I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

Privacy of Personal Information in the Financial Services Sectors of the United States and Japan: The Gramm-Leach-Bliley Act and the Financial Services Agency Guidelines

RYAN L. WAGGONER*

Abstract: This is a comparative analysis of the laws governing the disclosure of personal information held by financial institutions in the United States and Japan. Both nations have laws that aim to ensure that the personally identifiable information handled by financial institutions is treated in a secure fashion. However, the methods and structure of the laws differ. First, the U.S. privacy structure is generally sector-specific, whereas Japan has created an overarching law that government agencies use to create additional sector-specific guidelines. Second, the scope of the laws are different due to variance in: (1) which financial institutions are accountable under the applicable law; (2) whose information the applicable law protects; and (3) what types of data the laws regulate. Third, the laws have very different approaches to the notification provisions and privacy policies. Lastly, the U.S. and Japanese laws have similar opt-out provisions, but Japan places many more restrictions on the movement of personal information. Nonetheless, the laws of both countries provide individuals the assurance that financial institutions will securely handle their personal information.

* Ryan L. Waggoner is a Juris Doctor candidate in the class of 2010 at The Ohio State University Moritz College of Law and a Master of Arts candidate in East Asian Studies with a specialization in Japanese law. He received a Bachelor of Arts in History and Japanese from The Ohio State University in 2006.

I. INTRODUCTION

Japan and the United States are among the many nations that have enacted legislation to deal with the privacy of personal data in the possession of financial institutions. Although the American and Japanese approaches differ, both countries aim to accomplish the same goal: to help ensure that consumers' personally identifiable information handled by financial institutions is treated in a secure fashion. Title V of the Gramm-Leach-Bliley Act,[1] also known as the Financial Services Modernization Act, serves this function in the United States. Similarly, Japan's guidelines on the protection of personal information, which are based upon the Act on the Protection of Personal Information,[2] do so in Japan. Both of these legal structures have a data-privacy element and a data-security element. This note analyzes only the data-privacy element of the countries' laws.[3]

The first section of this note provides a brief explanation of the privacy law structures in the United States and Japan in a global and national comparative context. The second section compares the scope of coverage of the two laws: what types of information, whose information, and what data-handling entities the laws cover. The third section discusses the laws' notice requirements that govern financial institutions' privacy policies vis-à-vis disclosures of personal information. The fourth section highlights the differences between the countries regarding the consent required from those whose personal data is held by financial institutions and the access that individuals have over their personally identifiable information held by financial institutions. Additionally, the fourth section covers the laws'

---

[1] Gramm-Leach-Bliley (Financial Services Modernization) Act, Pub. L. No. 106-102, 113 Stat. 1338 (2006) (codified as amended in 29 U.S.C. § 2903 and scattered sections of 12 U.S.C., 15 U.S.C., 16 U.S.C., and 18 U.S.C.).

[2] Kojin jyōhō no hogo ni kansuru hōritsu [Act on the Protection of Personal Information], Law No. 57 of 2003, *available at* http://www5.cao.go.jp/seikatsu/kojin/houritsu/050815houan.pdf. The English translation is *available at* http://www5.cao.go.jp/seikatsu/kojin/foreign/act.pdf.

[3] Notice on translation: The names of Japanese documents provided in English literature are not consistent. This note uses the terms of the English translation of the laws and guidelines provided by the Cabinet Office of Japan or the pertinent ministry; if no official translation is available, the author's own translation is provided, which is indicated. If there is no location provided for an English version of a Japanese document, there is not an official translation available.

provisions dealing with an individual's option to opt-out of the transmission of personal information to third parties.

II. COMPARATIVE PERSPECTIVES: FINANCIAL SERVICES PRIVACY IN THE UNITED STATES AND JAPAN

The current global trend in privacy law is the creation of omnibus legislation that applies baseline protection to all types of personally identifiable information, whether in business or government.[4] The most notable example—and the yardstick by which many new privacy structures are measured—is the European Union Data Protection Directive.[5] The Directive sets a minimum standard for data privacy of all personal data throughout the European Union, regardless of business context or industry. The Directive regulates the use of personal information through rules regarding consent, disclosure, and maintenance of personal data,[6] with each E.U. country implementing additional data security provisions that it deems appropriate.[7] Many countries, such as Canada,[8] have used the E.U. Directive as a model for their own omnibus privacy law.

The United States has taken the opposite approach. The U.S. privacy structure is generally sector-specific; federal law only covers certain types of personal information deemed especially sensitive or important enough to create a national standard. Data not under federal jurisdiction is either left alone or regulated by market pressures, self-regulation, or state laws.

---

[4] Ruth Hill Bro, *Across the Pond: Recent Developments in EU Data Protection Laws, Regulation and Enforcement*, 934 PLI/PAT 681, 690–91 (June–July 2008).

[5] Council Directive 95/46/EC, 1995 O.J. (L 281) 1, *available at* http://www.cdt.org/privacy/eudirective/EU_Directive_.html.

[6] The transfer of personal data outside of the European Union is limited to countries that have received a rating of "adequate" by the E.U. Privacy Commission. Neither Japan nor the United States have received this rating. U.S. businesses are only able to receive data flows of personal information from the European Union through the International Safe Harbor Privacy Principles program. *See generally* U.S. Dep't of Com. & Eur. Comm'n, Safe Harbor Privacy Principles Program, http://www.export.gov/safeHarbor.

[7] *See* Wildman Harrold, *The Emerging Law of Data Security: A Focus on Key Legal Trends*, 934 PLI/PAT 13, 82–85 (June–July 2008).

[8] Personal Information Protection and Electronic Documents Act, 2000 S.C., ch. 5 (Can.), *available at* http://www.parl.gc.ca/PDF/36/2/parlbus/chambus/house/bills/government/C-6_4.pdf.

Japan has taken a middle-of-the-road approach. The Act on the Protection of Personal Information ("APPI") [9] outlines general requirements and obligations of personal-information-handling entities, but the APPI requires various government ministries to enact the details of regulation and enforcement processes through a series of guidelines pertinent to the sectors under the ministries' purview. Therefore, the European Union and the United States form the endpoints on a global data privacy law spectrum—one side is a nationwide, baseline regulatory scheme underscored with broad ideals (E.U.), and the other is a patchwork covering specific types of personal data with strict regulation (U.S.)—and Japan lies somewhere in the middle.

A. U.S. FINANCIAL SERVICES: GRAMM-LEACH-BLILEY ACT

Congress enacted the major U.S. privacy laws after significant events displayed the need for some type of Federal privacy protection. For instance, the first major privacy law in the United States, the Privacy Act of 1974,[10] was enacted after the scandals of the Nixon administration. Another example is the Video Privacy Protection Act ("VPPA"),[11] which was passed in 1988 after Robert Bork, a Supreme Court nominee, had his video rental history published during the nomination hearings. Title V of the Gramm-Leach-Bliley Act ("GLBA")[12] is no different. Just before the GLBA's passage, the Federal Trade Commission and a number of state attorneys general took action against several major financial institutions that were selling customer information, including account numbers and other sensitive information, to telemarketing firms. The firms were using the account numbers to charge customers for additional, unwanted services.[13] Congress responded by including the privacy and security protections of the GLBA.

---

[9] Act on the Protection of Personal Information, Law No. 57 of 2003, *supra* note 2.

[10] Privacy Act of 1974, 5 U.S.C. § 552a (2006).

[11] Video Privacy Protection Act of 1988, 18 U.S.C. § 2710 (2006).

[12] 15 U.S.C. §§ 6801–6809, 6821–6827 (2006).

[13] PETER P. SWIRE & SOL BERMANN, INFORMATION PRIVACY: OFFICIAL REFERENCE FOR THE CERTIFIED INFORMATION PRIVACY PROFESSIONAL 40 (Peter Kosmala ed., International Association of Privacy Professionals 2007).

Title V of the GLBA consists of Subtitle A, Disclosure of Nonpublic Personal Information,[14] and Subtitle B, Fraudulent Access to Financial Information.[15] There are three components to Title V: the Financial Privacy Rule ("Privacy Rule"), the Safeguards Rule, and pretexting. The Privacy Rule is found in the entirety of Subtitle A, except for 15 U.S.C. § 6801(b), which is the Safeguards Rule. Generally, the Privacy Rule governs the collection and disclosure of customers' personal information held by financial institutions. The Safeguards Rule requires financial institutions to create, implement, and maintain safeguards to protect customer information held by the financial institutions. Pretexting, commonly referred to as "social engineering," (e.g., phishing, spear phishing) is the act of using false pretenses to obtain customer information. Subtitle B specifies controls to safeguard customer information from pretexting, defines enforcement agencies, and outlines penalties.[16] Because this note covers the data-privacy aspect of the GLBA, it analyzes only the Privacy Rule. The security-oriented Safeguards Rule and the pretexting rules of Subtitle B are outside the scope of this note.[17]

B. JAPANESE FINANCIAL SERVICES: APPI; FINANCIAL SERVICES AGENCY GUIDELINES; AND MINISTRY OF ECONOMY, TRADE, AND INDUSTRY GUIDELINES

Much like the Privacy Rule in the GLBA, the APPI was promulgated in response to the nation-wide fear of identity theft. As stated in the *Cabinet's Basic Policy Concerning the Protection of Personal Information* ("*Basic Policy*"), [18] "large-scale leaks of

---

[14] 15 U.S.C. §§ 6801–6809.

[15] 15 U.S.C. §§6821–6827.

[16] See the Federal Trade Commission ("FTC") Privacy Initiatives website for more information about the FTC's rules and regulations regarding the GLBA and additional information on the three components of Title V, which is available at http://www.ftc.gov/privacy/index.html.

[17] See the FTC website for a wide range of information on the Safeguards Rule, which is available at http://www.ftc.gov/privacy/privacyinitiatives/safeguards.html. The FTC discussion of pretexting is available at http://www.ftc.gov/privacy/privacyinitiatives/pretexting.html.

[18] Kojin jyōhō no hogo ni kansuru kihon hōsin [Basic Policy Concerning the Protection of Personal Information] (Cabinet decision, April 2, 2004, amended May 25, 2008), *available at* http://www5.cao.go.jp/seikatsu/kojin/kakugi2008.pdf. An unofficial English

customer information from businesses, and the repeated incidents of this information being sold is becoming a social problem. Moreover, public anxiety over privacy is rising, as well as demands for business to start securely managing personal information."[19] However, the *Basic Policy* also states that the use of telecommunications technology and personal data is necessary for businesses to function.[20] The law establishes a minimum threshold for the handling of personal information. These rules are common to all sectors handling sensitive information, and they target businesses with the expectation that each business will independently secure its personal information according to the conditions in its respective business sector.[21]

The APPI is loosely based on the eight privacy principles of the Organization for Economic Cooperation and Development ("OECD"), [22] but the law departs from both the U.S. and E.U. regulatory schemes for data privacy. The departure arises from the fact that the Japanese approach is a hybrid of an overarching regulatory framework, individual sector guidelines, and private sector self-regulation. In other words, the APPI is the principal regulation for a series of policies, guidelines, decisions, and ordinances promulgated by various entities in the Japanese government to regulate the collection, retention, and use of personal information. However, for businesses, the ministry guidelines (in conjunction with the APPI) are most important. Some guidelines are more significant than others, affecting all business in Japan, such as the guidelines regulating employment or the transmission of data. Moreover, some ministries have overlapping authority, such that businesses must reconcile several ministry ordinances. As of January 1, 2009, there are thirty-seven sector-specific guidelines promulgated by fourteen

---

version, provided by Morrison & Foerster, is available at http://www.mofo.com/docs/mofoprivacy/Basic%20Policy.pdf.

[19] *Id.* at art. 1, no. 1 [author's translation].

[20] *Id.* at art. 1, no. 2(1).

[21] *Id.* at art. 2, no. 3(1) [author's translation].

[22] The eight principles are: (1) Collection Limitation Principle; (2) Data Quality Principle; (3) Purpose Specification Principle; (4) Use Limitation Principle; (5) Security Safeguards Principle; (6) Openness Principle; (7) Individual Participation Principle; and (8) Accountability Principle. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html (last visited Jan. 2, 2009).

ministries, which regulate twenty-four sectors in the Japanese economy.[23]

Four of these guidelines regulate the use of customers' personal information in the financial services sector. The first and most general of the guidelines is the *Guidelines for Personal Information Protection in the Financial Field* ("FSA Guideline"), which was created by the Financial Services Agency ("FSA").[24] The FSA also published *Practical Principles Regarding the Guidelines on Measures for Secure Management for Personal Data Protection in the Financial Sector* ("FSA Security Guideline"), which covers the security processes, measures, and systems that financial institutions must implement and maintain.[25] These processes are very specific and cover a wide-range of measures, including employee data-handling responsibilities, technological systems, incident and maintenance reports, mandatory and regularly performed audits and examinations, and the appointment of information officers.

The Ministry of Economy, Trade, and Industry ("METI") developed the other two guidelines regulating the use of customers' personal information. The guidelines that directly regulate information available to the financial services sector through credit information are the *Guidelines for the Protection of Personal Information in Credit Sector among Industrial Sectors* ("METI Credit Guidelines").[26] The METI Credit Guidelines are derived from METI's primary guidelines, *Guidelines Targeting Economic and Industrial Sectors Pertaining to the Act on the Protection of Personal*

---

[23] *See* Kojin jyōhō no hogo ni kansuru gaidorain ni tsuite: Jigyō bunya goto no gaidorain ichiran [About Guidelines on the Protection of Personal Information: Industry Sector Guideline Summary], http://www5.cao.go.jp/seikatsu/kojin/gaidorainkentou.html [Japanese language only].

[24] Kinyū bunya ni okeru kojin jyōhō hogo ni kansuru gaidorain [Guidelines for Personal Information Protecting in the Financial Field], http://www.fsa.go.jp/common/law/kj-hogo/01.pdf. The English translation is available at http://www.fsa.go.jp/frtc/kenkyu/event/20070424_02.pdf.

[25] Kinyū bunya ni okeru kojin jyōhō hogo ni kansuru gaidorain no anzen kanri sochi nado ni tsuite no jitsumu shishin [Practical Principles Regarding the Guidelines on Measures for Secure Management for Personal Data Protection in the Financial Sector (author's translation)], http://www.fsa.go.jp/common/law/kj-hogo/04.pdf [Japanese language only].

[26] Keizai sangyō bunya no uchi shinyō bunya ni okeru kojin jyōhō hogo ni kansuru gaidorain [Guidelines for the Protection of Personal Information in Credit Sector among Industrial Sectors], http://www.meti.go.jp/feedback/downloadfiles/i41202ij.pdf [Japanese language only].

Information ("METI Primary Guidelines"), which affect the financial services sector through the provisions adopted by the METI Credit Guidelines.[27]

METI has overlapping authority with the FSA over credit because secondary fraudulent charges often occur after pertinent credit card information is leaked. Entities that are not financial institutions under the scope of coverage of the FSA, but are businesses that qualify as credit card processors—like credit reporting agencies—must follow the METI security measures for credit cards. The METI Primary Guidelines also allow credit card companies to follow the METI case examples in the METI guidelines if they are regulated by the FSA Guidelines and are affected by rules in the METI Credit Guidelines.[28] However, because this note covers only the privacy aspect of these laws, the security portions of the APPI, of the FSA guideline, and of both METI guidelines, as well as the entirety of the FSA security guidelines, are outside the note's scope.[29]

The next three sections of this note analyze the following comparative privacy elements: (1) the scope of coverage of the U.S. and Japanese financial services data privacy laws; (2) the notice to customers required by the laws; and (3) the need for customers' consent, whether customers can request access to their personal information, and the opt-out processes for data transfer to third parties. Although the note separates into distinct categories the laws' ambit, notice, consent, and opt-out options, in practice they are often inseparable in the use of personal information.

---

[27] Kojin jyōhō no hogo ni kansuru hōritsu ni tsuite no keizai sangyō bunya o taisyō to suru gaidorain [Guidelines Targeting Economic and Industrial Sectors Pertaining to the Act on the Protection of Personal Information], http://www.meti.go.jp/policy/it_policy/privacy/041012_hontai.pdf. The English translation is available at http://www.meti.go.jp/policy/it_policy/privacy/0708english.pdf.

[28] *Id.* at annex. METI case examples are referenced in the METI Credit Guidelines.

[29] For clarification, broadly speaking, the security requirements given by the APPI and the FSA security guidelines are generally the same as those of the Safeguards Rule, Subtitle B of Title V, and 16 C.F.R. § 314.1–.5. Both sets of regulations require financial institutions to develop a security program and identify, evaluate, and defend against possible risks and threats. Each set of laws also govern the enforcement of the laws and appropriate penalties. The major difference is that the FSA security guideline offers long, specific instructions on the implementation of a security program, the appointment of several different data-handling officials, how and who should handle audits and examinations of the data-handling practices of financial institutions, and the appropriate measures to be taken in case of a leakage of personal information.

III. SCOPE OF COVERAGE OF U.S. AND JAPANESE FINANCIAL SERVICES DATA PRIVACY LAWS

There are three issues that underlie any data privacy law: (1) which entities are accountable under the law, (2) whose data it regulates, and (3) what type of data it regulates. This section will discuss each of the three questions in turn.

A. DATA-HANDLING ENTITIES

The data-handling entities regulated by the laws are generally the same institutions in both countries. In the United States, "financial institutions" are the regulated entities. The GLBA defines "financial institution" as "any institution the business of which is engaging in financial activities as described in section 1843(k) of Title 12 [the Bank Holding Act]."[30] This is a broad definition that includes lending, exchanging, transferring, investing for others, or safeguarding money or securities; providing any device or other instrumentality for transferring money or other financial assets; and arranging, effecting, or facilitating financial transactions for the account of third parties.[31] This also includes activities that the Federal Reserve Board has deemed "so closely related to banking or managing or controlling banks as to be a proper incident thereto."[32]

Examples of this activity are extending credit and servicing loans, offering credit bureau services, leasing personal or real property, and selling financial and investment advice. [33] The Federal Trade Commission ("FTC")—unlike the other regulatory agencies in the financial services sector[34]—has adopted a definition of "financial institution" that only includes institutions that are "significantly engaged" in financial activities.[35] This flexible standard was put in

---

[30] 15 U.S.C. § 6809(3)(A).

[31] 12 U.S.C. § 1843(k).

[32] 12 C.F.R. § 225.28(a) (2008).

[33] *Id. at* § 225.28(b).

[34] The other regulatory agencies are: Federal Deposit Insurance Corporation ("FDIC"), Commodity Futures Trading Commission ("CFTC"), Federal Reserve Board, National Credit Union Administration ("NCUA"), Office of Comptroller of the Currency ("OCC"), Office of Thrift Supervision ("OTC") and Securities and Exchange Commission ("SEC").

[35] 16 C.F.R. § 313.3(k)(1) (2008).

place to exclude certain activities that might otherwise fall under the Privacy Rule by taking into account all the facts and circumstances. The two factors that are important in determining whether an institution is "significantly engaged" in financial activities are: (1) whether there is a formal arrangement; and (2) the number of instances that the business engages in financial activity. Therefore, a retailer that only accepts credit cards for payment is not a "financial institution," but a retailer that issues its own credit card is "significantly engaged" and therefore does qualify as a "financial institution."[36]

In Japan, because the FSA Guideline and METI Credit Guidelines are based upon the APPI, each has the same definition of "financial institution." The APPI applies to "entities handling personal information," which are entities that use a personal information database[37] as part of its normal operation,[38] with the exception of (1) national institutions, (2) local public bodies, (3) independent administrative agencies subject to another statute regulating their collections and use of personal information, and (4) any entity specified by a Cabinet order as presenting a minimal likelihood of harming the rights and interests of individuals based on the volume of personal information at issue and the method by which it uses personal information.[39] Moreover, any entity that has not handled the personal information of more than 5000 individuals at any time in the previous six months is also exempted from this law.[40]

The caveat to the above referenced exceptions is found in the METI Guidelines, which provide that businesses that have the

---

[36] FED. TRADE COMM'N, HOW TO COMPLY WITH THE PRIVACY OF CONSUMER FIN. INFO. RULE OF THE GRAMM-LEACH-BLILEY ACT 2–3 (2002), http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus67.pdf.

[37] "Personal information database" is defined as a set of information systematically arranged in such a way that specific personal information can be retrieved by an electronic computer; or a set of information designated by a Cabinet order as being systematically arranged in such a way that specific personal information can be easily retrieved. Act on the Protection of Personal Information, Law No. 57 of 2003, *supra* note 2.

[38] *Id.* at art. 2, no. 3.

[39] *Id.*

[40] Kojin jyōhō no hogo ni kansuru hōritsu sekōrei [Cabinet Order for the enforcement of the Act on the Protection of Personal Information], Cabinet order No. 507 of 2003, art. 2, http://www5.cao.go.jp/seikatsu/kojin/houritsu/seireiindex.html. The English translation is available at http://www5.cao.go.jp/seikatsu/kojin/foreign/cabinet-order.pdf.

information of less than 5000 individuals in their database at any one time in a six-month period must still comply with the credit card security measures if the business takes credit card based payments.[41] When evaluating whether an entity falls under the purview of the APPI, the entity must account for all of the individuals in its database, including customers, staff, related companies, and business associates.[42] However, names, phone numbers, and addresses derived from commercial directories, navigational systems, and commercially available maps do not count toward the total number.[43]

B. WHOSE DATA IS REGULATED

The question of whose data is regulated differs substantially between the U.S. and Japanese methods of privacy protection. According to the GLBA, a financial institution's obligation depends on whether the personal information is that of a "customer" or a "consumer." The term "consumer" does not apply to commercial clients, but is defined narrowly as an "individual who obtains, from a financial institution, financial products or services which are to be used primarily for personal, family, or household purposes, and also means the legal representative of such an individual."[44] Therefore, if a client is not an individual or is an individual seeking services for a business purpose, the client is not a consumer, and the Privacy Rule does not apply.

The details of what constitutes a "customer" are not specified in the GLBA but "shall be defined by the regulations prescribed under Section 6804"[45] of the GLBA, which gives regulators of the financial services sector authority to define "customer."[46] However, regulators

---

[41] Guidelines Targeting Economic and Industrial Sectors Pertaining to the Act on the Protection of Personal Information, *supra* note 27, at art. 2-1-3.

[42] *Id.*

[43] *Id.* Also see METI's educational video for companies on the basics of APPI compliance, which is available at http://www.meti.go.jp/policy/it_policy/privacy/#11. In this author's opinion, the production value and acting is on par with an average Japanese television drama. The best part is when the supervisor is thunderstruck when he finds out his company must abide by the law after telling his workers their company is too small to be affected by it.

[44] 15 U.S.C. § 6809(9).

[45] *Id.* at § 6809(11).

[46] 15 U.S.C. § 6804(a)(1)–(2).

all use the same definition: a "customer," a subclass of "consumer," is one who has a continuing relationship with a financial institution.[47] For customers, it is the nature of a relationship that matters, not how long the relationship lasts. For example, if an individual uses a bank's ATM on a regular basis but does not have an account, that person is only a consumer. If the individual has an account and uses the ATM, then the individual is a customer. Moreover, former customers become consumers.

Unlike the GLBA, the APPI does not identify whose data the law covers. The APPI is a law concerned with the proper handling of personal information, not the protection of individual privacy. Indeed, there was careful consideration given to making the APPI *not* about privacy. Privacy in Japan is social etiquette, not an inherent right. The purpose of the APPI is just as much to police companies' manners regarding personal information as avoiding fraud.[48]

A comparison of the purposes of each law reveals a major difference between the privacy laws of the United States and Japan. The GLBA states that "[i]t is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information."[49] On the other hand, the basic philosophy of the APPI, stated in article three, says, "in view of the fact personal information should be handled cautiously under the philosophy of respecting the personalities of individuals, proper handling of personal information must be promoted."[50] The APPI subjugates the protection of individuals to the secure handling of personal information. In conjunction with the following section, this leads to the conclusion that the APPI relies more upon the definition of "data" to determine what data the law protects. Unlike the GLBA, which protects data according to its owner, the APPI's purpose is to protect the information itself, and the identity of the owner is not important.

---

[47] 12 C.F.R. §§ 40.3(h)–(i), 216.3(h)–(i), 313.3(h)–(i), 332.3(h)–(i), 573.3(h)–(i), 716.3(i)–(j) (2008); 17 C.F.R. §§ 160.3(h)(1), 248.3(k)(1) (2008).

[48] Yukiko Ko, *Japan at the Critical Juncture of Data Protection: Personal Information Protection Act and its Guidelines Under Review*, 5 PRIVACY & SECURITY LAW 1747 (2006).

[49] 15 U.S.C. § 6801(a).

[50] Act on the Protection of Personal Information, Law No. 57 of 2003, *supra* note 2, at art. 3.

C. TYPES OF DATA

Because the APPI relies upon its definition of "data" to identify whom the law protects, it should come as no surprise that the APPI utilizes several different definitions of "personal information" to flesh out what exactly it protects. "Personal information" is "information about a living individual which can identify the specific individual by name, date of birth, or other description contained in such information."[51] This also includes information that can allow easy reference to other personal information, such as car navigation records, occupation and title, and all other information that represents facts, judgments, and assessments about an individual.[52] The FSA Guideline further defines "personal information" by creating a category called "sensitive information." This is information that an "entity handling personal information in the financial field shall not acquire, use, or provide to third party [sic], information on political views, religion (meaning thoughts and creed), participation in union activities, race, family origin and registered domicile, health care, sex life, and past criminal record."[53] Thus, in the financial services sector, aside from several exceptional cases, "personal information" only includes non-sensitive information.

The GLBA's term for personal information, which the financial services sector regulators adopted, is "nonpublic personal information." This is personally identifiable financial information that is provided by a consumer to a financial institution through any type of transaction, or otherwise obtained by a financial institution.[54] "Nonpublic personal information" includes any list, description, or other grouping of consumers—and any publicly available information pertaining to them—that is derived using any nonpublic personal information other than publicly available information.[55]

The questions of which entities are covered by the data privacy laws, whose personal information the entities are responsible for, and

---

[51] *Id.* at art. 2, no. 1.

[52] *See* Guidelines Targeting Economic and Industrial Sectors Pertaining to the Act on the Protection of Personal Information, *supra* note 27, at art. 2-1-1.

[53] Guidelines for Personal Information Protecting in the Financial Field, *supra* note 24, at art. 6, no. 1.

[54] 15 U.S.C. § 6809(4).

[55] *Id.* at § 6809(4)(C).

what constitutes personal information in the U.S. and Japanese financial services sectors reveal the differing frameworks of the two privacy regimes. The Privacy Rule of the GLBA is "entity-centric," while the APPI and FSA Guideline are "data-centric." In other words, the GLBA protects personal information in the financial services sector because of an individual's relationship with a financial institution. The APPI and FSA Guideline, on the other hand, protect personal information because of the inherent characteristics of the personal information itself, and the protection of an individual's privacy is merely a beneficial outcome.

IV. NOTICE PROVISIONS AND PRIVACY POLICY

Notice and disclosure are pillars of information privacy in the financial services sector. Financial institutions acquire, use, and share personal information for a variety of reasons, including accounting, telemarketing, and new product development. The danger in allowing financial institutions to have access to so much personal information is that they could surreptitiously use that information in disagreeable ways. For example, financial institutions could impinge on an individual's privacy or expose them to fraudulent schemes. Notice provisions aim to avoid these uses of personal information by instilling a certain level of transparency into financial institutions' use of personal information by having them inform individuals of their data handling and privacy policies. Concordantly, notice and disclosure are integral parts of the GLBA, APPI, and FSA and METI guidelines.

The GLBA mandates that a financial institution "may not, directly or through any affiliate, disclose to a nonaffiliated third party any nonpublic personal information, unless such financial institution provides or has provided to the consumer a notice."[56] Yet, the notice and disclosure rules that apply to consumers are slightly different from those that apply to customers.[57] For consumers, a financial institution must provide "notice to customers that accurately reflects [its] privacy policies and practices," at least once a year, and a notice if the financial institution revises its privacy policy or if consumers'

---

[56] 15 U.S.C. § 6802(a).

[57] *Id.* at § 6803(a). The financial regulators are given authority to define what notice and disclosure rules apply to consumers and customers even though some rules are given in Title V.

personal information is going to be transferred to a third party.[58] Customers, on the other hand, must receive an initial notice at the time the relationship is established in addition to the annual and revised privacy policy notices.[59] Still, the notices provided to both consumers and customers include the same information: the categories of nonpublic personal information that the financial institution collects and discloses; categories of affiliates and nonaffiliated third parties to whom the financial institution discloses nonpublic personal information; the categories of nonpublic personal information about former customers that the financial institution discloses; and the categories of parties to whom the nonpublic personal information is disclosed.[60] Moreover, a financial institution must provide notices "so that each consumer can reasonably be expected to receive actual notice in writing or, if the consumer agrees, electronically."[61] Lastly, the notices must be "clear and conspicuous," which means that a notice is "reasonably understandable and designed to call attention to the nature and significance of the information in the notice."[62]

Notice, according to the APPI, the FSA guidelines, and the METI Credit Guidelines, is based upon the "purpose of use" of the personal information being handled.[63] Providing an abstract purpose of use, such as "this information will be used in a purpose required by our company" is not sufficiently specific. [64] The explanation of an institution's purpose of use should allow an individual to reasonably ascertain the type of activity for which the personal information will be used. Individuals must be notified of an entity's purpose of use at the time that the individual's data is acquired. If an entity acquires the information through a written agreement or document, the entity must provide an explanation of its purpose of use in advance of

---

[58] 16 C.F.R. § 313.5(a)(1). All of the financial services sector regulators have identical regulations regarding notice and disclosure, therefore only the FTC regulations are cited.

[59] *Id.* at § 313.4(a).

[60] *Id.* at § 313.6(a)(1)–(4).

[61] *Id.* at § 313.9(a).

[62] *Id.* at § 313.3(b)(1).

[63] Act on the Protection of Personal Information, Law No. 57 of 2003, *supra* note 2, at art. 15.

[64] *Id.*

completion of the agreement. Entities also need to provide additional notice if the purpose of use changes at any time.[65] Specifically, financial sector entities must present the purpose of use after providing financial instruments or services[66] and name any third party recipients of the personal information that are involved in its purpose of use.[67] It is not sufficient to list categories.[68] Moreover, the entity must state whether laws and regulations limit the purpose of use.[69]

In the case of a financial services entity providing data to a credit bureau, the entity needs to designate in a contract the purposes of use and the limitations that apply.[70] The standard method of notification for the financial services sector is to notify an individual in writing. However, an entity may also make a "public announcement" that is easily accessible for an individual and congruent with its general manner of conducting business; for example, placing the information on its webpage, posting a notice in its office, or placing it at a service counter.[71] Lastly, any financial entity must formulate a privacy policy to clarify its views and guidelines for PI protection, publicize it, and make it readily available to those whose information the entity handles.[72]

Once again, despite having similarities, the GLBA and APPI standards differ significantly. At first glance, it seems that the GLBA's "clear and conspicuous" notice of privacy policies and the FSA Guideline's notice of purpose of usage and declaration of a privacy policy are substantially the same. However, the degree of notice demanded by the FSA Guideline actually far surpasses that of the GLBA, as well as the OECD principles and even the E.U. Directive. First, the GLBA calls for "categories of information," while the FSA

---

[65] *Id.* at art. 18, no. 1–3.

[66] Guidelines for Personal Information Protecting in the Financial Field, *supra* note 24, at art. 3, no. 1.

[67] *Id.* at art. 13, no. 1.

[68] *Id.*

[69] *Id.* at art. 3, no. 2.

[70] *Id.* at art. 3, no. 3.

[71] *Id.* at art. 23.

[72] *Id.*

Guideline necessitates a description explicit enough so that an individual can reasonably ascertain how the data handling entity will use the information. Second, the FSA Guideline requires financial institutions to include this description in conjunction with the related financial products and services, whereas there is no such requirement in the GLBA. Third, financial institutions under the GLBA do not have to announce any specific usage for the personal information, but rather just their privacy policies. In contrast, the financial institutions under the purview of the FSA Guideline must submit a privacy policy and clearly state the purpose of use. Fourth, the GLBA's bifurcation of data-subjects into "consumers" and "customers" alleviates the need for financial institutions to provide initial notice to all individuals unless the data is going to be transferred to an unaffiliated third party. The financial institutions under the FSA Guideline must provide such notice to all individuals whose personal information is acquired and used. Furthermore, the FSA Guideline requires that third parties (which include affiliates) be listed by name, while the GLBA requires only categorical listings. Finally, and most significantly, the FSA Guideline requires a notification of the purpose of use every time personal information is used for a new purpose, whereas the GLBA only requires notification of financial institutions' privacy policy once a year. Thus, in the end, there seems to be little in common between the two standards of notification except for superficial similarities.

V. CONSENT, DATA ACCESS, AND OPT-OUT OF THIRD PARTY TRANSFERS

The issues of consent and opting-out of data transfer to third parties are almost inseparable. The GLBA only requires consent from consumers when a financial institution alerts consumers to the possibility of opting-out of third party data transfers, but practically speaking, this is passive consent since the financial institution assumes that consent is given if the consumer does not reply to the opt-out notice.[73] Consent in Japan plays a role greater than opting-out of third party data transfers. This includes consent for use of the personal information, and an allowance for individuals to access their personal information that is held by entities in the financial services sector so the individuals can correct, add, or delete information from the entity's database– an option not available under the GLBA.

---

[73] 15 U.S.C. § 6802(b)(1)(B).

As previously discussed, under the GLBA, as long as a financial institution provides adequate notice of its privacy policy to consumers, it can use the nonpublic personal information without obtaining additional consent (except for third party transfers). According to the APPI (applicable provisions of which were adopted word-for-word by the FSA Guideline and METI Credit Guidelines), no entity can handle personal information in a manner beyond the scope of what is necessary for the achievement of the stated purpose of use without obtaining prior consent from that individual. This includes mergers between two or more companies that retain personal information; the newly merged entities cannot handle personal information beyond the scope of the purpose of use stated before the merger unless it receives new consent.[74]

Furthermore, pursuant to the APPI, in limited circumstances, individuals can withdraw their consent to the use of their personal information by requesting that an entity stop using and erase the information that may lead to the identification of that person. The person must meet a high threshold: the personal information had to be acquired either without consent or by some type of fraud, and the individual must present a sufficient reason why the entity must stop using the data. This provision does not apply to cases in which it would be difficult or expensive to stop using or erase the data.[75] If an individual requests that an entity disclose personal information that could lead to the identification of that individual, the entity must comply immediately.[76] Additionally, an individual may request an entity to correct, add, or delete personal information that is contrary to fact, and the entity must promptly engage in a responsive investigation.[77] This is a right not available under the GLBA. In the United States, consumers and customers have no right to access, correct, add to, or delete the personal information held by a financial institution.[78]

The APPI framework appears to give greater control (at least in theory) over personal information to an individual than does the

---

[74] Act on the Protection of Personal Information, Law No. 57 of 2003, *supra* note 2, art. 16, no. 1–2.

[75] *Id.* at art. 27, no. 1–2.

[76] *Id.* at art. 25, no.1.

[77] *Id.* at art. 26, no. 1.

[78] *See* 15 U.S.C. §§ 6801–6809.

GLBA. To prove this statement more conclusively, the opt-out options for data transfer to third parties must be taken into account. Similar to the jurisdictional questions in the second section of this note, the possibility of opting-out of third party transfers depends upon the definition of a third party. The GLBA uses the term "nonaffiliated third party ("NATP")," but leaves the exact definition up to the financial services sector regulators.[79] Conveniently, the regulators all use the same definition: a NATP is any person that is not an affiliate[80] or a person employed by a company that is not an affiliate.[81] Moreover, a NATP is also any company that is "an affiliate by virtue of [a financial institution having] direct or indirect ownership or control of the company in conducting merchant banking or investment banking activities."[82]

The FSA Guideline states that a third party is a natural person, corporation, or other group that is not an entity that provides personal information or the individual to whom the personal information belongs.[83] This includes affiliates as third parties, making the FSA Guideline definition much broader than that of the GLBA. This means that any entity under the jurisdiction of the APPI cannot freely transfer information to affiliates. For example, a bank cannot transfer personal information to a subsidiary without giving notice of a purpose of use and obtaining consent for each transfer of personal information with a different purpose than previous transfers. This significantly raises the cost of compliance for APPI-regulated entities in comparison to financial institutions under the GLBA, who can freely transfer information to affiliates, because APPI greatly increases the number of times an entity has to seek consent from, and give notice to, individuals.

The GLBA mandates that a financial institution cannot transfer nonpublic information to a nonaffiliated third party without notice.[84]

---

[79] 15 U.S.C. § 6802(b)(1)(A).

[80] An affiliate is "any company that controls, is controlled by, or is under common control with another company." 16 C.F.R. § 313.3(a).

[81] *Id.* at § 313.3(m)(1).

[82] *Id.* at § 313.3(m)(2).

[83] Guidelines for Personal Information Protecting in the Financial Field, *supra* note 24, at art. 13, no. 2.

[84] 15 U.S.C. § 6802.

This notice must include an opt-out provision that consumers (throughout this section, "consumers" includes customers) receive that clearly and conspicuously states an individuals' right to opt-out of data transfers to a third party. The notice must explain that the financial institution has the right to disclose nonpublic personal information about consumers to nonaffiliated third parties and that those consumers have the right to opt-out. The notice must also provide a reasonable method to opt-out, such as check boxes placed in a prominent position on the notice.[85] A consumer must have the option to opt-out at any time, and financial institutions must comply with all opt-out requests "as soon as reasonably practical."[86] An opt-out decision by a consumer is valid until that consumer revokes it, and even when a customer relationship ends, the opt-out still applies to all nonpublic personal information collected during the course of the relationship. If a customer relationship is reestablished, the opt-out that previously applied is no longer valid.[87]

However, a consumer cannot stop the flow of all nonpublic personal information under the GLBA. A financial institution has the right to some nonpublic personal information without having to provide an opt-out provision. As long as notice is given, opt-out requirements do not apply if a financial institution employs a nonaffiliated third party to perform a service on its behalf, or if a financial institution enters into a contract that prohibits the nonaffiliated third party from disclosing or using the nonpublic personal information it receives from the financial institution for any purpose outside the scope of the agreement.[88] The services that a nonaffiliated third party performs may include the marketing of financial products or services offered pursuant to joint agreements between one or more financial institution.[89] Lastly, the requirements for initial notice, opting-out, and for service providers and joint marketing do not apply if, in addition to other exceptions, a financial institution discloses nonpublic personal information because it is

---

[85] 16 C.F.R. § 313.7(a)(1).

[86] *Id. at* § 313.7(e)–(f).

[87] *Id. at* § 313.7(g).

[88] *Id.* at § 313.13(a).

[89] *Id.* at § 313.13(b).

necessary to effect, administer, or enforce a transaction that a consumer requests or authorizes.[90]

The major difference of the APPI is that its opt-out provision is shaped more by its various exceptions than by clearly stating when an individual can opt-out of a third party transfer. In addition, the APPI interprets opting-out as withholding consent, not revoking consent like the GLBA. In order to disclose information to a third party, an entity in the financial services sector needs to provide notice and receive prior opt-in consent unless the transference of personal information was included in a previous notice or cited in the purpose of use.[91] A financial sector entity can also share personal information with a third party if the entity provides notice to individuals that certain personal information is going to be jointly used, and if the notice specifies the type of personal information used, names the parties involved, and provides the purpose of use.[92] Furthermore, when a financial institution entrusts personal information to another entity within the scope of the purpose of use, the financial institution may transfer personal information without obtaining consent.[93]

There are only four cases in the APPI and FSA Guideline requiring neither notice nor consent: (1) cases in which the provision of personal information is based on laws; (2) cases in which the provision of personal information is necessary for the protection of the life, body, or property of an individual and in which it is difficult to obtain consent; (3) cases in which the provision of personal data is specially necessary for improving public hygiene or promoting the sound growth of children and in which it is difficult to obtain consent; and (4) cases in which the transfer of personal information is necessary for agents of national institutions and local entities to perform their duties and in which obtaining the consent of the person might impede the execution of the operations concerned.[94]

Lastly, there are three exceptions for consent carved out for the credit industry under the APPI. First, when personal information is transferred to a credit bureau, a financial services sector entity must

---

[90] 15 U.S.C. § 6802(e).

[91] Act on the Protection of Personal Information, Law No. 57 of 2003, *supra* note 2, at art. 23, no. 2.

[92] *Id.* at art. 23, no. 3.

[93] *Id.* at art. 23, no. 4(1).

[94] *Id.* at art. 23, no. 1.

obtain consent from all individuals that can be identified by the transferred personal information because that personal information will then be distributed to various financial institutions. In doing so, individuals should be able to determine whether to give consent with the assistance of a description of the purpose of use of the personal information by the credit bureau's member companies and a list of these member companies provided by the financial entity. Second, a financial services sector entity must take particular care not to use the personal information for purposes other than examining the repayment capacity of financial customers.[95] Third, an opt-out cannot be used within the consumer credit industry because of the need for information exchange between the credit bureaus to address the management of credit limits and heavy debt loads.[96]

There is not a significant difference between the opt-out provisions in the GLBA and the Japanese law. However, the APPI seems to be stricter than the GLBA. Both laws allow individuals to stop their personal information from being transferred to third parties, but the APPI severely constrains the movement of personal information within an entity by putting affiliate companies into a third party category. In addition, although a financial institution must provide notice when transferring nonpublic personal information to credit bureaus, the GLBA does not include a rule that requires the notice to include as much information as the FSA Guideline requires. Once again, the APPI and its attendant guidelines create a stricter framework than does the GLBA.

VI. CONCLUSION

The U.S. and Japanese financial services sectors serve hundreds of millions of people worldwide, and both store massive amounts of data upon which their businesses operate. Accordingly, it is imperative to protect the pertinent information of customers whose sensitive data is held by these institutions. It is Title V of the Gramm-Leach-Bliley Act, the Act for the Protection of Personal Information, and the various guidelines created by Japanese government ministries that provide this protection. Together these form a framework to ensure the

---

[95] Guidelines for Personal Information Protecting in the Financial Field, *supra* note 24, at art. 13, no. 3.

[96] Guidelines for the Protection of Personal Information in Credit Sector among Industrial Sectors, *supra* note 26, at art. 2, no 4(2).

responsible disclosure of personal information in the financial services sectors of both countries.

Despite having the same general purpose, these privacy laws differ significantly. The APPI protects personal information because of the inherent characteristics of personal information; the protection of an individual's privacy is merely a positive outcome (data-centric), while the GLBA protects personal information in the financial services sector because of an individual's relationship to a financial institution (entity-centric). The laws even have different definitions of "personal information," of the individuals whose data are handled by financial institutions, and of what qualifies as a "financial institution." The pillars of both privacy regimes are notice, consent, and the option to opt-out, but none of these are similarly dealt with by the laws of the two countries.

The APPI has a more rigorous process for notice, consent, and opting-out. A financial entity under the APPI must give the same notice to all individuals whose information it utilizes. The GLBA, however, differentiates between customers and consumers. APPI-regulated entities must provide notice every time it utilizes personal information for a new purpose, which is quite unlike the GLBA's annual reporting requirement. The APPI gives individuals the right to access and modify their personal information, and financial institutions must receive consent for any utilization of personal information. The GLBA's only consent requirement is that financial institutions cannot transfer personal information to a third party if an individual actively opts-out of such transfers. The option to opt-out differs because the APPI's definition of "third parties" includes affiliates, making it much broader than the GLBA's definition. Despite these differences, both of these laws provide individuals the assurance that financial institutions will securely handle and use their personal information.