account, or transaction account of a consumer to any nonaffiliated third party for use in telemarketing, direct mail marketing, or other marketing through electronic mail to the consumer."[66]

Two relevant federal statutes do allow private actions, though their coverage is significantly limited. The Fair Credit Reporting Act (1970) protects personal financial information collected by credit reporting agencies and requires that these agencies "adopt reasonable procedures for meeting the needs of commerce for consumer credit, personnel insurance, and other information … with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information…."[67]A consumer may sue for actual damages for a negligent breach of the duty, penalty damages for a willful violation, and costs and reasonable attorney's fees.[68] The Computer Fraud and Abuse Act (1986) creates a private civil cause of action for persons who suffered a loss of at least five thousand dollars, aggregated over one-year, or when the damage affects ten or more protected computers within one-year.[69] The act does not include a claim for the negligent design or manufacture of computer hardware, computer software, or firmware, and the minimum dollar amount has proven difficult for victims to establish.

Two more recent and broadly useful references are the Obama Administration's proposed Consumer Privacy Bill of Rights Act (2015) and The President's Identity Theft Task Force Report (2008).The Privacy Bill of Rights would cover entities that collect, create, use, or disclose personal

---

v. Bristol-Myers Corp., 485 F.2d 986, 987-1001 (D.C. Cir. 1973).

66) Gramm-Leach-Bililey Act, 15 U.S.C. § 6802(d).

67) FCRA, 15 U.S.C. § 1681(b).

68) 15 U.S.C. §§ 1681n - 1681o. *See* Boggio v. USAA Federal Savings Bank, 696 F.3d 611, 615 (6th Cir. 2012) (FCRA recognizes private right of action against furnisher of credit information, but only for failing to comply with FCRA requirements); Perry v. First National Bank, 459 F.3d 816, 823 (7th Cir. 2006) (congressional amendments to FCRA eliminated private enforcement of a § 1681m violation).

69) 18 U.S.C. § 1030.

information.[70] The entities must (1) identify risks to the privacy and security of personal information; (2) implement safeguards reasonably designed to ensure the security of such personal information; and (3) regularly assess and adjust the sufficiency of these safeguards. The 'reasonableness' of the safeguards is determined considering (1) the degree of privacy risk associated with the personal information; (2) the foreseeability of threats to the security of the information; (3) widely-accepted administrative, technical, and physical safeguards for protecting personal information; and (4) the cost of implementing and regularly reviewing the safeguards. The Task Force Report provides recommendations to reduce the incidence and impact of identity theft, including policies for data protection and avoiding criminal misuse of data.[71]

Several states have enacted standards for the safeguarding and disposing of personal information. For example, Massachusetts state law requires that "Every person that owns or licenses personal information about a resident of the Commonwealth shall develop, implement, and maintain a comprehensive information security program…."[72] To accomplish this, the statute lists non-exclusive procedures, including disciplinary measures for violations and standards for selecting and maintaining third-party providers who can follow appropriate security measures.

2) The Notice Requirement

US law, like Korea's, generally requires ITSPs to provide notice when

---

70) Consumer Privacy Bill of Rights Act of 2015 (Draft), https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf. *See also*, National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity (Feb. 12, 2014), http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

71) The Federal Trade Commission, The President's Identity Theft Task Force Report (September 2008), https://www.ftc.gov/reports/presidents-identity-theft-task-force-report [hereinafter Task Force Report]. *See also* proposed Data Security and Breach Notification Act of 2013, S. 1193, 113th Cong. § 6 (2008), https://www.govtrack.us/congress/bills/113/s1193.

72) Mass. Regs. Code tit. 201, §§ 17.00 et seq.; § 17.03-04. *See, generally,* Selected State Laws Governing the Safeguarding and Disposing of Personal Information, Vedder Price, http://www.vedderprice.com/selected-state-laws-governing-safeguarding-and-disposing-of-personal-information/ (last visited Dec. 5, 2015). Other sources of standards are the U.S. - EU Safe Harbor Framework, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/u.s.-eu-safe-harbor-framework (last visited Dec. 5, 2015).

there is an information breach. Forty-seven states have notification laws mandating that private or government entities notify individuals of breaches involving personal information.[73] The time frame for notification is often vague; some states provide a specific deadline, from five to forty-five days after discovery of the breach, while others require notice in the most expedient time possible. Some laws permit delays for an investigation and analysis of the consequences of the breach.[74] Some permit extensions when required by legitimate law enforcement needs, such as when notification could interfere with a criminal investigation.[75] California's law is notable because it requires that notice be accompanied by an offer to provide free and appropriate identity theft prevention and mitigation services for at least twelve months, if the breach exposed or may have exposed the person's Social Security, driver's license, or state identification card number.[76]

The adequacy and timeliness of notice can be a fact question based on the specific circumstances. In a federal district case from Illinois, a large retailer was the victim of 'pin pad skimming' which allowed the skimmers to capture the plaintiffs' credit numbers and passwords.[77] The plaintiffs alleged that the retailer violated Illinois' Personal Injury Protection Act which required that the merchant notify the plaintiffs of the information breach "in the most expedient time possible and without unreasonable delay." The retailer claimed that it timely notified affected customers and sought to dismiss the case. The court denied the dismissal motion because there were disputed fact issues regarding when the retailer first learned of the information breach and, consequently, whether the notice was in the

---

73) National Conference of State Legislatures, Security Breach Notification Laws, June 11, 2015, http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx. Many states also have pending legislation which adds to or amends existing law. National Conference of State Legislatures, 2015 Security Breach Legislation, June 11, 2015, http://www.ncsl.org/research/telecommunications-and-information-technology/2015-security-breach-legislation.aspx.

74) *Id. See, e.g.*, Ariz. Rev. Stat. Ann. § 44-7501; Haw. Rev. Stat. Ann. § 487N-1. *See also* Jill Joerling, *Data Breach Notification Laws: An Argument for a Comprehensive Federal Law to Protect Consumer Data*, 32 Wash. U. J.L. & Pol'y 467, 474-76 (2010).

75) *See, e.g.*, Me. Rev. Stat. Ann. tit. 10, § 1348(3); Fla. Stat. Ann. § 501.171(4)(b).

76) Cal. Civil Code § 1798.82.

77) In re Michaels Stores Pin Pad Litigation, 830 F. Supp. 518, 527-28 (N.D. Ill. 2011).

"most expedient time possible."

3. The Causes of Action – A Comparison

Both Korea and the United States now have a body of statutory and case law that sometimes allows plaintiffs to sue ITSPs for the unauthorized disclosure of personal information and failure to notify victims of the disclosure. Korea has earlier and more fully accepted these claims than has the United States, and, not surprisingly, Korean jurisprudence on information security is more uniform. The multiple US jurisdictions remain divided over whether and which claims are available, but the trend is toward recognizing some types of claims, primarily by expanding current legal duties to impose an obligation on ITSPs to protect against disclosures.

While the United States may be in an expansion stage, Korean courts appear to be retreating from their early accommodative rulings. The initial successful cases of the early 2000s often involved obvious security failures, and the plaintiffs probably benefited from an initial public shock over those breaches. As ITSPs have better addressed security risks and the breaches have proliferated, Korean appeals courts appear more cautious about permitting claims. The Supreme Court's decision in the *Auction* case and the Seoul High Court's ruling in *SK Comm* may portend this new approach.

If Korean courts become more conservative, Korean claimants will need to experiment, as US plaintiffs have, with a diverse set of legal theories. Judge Choi Ho-Jin has opened this door, arguing that, even when an ITSP is not liable under Article 28 of the Network Act, it may be legally responsible under the general tort duty set out in Article 750 of the Civil Act. Article 750 is more open-ended, allowing plaintiffs and courts flexibility in shaping the standards for adequate information protection.[78] Judge Choi's argument would permit courts to move beyond their recent focus on whether the ITSP incorporated mandated technological measures and, instead, impose a broader standard of reasonable care.

Regardless whether these two jurisdictions are expanding or contracting claims, both need to further clarify the standards for ITSPs to reasonably

78) Choi, *supra* note 40, at 145-147.

protect information and provide notice of a breach. Even seemingly specific statutory notice provisions, such as Korea's Article 27-3 of the Network Act have ambiguous exceptions that sometimes permit delays with just reason. Ambiguity allows ITSPs flexibility in determining when, and in the United States *if*, notice is required.

The lack of clarity reflects the legal field's evolving efforts to address unauthorized personal information disclosures. So far, trial courts have largely fashioned the standard of care. Even frequent amendments to Korea's Network Act and underlying Regulation leave much room for courts to model the standards. Consequently, although the Korean legal system evolved from a civil law, statutory tradition, it is relying on courts to shape these standards almost as much as is the US' common law jurisprudence.

Trial courts necessarily produce more numerous and diverging results, and here, the Korean system has advantages. Compared to the US legal system, Korean courts have more quickly provided appellate, even Supreme Court, guidance. Most US appellate decisions have dealt with the trial court's preliminary dismissal of cases rather than the result of completed trials which finally determined ITSP liability. Only when more verdicts reach the appellate courts will US standards become clearer. The US class action system may hamper this process, since class actions frequently result in settlements, preventing appellate courts from contributing to the law's evolution. Korean litigants often reject settlement and press their arguments into the appellate levels. Ambiguous standards of care also result from rapid changes in both hacking and security technology, which make crafting specific criteria difficult for slow-moving courts and legislatures. But 'duty' is not the only legal area in flux; both Korea and the United States are struggling to define the remedies available in information disclosure cases.

V. The Remedies

Various issues have arisen regarding plaintiffs' legally available remedies for an information breach. For example, must the plaintiff suffer an economic loss or is a fear of loss enough? Can plaintiffs recover their

costs for mitigating the risks from an information disclosure (e.g., the cost of identity theft insurance)? Are mental anguish damages available? Is there a role for injunctive relief?

1. Remedies - Korea

The Network Act not only permits a private claim against ITSPs, but a new damage provision, added in 2014, provides a statutory damage amount of not more than three million won when the ITSP intentionally or negligently violated the personal information protection provisions.

Most plaintiffs, who have brought actions against ITSPs for a personal information breach, asked for consolation money for their mental suffering. 'Consolation money' is compensation given for mental anguish in Korea, and it can be awarded without any economic or physical injury. The relevant Civil Act provision (Article 751, Compensation for Non-Economic Damages) states that "a person, who has injured the body, liberty, or fame of another, or has inflicted any mental anguish on another person, shall be liable to make compensation for damages arising therefrom." The majority of scholars in Korea categorize consolation money as compensation for actual damages, but some argue that it is used to penalize the defendant's bad behavior.[79] It is also said that consolation money has a supplementary function: when it is difficult to calculate economic damages, consolation money is used to supplement the plaintiff's recovery. The Korean Supreme Court has cautioned that consolation money should be very carefully used for this purpose and only when there is no doubt that economic damage has incurred.[80]

Korean courts awarded consolation money in some earlier cases against ITSPs but, recently, seem somewhat unwilling to do so. We introduce three cases – *Kookmin Bank, LG Electronics and SK Comm* – where courts held the defendant companies liable and awarded consolation money.

---

79) Lee Chang-Hyun, Wijalyoe Gwanhan Yeongu [A Study on Consolation Money-Focused on Torts] 259-260 (2011).

80) *Id.* at 268. Supreme Court [S. Ct.], 84Daca722, Nov. 13, 1984 (S. Kor.).

Ps v. Kookmin Bank

In *Kookmin Bank*, the trial and appellate courts awarded consolation money, concluding that the plaintiffs must have had mental suffering which the defendant could foresee. The trial court considered various factors in determining the award. An ITSP has a high duty of care in handling personal information, given the vulnerability and complexity of computer and Internet technology. The Network Act and the Regulation provide active duties to deliver a system to protect personal information. The defendant failed to fulfill this duty. The resident numbers were leaked, which created a risk that other personal information related to the number could be misappropriated and misused. Even if, as the defendant argued, there was no concrete and present damage to the plaintiffs from the leak, the plaintiffs' mental suffering was an 'ordinary damage,' since the plaintiffs' rights were related to a private right provided by the Constitution. The court explained that the defendant's quick reaction to the disclosure, and the absence of reported misuse by a third party, were factors in calculating damages, but they did not establish that there was no mental suffering.

Ps v. LG Electronics

Ps v. LG Electronics involved the disclosure of the personal information of more than three thousand job applicants, stored in the defendant's Internet application site.[81] The appellate court, applying Article 750 (Torts) of the Korea Civil Act, decided that LG Electronics breached its duty of care under the Article, primarily because the defendant did not provide basic security available at that time. Anyone could easily identify the URL of the job application site by simultaneously pressing the keyboard's 'ctrl key' and 'N key,' and, by doing this, one college student gathered and distributed the job applicants' personal information.

The appellate court listed seven factors to consider in deciding the

81) Seoul High Court [Seoul High Ct.], 2008Na25888, Nov. 25, 2008 (S. Kor.).

amount of consolation money: (1) the security level adopted by the company at the time of the breach; (2) whether the defendant took quick and proper steps to minimize the damage after the breach; (3) whether the defendant took proper steps to notify the victims and compensate them; (4) the type and amount of leaked information; (5) how widely the personal information was distributed and the possibility of further distribution; (6) whether there was additional damage, such as names being used for unlawful purposes; and (7) whether the company profited by storing and processing the personal information. The court further decided that the plaintiffs had experienced mental suffering due to the disclosure of their personal information. 'Leaking personal information,' according to the court, means a situation where third parties can see the contents of the personal information outside the defendant's managerial boundary. The trial court awarded fifty thousand won in consolation money to each plaintiff.

Ps v. SK Comm

As earlier discussed, there were two conflicting appellate court judgments in the *SK Comm* cases. In an appellate decision by the Daegu District Court, the court considered the totality of various factors to determine if the plaintiff had mental damages. Those factors were (1) the types and characteristics of the leaked personal information; (2) whether the owner could be identified from the leaked information; (3) whether a third party saw or may possibly see the information; (4) how widely the leaked information was distributed; (5) whether the plaintiff's legal rights might be infringed due to the disclosure; (6) how the defendant managed the personal information which was leaked; and (7) measures taken by the defendant to minimize any damage due to the leak. These factors were laid down by the Supreme Court in the well-known *GS Caltex* personal information disclosure case to determine whether plaintiffs experienced mental suffering.[82)]

82) Supreme Court [S. Ct.], 2011Da59834, 59858, 59841, Dec. 26, 2012 (S. Kor.). In *GS Caltex*, some employees of customer service agents stole the personal data of eleven million customers. The employees placed the customers' names, resident numbers, addresses, phone

The Daegu District Court used these factors to determine that mental anguish damages had occurred and the compensation should be one million won. The leaked information was basic personal information such as the plaintiff's name, resident number, ID, password, address, and phone number. The resident number was the most important and sensitive information disclosed, because it is widely used by government and financial agencies. Although the hacker's purpose was not clear, this type of personal information has been misused for fraud through various communications tools, such as the phone, text messages, and e-mails. There was a considerable possibility that the leaked information had already been distributed or would be distributed for a profit. There was a possibility that additional violations of the plaintiff's legal rights would occur because of the leak. SK Comm was careless in carrying out its duty to protect personal information. Because of the hacking, the plaintiff felt anxious regarding the disclosure of his personal information, its unlawful use, and possible additional damages.

2. Remedies – United States

US law regarding remedies for a personal information disclosure is more complicated and uncertain than that in Korea. For any civil claim, the plaintiff must, first, demonstrate an injury sufficient to create standing to bring the lawsuit. Next, the plaintiff must establish that the relief sought is legally recoverable. Finally, the plaintiff will prove the amount of damages. US plaintiffs have had difficulty establishing injury and damages because it is often uncertain whether the breach disclosed their personal information, whether the disclosed information has been or will be used to cause financial injury, and the nature of the injury. Even when personal information is misused, it may be difficult or impossible to prove that the information came from the security breach. The plaintiff must establish

---

numbers, and e-mail addresses on a DVD and reported the theft through the media to gain leverage in lawsuits against GS Caltex. More than two thousand plaintiffs filed a lawsuit against GS Caltex, claiming a breach of their constitutional rights to control personal information. They sought consolation money for their mental suffering. The Supreme Court affirmed the lower court's decision not to award damages.

that no other disclosures occurred; a plaintiff who is the victim of multiple information breaches may be without a remedy.

Standing

Understanding the plaintiff's burden of proof begins with the US Supreme Court case of *Clapper v. Amnesty International USA*, which held that, to establish standing, the injury must be "certainly impending" and not based on "a highly attenuated chain of possibilities."[83] Standing cannot be based on fears of a "hypothetical future harm."[84] Even when there is an "objectively reasonable likelihood" of an injury, the injury is not necessarily "certainly impending."[85]

In personal information disclosure cases, standing is clearly established when the data have been misused in a manner that costs the plaintiff financially. For example, in *Resnick v. AVMed Inc.*, current and former members of health care plans sued the plan operator because unencrypted laptops, containing the members' sensitive information, were stolen from the operator.[86] Information regarding one class representative was used by a third party to set up credit cards and make unauthorized purchases; for another representative, a financial account was opened and overdrawn. The Eleventh Circuit federal appeals court found that these harms were not speculative and, thus, satisfied the injury requirement.

The injury is less clear when the plaintiff faces only a risk of future harm

---

83) Clapper v. Amnesty International USA, 133 S. Ct. 1138, 1147-51 (2013). We discuss the federal standard for 'standing' because many cases have been litigated in federal courts. However, the state court claims will turn on state law, which may have different requirements for standing.

84) *Id.* at 1143.

85) *Id.* at 1147-48. The *Clapper* standard became somewhat less clear after the Supreme Court's decision in *Susan B. Anthony List v. Driehaus,* where the Court stated that "An allegation of future injury may suffice if the threatened injury is 'certainly impending,' or there is a "'*substantial risk*' that the harm will occur." *See* Susan B. Anthony List v. Driehaus, 134 S.Ct. 2334, 2341 (2014) (emphasis added). Consequently, a federal district court in Illinois has interpreted *Driehaus* as indicating that the 'imminence' standard is applicable only to cases involving national security or constitutional issues. Moyer v. Michaels Stores, Inc., 2014 WL 3511500 at *5 (N.D. Ill. July 14, 2014).

86) Resnick v. AVMed Inc., 693 F.3d 1317, 1326-27, 1330 (11th Cir. 2012).

from the disclosure; here, U.S. courts are divided. The more conservative view is represented by the First and Third federal appeals courts which have indicated that, where there has been an information breach but it is uncertain whether the plaintiff's identity data have been acquired, the mere increased risk of future harm is too hypothetical to create standing.

In *Katz v. Pershing*, the plaintiff was an account holder in a brokerage firm that subscribed to the defendant's electronic platform which allowed the brokerage to manage client accounts.[87] The plaintiff claimed that the defendant's platform permitted unauthorized access to her personal information, but she did not claim that there had been an unauthorized disclosure or misuse of that information. Nonetheless, the plaintiff, fearing an increased risk of identity theft, purchased identity theft insurance and credit monitoring services. The First Circuit held that the plaintiff had not suffered a sufficient injury because the "risk of harm that she envisions is unanchored to any actual incident of information breach."[88]

The Third Circuit reached the same conclusion in *Reilly v. Ceridian Corporation*, where a law firm's employees sued their employer's payroll processing firm over a security breach.[89] The plaintiffs alleged that they suffered an increased risk of identity theft and incurred costs to monitor credit activity. The appeals court held that the plaintiffs merely speculated that the hacker read, copied, and understood their personal information, intended to misuse the information, and could misuse it to the plaintiffs' detriment. The court concluded that "Unless and until these conjectures come true, [plaintiffs] have not suffered any injury."[90] Consequently, the plaintiffs' expenditures for credit monitoring were not actual injuries, because the plaintiffs incurred them in anticipation of a hypothetical, speculative future criminal act.[91]

---

87) *See also* Katz v. Pershing, L.L.C., 672 F.3d 64, 70, 79 (1st Cir. 2012).

88) *Id.* at 79-80.

89) Reilly v. Ceridian Corp., 664 F.3d 38, 40-43 (3d Cir. 2011).

90) *Id.* at 42.

91) *Id.* at 42. *See also* Green v. eBay Inc., 2015 WL 2066531, at *4-5 (E.D. La May 4, 2015) (plaintiffs sought damages for a data breach, including expenses and time spent to mitigate the increased risk of identity theft; district court dismissed the claims because increased risk of future identity theft or fraud was not "concrete, particularized, and imminent;" and mitigation expenses are not recoverable unless the threat is imminent); Allison v. Aetna, Inc.,

Other courts have applied a more liberal injury standard, sometimes analogizing personal information disclosures to 'latent injuries.' The latent injury rule permits a plaintiff to bring a lawsuit when she has suffered an incomplete injury that has placed her at an increased risk of future harm.[92] The rule is commonly applied in cases of toxic exposure, other environmental injury, and defective medical devices, where the plaintiff's future injury is more a possibility than a certainty.[93] It better ensures fairness for the plaintiff, who need not wait until all injuries have manifested to sue, and it promotes economic efficiency by providing the plaintiff with an early monetary remedy so that she can seek medical treatment and, possibly, reduce her future injuries.[94]

The Ninth Circuit pursued this reasoning in *Krottner v. Starbucks Corporation*, where a laptop, containing employees' personal identity information, was stolen from their employer, Starbucks.[95] Two employees brought a putative class action claiming that Starbucks breached various duties by not protecting the personal information. There was no evidence that the information had been misused, but the class representatives alleged that they had spent time and would spend money on credit monitoring; one class representative also claimed "generalized anxiety and stress." The

---

2010 WL 3719243, at *5-6 (E.D. Pa. March 9, 2010) (users of Aetna's website received phishing emails supposedly from Aetna; plaintiffs had not suffered any loss from the theft but sought cost for credit monitoring; district court held that risk of identity theft, which is not imminent, is not an injury-in-fact and, thus, monitoring costs were not related to an actual injury). *See also* Jonathan Wall, *Why the Third Circuit Should Recognize Fear of Identity Theft as an Injury-in-Fact*, 22Temp. Pol. & Civ. Rts. L. Rev. 587 (2013).

92) *See* James P. Nehf, *Recognizing the Societal Value in Information Privacy*, 78 Wash. L. Rev. 1, 7 (2003).

93) *See* Carlough v. Amchem Products, Inc., 834 F.Supp. 1437, 1454-55 (E.D. Pa. 1993) (plaintiffs exposed to asbestos, but who had not developed asbestos-related conditions, met injury-in-fact requirement for standing, since the weight of recognized medical research shows that exposure to asbestos causes immediate cellular changes).

94) The Sixth Circuit explained that "There is something to be said for disease *prevention,* as opposed to disease *treatment.* Waiting for a plaintiff to suffer physical injury before allowing any redress whatsoever is both overly harsh and economically inefficient." Sutton v. St. Jude Medical S.C., Inc., 419 F.3d 568, 575 (6th Cir. 2005) (emphasis included). *See also* Restatement (Second) of Torts (person "whose legally protected interests have been endangered by the tortious conduct of another is entitled to recover for expenditures reasonably made or harm suffered in a reasonable effort to avert the harm threatened").

95) Krottner v. Starbucks Corp., 628 F.3d 1139, 1141 (9th Cir. 2010).

Ninth Circuit held that the anxiety and stress were the only present injuries. Credit monitoring services were a future injury because Starbucks voluntarily provided free monitoring for one year, and the time spent guarding against future identity theft did not involve a present injury. The court, however, accepted that future injuries can, sometimes, establish standing if the "plaintiff faces 'a credible threat of harm' … and that harm is 'both real and immediate, not conjectural or hypothetical….'"[96] The court analogized this standard to the latent injury rule.[97]

The Eleventh Circuit, in *Pisciotta v. Old National Bancorp*, also employed a more flexible approach.[98] The defendant, ONB, operated a marketing website where individuals could make online applications for accounts, loans, and other banking services. ONB suffered a security breach, and the plaintiffs filed a putative class action, claiming that ONB failed to protect their confidential information. The plaintiffs did not allege any financial loss to their accounts or that any other member of the putative class had been the victim of identity theft because of the breach.[99] Nonetheless, the appeals court found a sufficient injury for standing:

> Many … cases have concluded that the federal courts lack jurisdiction because plaintiffs whose data has [sic] been compromised, but not yet misused, have not suffered an injury-in-fact sufficient to confer Article III standing. We are not persuaded by the reasoning of these cases. As many of our sister circuits have noted, the injury-in-fact requirement can be satisfied by a threat of future harm or by an act which harms the plaintiff only by increasing the risk of future harm that the plaintiff would have otherwise faced, absent the defendant's actions. We concur in this view. Once the plaintiffs allegations establish at least this level of injury, the fact that the plaintiffs anticipate that some greater

96) *Id.* at 1143.

97) *Id. Accord* Ruiz v. Gap, Inc., 380 F. App'x 689, 690-91 (9th Cir. 2010) (plaintiff had standing to sue prospective employer after employer's laptop, which contained plaintiff's Social Security number, was stolen; plaintiff was subjected to an increased risk of identity theft).

98) Pisciotta v. Old National Bancorp, 499 F.3d 629 (7th Cir. 2007).

99) *Id.* at 631-32.

potential harm might follow the defendant's act does not affect the standing inquiry.[100)]

Judicial division continues over standing in personal information disclosures cases. Some very recent federal district court cases have accepted that an elevated risk of identity theft satisfies the injury requirement,[101)] while others have found this risk insufficient.[102)] The US Supreme Court recently granted *certiorari* in *Spokeo v. Robins* which will shed light on the injury requirement necessary for standing in federal courts.[103)] Robins filed a putative class action against Spokeo (a 'people search engine'), claiming that it exaggerated his education and wealth and these inaccuracies injured him. But, critically, he argued that, even if he did not suffer actual harm, the online profile's mistakes violated the Fair Credit Reporting Act (FCRA) and this statutory violation, alone, created standing to sue. The Ninth Circuit appeals court agreed.[104)] Though the case addresses the FCRA, one of the rare federal statutes granting a private cause of action for identity disclosure, accepting Robins' argument could liberalize courts' general approach to standing in personal information disclosure cases.[105)]

---

100) Pisciotta, 499 F.3d 629, 634 (7th Cir. 2007). *See also* Task Force Report, *supra* note 71, at 46. (task force recommended that a 'victim' be defined as any person who sustained any monetary or non-monetary harm, including the theft of a means of identification, invasion of privacy, reputational damage, and inconvenience).

101) *See, e.g.,* In re Adobe Systems, Inc. Privacy Litigation, 66 F.Supp.3d 1197, 1211-17 (N.D. Cal. 2014); In re Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F. Supp.2d 942, 956-63 (S.D.Cal.2014); Moyer, 2014 WL 3511500, at *5-6.

102) Strautins v. Trustware Holdings, Inc., 27 F.Supp.3d 871, 875-79 (N.D. Ill. 2014); In re Barnes & Noble Pin Pad Litig., 2013 WL 4759588, at *3 (N.D. Ill. Sept. 3, 2013). *See, generally,* Miles L. Galbraith, *Identity Crisis: Seeking a Unified Approach to Plaintiff Standing for Data Security Breaches of Sensitive Personal Information*, 62 Am. U. L. Rev. 1365 (2013).

103) Spokeo v. Robins, 135 S.Ct. 1892 (2015), http://sblog.s3.amazonaws.com/wp-content/uploads/2014/05/13-1339-Spokeo-v-Robins-Cert-Petition-for-filing.pdf.

104) Robins v. Spokeo, 742 F.3d 409 (9th Cir. 2014).

105) The Court's grant of *certiorari* states that it will consider "Whether Congress may confer Article III standing upon a plaintiff who suffers no concrete harm, and who therefore could not otherwise invoke the jurisdiction of a federal court, by authorizing a private right of action based on a bare violation of a federal statute." *See* Spokeo, 135 S.Ct. 1892 (2015), http://sblog.s3.amazonaws.com/wp-content/uploads/2014/05/13-1339-Spokeo-v-Robins-Cert-Petition-for-filing.pdf.

Damages

While alleging a legal 'injury' satisfies the standing requirement, a viable claim also involves alleging and proving legally recoverable damages. When the plaintiff has suffered a clear economic injury from misuse of the information, for example, unauthorized credit card charges, there should be no difficulty satisfying this requirement.[106] When injuries involve only a threat of future harm, US jurisprudence will likely be hostile to the damage claims.

Thus, in *Ruiz v. Gap, Inc.*, the Ninth Circuit held that the threat of future harm from an identity theft is, alone, insufficient to establish damages under California's negligence and contract law.[107] The Seventh Circuit, in *Pisciotta v. Old National Bankcorp*, which, as earlier described, had accepted the risk of future injury for standing, concluded that this risk, alone, is insufficient to support damages.[108] In a putative class action involving data disclosure, *In re Sony Gaming Networks*, a California federal district court recognized that some cases had allowed disclosure victims to recover expenses for credit monitoring services by drawing an analogy to medical monitoring costs. However, the court held that the *Sony* plaintiff failed to meet this "high burden" of proof because he had not alleged any actual identity theft resulting from the intrusion.[109]

Instead of damages, a plaintiff could seek injunctive relief, arguing that

---

106) *See* Anderson v. Hannaford Bros. Co., 659 F.3d 151, 154, 162-66 (unauthorized charges).

107) Ruiz v. Gap, Inc., 380 F. App'x 689, 691-92. The court did not determine whether time and money spent on credit monitoring were recoverable, because the plaintiff failed to offer evidence on those claims and on whether the defendant would voluntarily reimburse him.

108) Pisciotta, 499 F.3d at 639-40 (applying Indiana law).

109) In re Sony Gaming Networks, 996 F.Supp. 942, 970. *Accord*, Moyer, 2014 WL 3511500, at * 7 ("Illinois courts have rejected the argument that an elevated risk of identity theft constitutes actual damage for purposes of stating common law or statutory claims[;] … Moyer's purchase of credit monitoring protection also falls short of constituting an economic injury under Illinois law."). Plaintiffs' negligence claims must also address the economic loss doctrine which usually bars the recovery of economic losses in tort cases, where there is not a personal injury or property damage. *See* In re Michaels Stores Pin Pad Litig., 830 F. Supp. 2d 518, 529-31 (N.D. Ill. 2011) (economic loss rule required dismissal of negligence claim for identity theft because no alleged personal injury or property damage).

damages are an inadequate remedy because it is difficult to value the loss of private information. Considering the risk of future data misuse, a court might be willing to order that the defendant provide credit monitoring for the plaintiff.

Causation

Related to the injury/damages hurdle is the 'causation' requirement. Plaintiffs must demonstrate "a nexus between the two instances [disclosure and damages] beyond allegations of time and sequence."[110] The Ninth Circuit found a sufficient causal relationship for a claim to proceed to trial where (1) the plaintiff gave the defendant his personal information; (2) the identity fraud incidents began six weeks after hard drives containing customers' personal information were stolen from the defendant; (3) the plaintiff had not previously suffered similar incidents of identity theft; and (4) the jury could infer that the type of information stolen was the same type needed to open fraudulent accounts.[111] As the time between the information disclosure and its alleged misuse lengthens, causation becomes harder to prove, but the temporal connection is only one factor. The Eleventh Circuit permitted a claim to proceed where the time gap was ten and fourteen months because there was a "*logical* relationship between the two events."[112]

3. The Remedies – A Comparison

There are more differences than similarities between Korean and US remedies in personal information disclosure cases. Korean courts have relied on Article 751 of the Civil Act to award 'consolation money' even when there was no economic damage. US law is generally less willing to allow similar mental anguish damages, absent some physical injury or intentional conduct by the defendant, and courts seem to be following this

110) Resnick v. AvMed, Inc., 693 F.3d 1317, 1327.

111) Stollenwerk v. Tri-West Health Care Alliance, 254 Fed.Appx. 664, 667-68 (9th Cir. 2007).

112) *Id.* at 668 (emphasis included).

approach in information disclosure cases. US courts have allowed economic damages when the misuse of information has caused unauthorized credit card charges, bank withdrawals, and similar direct economic losses. When the evidence shows that there was an intentional breach, designed to steal and misuse the information, more courts may come to accept that this creates a sufficient risk to support damages for credit monitoring and other preventive acts. However, damages will probably remain unavailable when the risk is speculative, for example, when there has been an information breach for unclear reasons and the breach may or may not have disclosed the plaintiff's personal information.

Korea and the United States are even farther apart on the 'standing' requirement. Currently, US courts often require the plaintiffs to plead an injury that is "certainly impending." Otherwise, they have no chance to develop their claims through discovery and, perhaps, pressure the defendant to settle. Korean courts have permitted these lawsuits to proceed even when the plaintiff alleges only a possible injury. This Korean approach allows the plaintiffs to at least litigate their claims, giving them a tactical advantage over US claimants.

Another distinction is that Korean courts determine mental damage by considering not only the plaintiff's suffering but various aspects of the defendant's misbehavior. In US jurisprudence, the defendant's misbehavior is only occasionally relevant when calculating actual damages. For example, actual damages in claims for an intentional infliction of emotional distress, assault, and defamation depend, in part, on how badly the defendant behaved. Here, the defendant's misbehavior is considered to better assess the plaintiff's injury. But, Korean courts go further when awarding consolation money. They have considered such factors as the ITSP's security level, methods for managing personal information, and profit from storing and processing the information. These factors seem independent of the plaintiff's actual damages, and, in US jurisprudence, would be considered in assessing punitive damages. Some scholars have argued that Korean consolation money is not for compensation, but functions as a punitive damage. Notably, a recent amendment to PIPA adds a punitive damage claim, allowing courts to award as much as treble damages when the personal information is lost, stolen, leaked, forged, or

falsified with intent or gross negligence (effective 25 July 2016).[113] With this new provision, Korean courts may come to rely less on consolation money to address the defendant's misbehavior.

VI. Conclusions and Suggestions

Civil litigation over personal information disclosures is rapidly growing, and, because it often involves millions of victims, its economic and social impacts will be among the most significant addressed by Korean and US jurisprudence. Liberal standards for liability and remedies seem appropriate, given that the plaintiffs are practically helpless to protect against the disclosures and must depend on the ITSP. Notification to the victim is a weak remedy, since it places the entire burden of repair on the victim and does not encourage companies to better protect information. However, if standards for liability and damages are too liberal, ITSPs may find it financially impossible to do business online and, perhaps, even to have digital records. On-line commerce will be inhibited and companies ruined, even if there is no significant damage to information owners.

Some steps can be taken to reduce these problems. Both jurisdictions should better define 'reasonableness' for liability and notice, and, here, courts would benefit from more administrative guidance. An administrative agency is more adroit at determining the latest, reasonable steps that a company can take to protect information. This approach would also produce a more uniform standard than that delivered by litigation. Regulatory provisions could be 'safe harbors' for companies.

A standard for required technology would consider, among other factors, the nature of the information, the state of security technology, the cost of implementing a technology, and the level of security achieved. An ITSP's information protection policies should, among things, (1) address the categories of information subject to security; (2) explain how safeguarding will be accomplished; (3) state who is responsible for various safeguarding procedures; (4) impose procedural and technical controls to

113) Personal Information Protection Act, art. 39.

ensure that only authorized individuals have access to the protected information; (5) periodically change passwords; (6) have different passwords for different persons and information storage systems; (7) ensure that the physical facilities and mobile devices are secured, inventoried, and tracked; (8) use encryption which is at least the industry standard; (9) train employees and discipline them for security failures; (10) monitor, record, and respond to intrusions, viruses, and other malware; (11) create policies to destroy information which is no longer current or needed; (12) periodically test and update all security procedures, hardware, and software; (13) establish procedures for notifying affected persons and government regulators; and (14) establish procedures for reacting to information breaches. These standards should consider industry practices, requirements imposed by foreign jurisdictions, local and international model codes, and input from stakeholders. Different standards may be appropriate for protecting information which the plaintiff voluntarily released (e.g., on Facebook) versus information provided as a necessity (e.g., to conduct banking).[114)]

Legislation could also assist with uncertainty over damages. Other jurisdictions might mimic the California notice statute and require that victims receive a free credit monitoring service for a certain time after the disclosure. This, like medical monitoring, might efficiently prevent future damages but requiring automatic monitoring every time there is a disclosure, involving millions of potential victims, could be economically inefficient and unfair to ITSPs. US courts may be too strict in their standards for recoverable damages and Korean courts too liberal. One compromise is extending statutes of limitations, so that potential victims could afford to wait to determine whether there is any actual injury.

Once more precise liability standards and damage measurements are developed, ITSPs would be encouraged to seek insurance and, in turn, insurance companies would develop specialized policies. As a condition for issuing the policies or offering lower insurance rates, the insurance companies would require companies to take steps to reduce the risk of an information breach.

---

114) Several of these suggestions are drawn from Peters, *supra* note 12, at 1194-1201, and Sloan, *supra* note 10.

Class action lawsuits may seem an attractive option, given the victims' small damages. Korea's PIPA provides a new litigation scheme which allows consumer organizations to bring a suit for injunctive relief on behalf of the injured consumers.[115] The same procedure has been part of the general Consumer Protection Act since 2008. However, it is questionable how much benefit injunctive relief will be in information disclosure cases. The United States allows the victims to bring class actions, but these have sometimes been poor mechanisms for providing remedies. For example, an information broker, ChoicePoint, paid ten million dollars to settle a consumer class action for an information breach, which came to approximately $61.35 per disclosed record.[116] Compare this recovery to the estimated average cost to a victim of an unauthorized information disclosure: $631 and 33 hours trying to address identity theft.[117]

Given these hurdles to a fair resolution of information disclosure claims, both Korea and the United States should invest more in developing approaches to alternative dispute resolution (ADR). Korea's PIPA provides its own mediation mechanism. Any party, either a consumer or company, can apply for mediation by a "personal information mediation committee" to resolve an information disclosure claim. The mediation's result has the same effect as a final court judgment. A special form of this mechanism is "class mediation," where parties can ask for the collective resolution of claims asserted by all similarly situated people. Potential plaintiffs should consider this alternative which resolves matters much quicker than does litigation. For example, after several months of mediation, 5,747 Auction users received consolation money of one hundred thousand won each in 2008.[118] Auction users who pursued litigation did not receive anything with

---

115) Personal Information Protection Act, art. 51.

116) Federal Trade Commission, *ChoicePoint Settles Data Security Breach Charges*, Jan. 26, 2006, https://www.ftc.gov/news-events/press-releases/2006/01/choicepoint-settles-data-security-breach-charges-pay-10-million.

117) Justine Rivero, *Three New Ways to Protect Your Identity in 2012*, Forbes, Jan. 3, 2012, http:// www.forbes.com/sites/moneywisewomen/2012/01/03/three-new-ways-to-protectyour-identity-in-2012/.

118) Press Release, Hangugsobijawon [Korea Consumer Agency], Sobijabunjaengjojeongwiwonhoe, SKBroadband (Gu. Hanalotellekom)ui gaeinjeongbomudaniyong haengwi, Ogsyeonui gaeinjeongboyuchule daehae chaegim muleo [*Consumer Disputes Mediation Committee held SK Broadband and Auction Liable for Personal Data*

the final judgment, rendered in 2015.

Our society and economy are very different from that even twenty years ago, primarily because of the increased use of and dependency on Internet and telecommunication services. This technology is developing exponentially while the law is changing slowly. However, this is not the first time jurisprudence has grappled with evolving technology. The tools are there; courts and legislatures should develop the law to reach an appropriate balance between the use of this technology and the protection of personal information.

Breach] (Dec. 5, 2015), http://kca.go.kr/brd/m_32/view.do?seq=902&srchFr=&srchTo=&srchWord=옥션&srchTp=0&itm_seq_1=0&itm_seq_2=0&multi_itm_seq=0&company_cd=&company_nm=&pitem=10&page=1.