Personal Data Privacy in the United States and Asia

Introduction

This paper examines principles governing the privacy of personal, consumption-related data or information, primarily in the United States but also in Asia, with a view toward identifying best practices for businesses engaged in the collection, handling, use, disclosure, transfer, or sale of individuals' personal data or information. Part I gives a picture of the legal landscape in the U.S. Although that landscape is a patchwork quilt of state regulation, federal regulation, and litigation, certain common, fundamental elements do emerge, which can help guide businesses toward mitigation of government and private litigation risk. Parts II and III discuss recent data privacy initiatives in Asia, specifically in India and by the Asia-Pacific Economic Cooperation (APEC). APEC has created a multinational framework of voluntary privacy rules for businesses and government enforcement, which the U.S. has joined. As more nations join the APEC system, the flow of data across the Pacific will become increasingly smooth. Part IV concludes with a list of best practices for businesses that need to be concerned with data privacy, particularly those involved in the cross-border transfer of individuals' personal data to Asian-Pacific nations.

I. Sources of Data Privacy in the United States

There is no explicit right to privacy in the U.S. Constitution. The Fourth Amendment guarantees the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable

---

[1] This paper is intended for informational and continuing legal education purposes only; it does not constitute the giving of legal advice. The author would like to thank Mitch Stoltz of the Electronic Frontier Foundation for his valuable research on some of the issues discussed below.

searches and seizures," to which Fourth Amendment jurisprudence commonly refers as a "reasonable expectation of privacy." However, the Fourth Amendment is a guarantee, not against "invasion of privacy" per se, but against "unreasonable" invasion of privacy by the government when searching citizens' "persons, houses, papers, and effects."[2] And although Supreme Court Justice Louis Brandeis's often cited dissent in *Olmstead v. United States*[3] (a case involving the constitutionality of the then-revolutionary technology of telephone wiretapping) has become constitutional apocrypha—describing the right to privacy as "the most comprehensive of rights and the right most valued by civilized men"[4]—the Constitution itself offers no guidance as to the nature or extent of that right.

While Congress has legislated that certain categories of personal information be protected by statutes specifically governing the protection and use of such information,[5] vast amounts of personal data—most notably data on personal consumption—remain unregulated by any national privacy framework.

---

[2] United States v. Jones, 565 U.S. ___, ___, slip op., at 5 (Jan. 23, 2012) (Scalia, J.).

[3] 277 U.S. 438 (1928).

[4] *Id.* at 478 ("The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the government, the right to be let alone-the most comprehensive of rights and the right most valued by civilized men. To protect, that right, every unjustifiable intrusion by the government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment.").

[5] Examples include: medical information (Health Insurance Portability and Accountability Act of 1996 (HIPAA)); information held by financial institutions and credit reporting agencies (Graham-Leach-Bliley Act and Fair Credit Reporting Act); information about children (Children's Online Privacy Protection Act of 1998 (COPPA)); and video tape sales and rentals (including DVDs but not streamed titles) pursuant to the Video Privacy Protection Act of 1988.

At the state level, some regulation does exist, but it generally requires only an online business posting a policy on its use of customers' personally identifying information and compliance with that policy. The California Online Privacy Protection Act[6] requires any website that collects "personally identifiable information" (i.e., name, address, email address, phone number, Social Security number) to post a privacy policy describing the categories of information it collects, with what entities it may share that information, and how a customer can review and request changes to their information *if* such review is provided. The act imposes penalties for violation of a site's own posted policy. California Attorney General Kamala Harris has stated California's intent to enforce its Online Privacy Protection Act against mobile apps as well, and to impose fines up to $5,000 per user. Nebraska and Pennsylvania have laws that prohibit false or misleading statements in a posted privacy policy, although they do not specify what information such policies must contain.[7] Connecticut requires a posted policy for any site that collects Social Security numbers.[8]

Posting a privacy policy, keeping it up to date, and putting in place human and technical infrastructure for conforming to the policy is a basic, foundational element of an effective privacy strategy. But it is not likely to be enough in the near future. In an August 2011 speech, FTC Chairman Jon Leibowitz amusingly but tellingly remarked how one web site's privacy policy required 109 mouse clicks to get through it. Even lawyers (at least this author) do not even come close to reading many sites' privacy policies. One of the fundamental principles of data privacy regulation is informed consent to disclose personal information. Dense, lengthy privacy policies filled with legalese are unlikely to

---

6 Cal. Bus. and Prof. Code §§ 22575-22577.

7 Neb. Stat. § 87-302(114); 18 Pa. C.S.A. § 4107(a)(10).

8 Conn. Gen Stat. § 42-471.

convey to individuals, even lawyers, of precisely what privacy they are giving-up in a plain, unambiguous way.

Federal Trade Commission Enforcement

The Federal Trade Commission has been highly active in enforcing data privacy by using its authority under § 5(a) of the Federal Trade Commission Act to stop "unfair and deceptive business practices," typically misrepresentations to consumers about the security and privacy of their data. On August 10, 2012, the Commission approved the final consent order in *In re Facebook, Inc.*,[9] among the FTC's highest-profile privacy-enforcement actions. The FTC had alleged multiple violations of § 5(a) of the FTC Act, namely Facebook's:

- not preventing users' information from being shared with apps that users' Friends used, despite Facebook's communicating to users that they could restrict certain information they provided on the site to a limited audience;
- changing certain privacy settings in 2009 without adequately disclosing the changes to users;
- representing to users that an app would access only the information it needed, when in fact the app accessed all the user's information, e.g., a horoscope app would access photos;
- sharing user information with advertisers when it represented it would not;
- representing that it had certified the security of certain apps when it had not;
- telling users that their photos and videos would be deleted when users deactivated their accounts, when Facebook continued to allow access to such content; and
- deceptively stating that it complied with the U.S.-European Union Safe Harbor Framework for the transfer of data from the EU to the U.S. consistent with European law.[10]

---

[9] File No. 092 3184, Docket No. C-4365 (FTC Aug. 10, 2012).

[10] Analysis of Proposed Consent Order to Aid Public Comment, at 1-2 (Nov. 29, 2011), available at http://www.ftc.gov/os/caselist/0923184/111129facebookanal.pdf.

The Facebook consent order requires Facebook to:

- not misrepresent the privacy or security of "covered information";[11]
- give users "clear and prominent notice and obtain their affirmative express consent before sharing their previously collected information with third parties in any way that materially exceeds the restrictions imposed by their privacy settings";
- "implement procedures reasonably designed to ensure that a user's covered information cannot be accessed from Facebook's servers after a reasonable period of time, not to exceed thirty (30) days, following a user's deletion of his or her account"; and
- "establish and maintain a comprehensive privacy program . . . documented in writing [and] appropriate to Facebook's size and complexity," including: designation of employees "to coordinate and be responsible for the privacy program"; identification of both internal *and* external reasonably foreseeable privacy and security risks; controls and safeguards to address those risks; regular testing, monitoring, evaluation, and readjusting of these controls; and contractual requirements from third-party service providers that they will implement and maintain appropriate privacy protections.[12]

Facebook must also provide to the FTC an independent assessment of its privacy program every year for 20 years, and must retain all: "widely disseminated" privacy or security policies; consumer privacy complaints; documents calling into question any aspect of Facebook's compliance with the consent order; and materially different documents concerning the obtaining of users' express consent to disclosure of personal information, and information sufficient to show each user's consent.[13] Each violation of the consent order is punishable by up to $16,000.[14]

---

[11] Name; physical address; email and other online contact information; telephone numbers; photos and videos; and physical location.

[12] Analysis of Proposed Consent Order to Aid Public Comment, at 2-3.

[13] *Id.* at 3.

[14] See also *In re Google, Inc.*, Docket No. C-4336 (FTC Oct. 13, 2011), available at http://www.ftc.gov/opa/2011/10/buzz.shtm, in which the FTC charged Google with publicizing users' Gmail contacts without their consent and contrary to Google's privacy policies for the purpose of generating and populating Google's then-new social network, Buzz. Similar to the Facebook consent order, the Google consent order requires Google to seek users' affirmative consent if Google seeks to make any user data more widely

In March 2012, the FTC also issued its Final Privacy Report, which outlines what the FTC perceives to be best practices for companies that collect and use consumer data.[15] As summarized by FTC Chairman Leibowitz, these best practices include:

- "reasonable security for consumer data";
- "collecting only the data needed for a specific business purpose";
- "retaining data only as long as necessary to fulfill that purpose";
- "safely disposing of data no longer in use";
- "implementing reasonable procedures to promote data accuracy";
- "provid[ing] simpler and more streamlined choices to consumers about [companies'] data practices," including standardized privacy disclosures across companies within an industry and perhaps across industries; and
- granting consumers reasonable access to their data.[16]

Data security

A critical element of data privacy is data security: keeping private and valuable information out of the hands of malicious entities. Existing federal and state law can impose liability on merchants and advertisers for preventable third-party theft of personal information. Some state laws also impose a duty to safeguard the personal information of customers and users with reasonable security. California requires "[a] business that owns or licenses personal information about a California resident" to

---

available to third parties. Like Facebook, Google was also required to implement a comprehensive privacy program subject to FTC oversight for 20 years.

[15] Federal Trade Comm'n, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*, available at http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.

[16] Prepared Statement of the Federal Trade Commission on the Need for Privacy Protections: Perspectives from the Administration and the Federal Trade Commission, Before the Committee on Commerce, Science, and Transportation, U.S. Senate (May 9, 2012), at 3-4, available at http://www.ftc.gov/os/testimony/120509privacyprotections.pdf.

"implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."[17] In addition, when disclosing personal information to a third party, a company must require, by contract, that the third party maintain the information with reasonable security.

These secure handling laws are, for the most part, nonspecific. They do not require businesses to follow "best practices," but instead permit businesses to decide for themselves what constitutes reasonable security. In light of the recent, highly publicized epidemic of data security breaches, there is a debate whether these laws are effective. In addition, the absence of specific data security standards leaves the issue to the mercy of American tort law and likely varying jury determinations.

A recent Federal Trade Commission enforcement action offers some guidance as to minimum data security precautions. In June 2012, the FTC filed a complaint against Wyndham Hotels for Wyndham's "failure to maintain reasonable and appropriate data security for consumers' sensitive personal information," which allegedly allowed unauthorized access to consumers' data "on three separate occasions in less than two years" and led to more than $10.6 million in losses for fraudulent payment card charges.[18] Outside information held by financial institutions and credit reporting agencies, the FTC does not have direct authority over data security practices; however, again the FTC was able to bring an action based on Wyndham's representation to consumers that Wyndham protected

---

[17] Cal. Civ. Code §§ 1798.80-1798.84.

[18] Complaint ¶¶ 1-2, FTC v. Wyndham Worldwide Corp., Case No. 2:12-cv-01365-SPL (D. Ariz. Jun. 26, 2012), available at http://www.ftc.gov/os/caselist/1023142/120626wyndamhotelscmpt.pdf.

consumers' personally identifiable information using "standard industry practices" and "commercially reasonable efforts."[19]

The FTC alleges that Wyndham "failed to provide reasonable and appropriate security . . . by engaging in a number of practices that, taken together, unreasonably and unnecessarily exposed consumers' personal data to unauthorized access and theft," including:

- failing to employ firewalls;
- allowing software to be configured such that payment-card information was stored in clear readable text;
- "failing to remedy known security vulnerabilities," including allowing insecure servers to connect to Wyndham's network and "using outdated operating systems that could not receive security updates";
- enabling default user IDs and passwords on servers;
- failing to require the use of complex passwords;
- failing to inventory computers connected to the network, which resulted in failure to locate the computers from which it was known the unauthorized access originated; and
- failing to conduct security investigations and therefore to detect and prevent future unauthorized access.[20]

The FTC, and at least 29 states, also require businesses to destroy personal data securely when they are no longer to be used, such as by shredding.[21] Generally, these laws do not specify what events trigger a requirement to destroy data. Thus, it is up to the business to determine when data are no longer needed. However, improper disposal can lead to fines even if no theft of information occurs. In 2008, the FTC filed a complaint against a Las Vegas businessman for discarding customer financial

---

19 *Id.* ¶ 21.

20 *Id.* ¶ 24.

21 The FTC rule can be found at 16 CFR Part 682.

documents, such as tax returns, bank statements, and mortgage applications, in a dumpster behind his office. The FTC claimed that this violated secure disposal rules and also the company's own privacy policy, which promised to "maintain physical, electronic, and procedural safeguards that comply with federal standards to store and secure information about you from unauthorized access."[22]

Because of these laws, an internal policy for secure disposal of data (electronic and hard copy) is essential. In this context it is important to note that the basic delete function on a personal computer does not securely delete data; generally, the data are easily recoverable until overwritten by other data, which happens unpredictably. The solution is to use a readily available secure deletion tool that immediately overwrites "deleted" data.

As of the end of 2010, 46 states and the District of Columbia also have laws requiring businesses to notify customers after a theft of, or unauthorized access to, personal data. Requirements vary by state as to what types of information are covered and how notice must be given. For example, the Massachusetts notification law covers information "that creates a substantial risk of identity theft or fraud," and requires either written or electronic notice unless the cost of notice would exceed $250,000.[23]

Safe-disposal and breach-notification rules apply to financial information and the information generally found in credit reports, that is, social security numbers, credit card numbers, and financial account numbers, and to passwords giving access to financial data—in other words, information that can be used for identity theft. These rules generally do not apply to customer names or email addresses where more sensitive information is not present. They also do not apply to unauthorized or undisclosed

---

[22] http://www.ftc.gov/os/caselist/0723067/090121navonecmpt.pdf.

[23] Mass. Gen. Laws § 93H-1 et seq. For a list of all current state notification laws, see http://www.ncsl.org/Default.aspx?TabId=13489.

sale of personal information, even inadvertent sales to identity thieves posing as legitimate businesses. For these reasons, notification laws have been criticized as incomplete, and there may be pressure to broaden them.

Location tracking

In 2011, policymakers and litigants began focusing on the potential of mobile computing devices such as smartphones and tablets to track a user's geographic location. The ability to track the approximate location of a device is inherent and necessary in the design of wireless networks (which must be able to detect which tower sites are nearest to a given device). In some cases, location awareness may even be required by law for use by emergency responders. The catalyst for new rules has been the explosion of mobile computing and downloadable "apps" for which the user's location can be a very useful piece of information. One of the major advantages to mobile devices with a continuous connection to the Internet is the ability to deliver information relevant to the user's real-time location. However, the data generated by "geolocation" services can be abused, and the very generation of such data has been perceived by the public as an invasion of privacy. This has led to public outcry and possible regulation.

In April 2011, two security researchers discovered that devices running Apple's iOS 4.0 recorded the approximate physical location of the device to a file. The data were persistent, showing a long history of the device's approximate location whenever it was turned on. Apple potentially had access to these data. The company's reason for the tracking file was: using the location of nearby cell towers as a means of pinpointing the device's exact location more quickly using the Global Positioning System (GPS) for use by applications on the device. Nonetheless, the discovery of the tracking file caused an outcry. Similar location data were also discovered in devices running versions of Google's Android operating system.

In response, Senators Franken (D.-Minnesota) and Blumenthal (D.-Connecticut) introduced a bill, S. 1223 (2011), under which "a covered entity may not knowingly collect, receive, record, obtain, or disclose" geolocation data without express authorization from the user. The bill is still being considered by the Senate Judiciary Committee.

Apple was also sued in federal court by a putative nationwide class of users of Apple iOS devices, under a variety of federal and state laws.[24] The information that Apple allegedly unlawfully collected from users (it was also allegedly unencrypted) included location data, the unique device identifier assigned to each device, the user's gender, age, and zip code, and search terms run by the user.[25] The district court dismissed the majority of the plaintiffs' claims—including their claim for invasion of privacy under the California Constitution. The court allowed only their claims under California's Consumer Legal Remedies Act and California's Unfair Competition Law, because Apple's representations to consumers, that it "takes precautions—including administrative, technical, and physical measures—to safeguard your personal information against theft, loss, and misuse, as well as against unauthorized access, disclosure, alteration, and destruction," may have caused consumers to overpay for their devices within the meaning of the Consumer Legal Remedies Act and may have constituted unlawful conduct and misrepresentations within the meaning of the Unfair Competition Law.[26] Also, Apple's user agreement was sufficiently ambiguous for the plaintiffs to avoid dismissal on the ground that they consented to the disclosure. Although Apple informed users that it would collect the information at issue, it also conflictingly informed users that it would limit how it would use users'

---

[24] *In re* iPhone Application Litig., Case No.: 11-MD-02250-LHK (N.D. Cal.).

[25] Order Granting in Part and Denying in Part Defendants' Motions to Dismiss, at 3, 10 (Jun. 12, 2012).

[26] *Id.* at 32-38.

"personal information," including "data that can be used to uniquely identify or contact a single person."[27]

With respect to the California invasion-of-privacy claim, the court held that such a claim only existed for "egregious breach[es] of [] social norms," and that Apple's alleged disclosure of the above personal information—even without users' knowledge or consent—was not so egregious but was "routine commercial behavior."[28] Thus, it was not any "private" nature in the information collected and disclosed that gave rise to the claim against Apple; but Apple's possible failure to honor its own ambiguous privacy policy.

But there has been some substantive recognition in the courts of the invasiveness of pervasive location tracking. In *United States v. Jones*,[29] the Supreme Court's most recent exposition of the "reasonable expectation of privacy" within the meaning of the Fourth Amendment, the Court assessed warrantless GPS tracking. There, the police attached a credit-card sized GPS device to a suspect's car and tracked the suspect's movements electronically, obtaining 2,000 pages of data over a four-week period.[30] The Court held the GPS tracking unconstitutional—not because of any inherent right not to be tracked—but because of the physical intrusion on the suspect's car (automobiles are personal "effects" within the meaning of Fourth Amendment).[31] The Court noted how its precedents found *no* reasonable expectation of privacy in public, "open fields"[32] and "thoroughfares."[33]

---

27 *Id.* at 42.

28 *Id.* at 23.

29 Note 2, *supra*.

30 *Id.* at 2 (opinion of Scalia, J., for the Court).

31 *Id.* at 3-4.

32 *Id.* at 10 (citing Oliver v. United States, 466 U.S. 170 (1984)).

However, four justices expressed the opinion that such pervasive tracking as in *Jones* gave rise to a violation of Jones's reasonable expectation of privacy and thus required a warrant.[34] And Justice Sotomayor expressed the opinion that such tracking was a potential cause for concern because "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."[35] So it appears that a majority of the Court would find that pervasive location tracking implicates privacy concerns, and very serious ones are described by Justice Sotomayor.

II. Sources of Data Privacy in Asia

In contrast to the lack of codified, national privacy standards for personal information in the U.S., many countries in Asia have elevated protection of personal information to a statutory or regulatory right.

On April 11, 2011, the Indian Central Government's Ministry of Communications and Information Technology promulgated, pursuant to the Information Technology Act of 2000, the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 (hereinafter, the "Rules"). The Rules define personal data or information to mean "any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate [an

---

[33] *Id.* at 11 (citing United States v. Knotts, 460 U.S. 276, 281 (1983)).

[34] Alito, Ginsburg, Breyer, and Kagan, in an opinion by Alito, concurring in the judgment.

[35] *Id.* at 3 (Sotomayor, J., concurring) (citing People v. Weaver, 12 N.Y.3d 433, 441-42, 909 N.E.2d 1195, 1199 (2009) ("Disclosed in [GPS] data . . . will be trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on")).

association, firm, corporation, or other corporate entity], is capable of identifying such person." (Rule 2) The Rules further create a subcategory of "sensitive personal data or information," which includes any information comprising or "relating to": passwords; financial and payment information; physical, physiological, and mental health; medical records or history; biometric information; and sexual orientation. (Rule 3)

Rules 4 through 6 create detailed obligations concerning the collection and disclosure of personal data and information on the part of any corporate entity that "collects, receives, possess[es], stores, deals *or* handle[s]" such information, namely:

- providing "[c]lear and easily accessible statements" of the entity's privacy and security policies and practices, including specifically publication on the entity's website;
- identifying the "type" of personal data or information collected by the entity;
- identifying the "purpose of collection and usage of such information";
- obtaining "consent *in writing* through letter or Fax or email from the provider of the sensitive personal data or information *regarding the purpose* of usage before collection of such information";
- prohibiting collection of sensitive personal data or information unless *necessary* for "a lawful purpose connected with a function or activity" of the entity;
- while engaged in the process of collecting the information, taking reasonable steps to inform the provider of the information of "the fact that the information is being collected," "the purpose for which the information is being collected," "the intended recipients of the information," and "the name and address of—the agency that is collecting the information" and "that will retain the information";
- prohibiting retention of sensitive personal data or information "for longer than is required for the purposes for which the information may lawfully be used";
- granting providers of information with access to their information upon request and with the ability to correct or amend their data "as feasible";
- providing providers of information with the option "not to provide the data or information sought to be collected," *and* with an option to withdraw consent given earlier;

- designating a Grievance Officer to redress grievances "expeditiously but within one month" from receipt of the grievance; and

- prohibiting disclosure of sensitive personal data or information to any third party without prior permission "or where the disclosure is necessary for compliance of a legal obligation"; the third party receiving the information "shall not disclose it further."

Rule 7 provides that sensitive personal data or information may be transferred only to another entity (either within India or without) "that ensures the same level of data protection . . . as provided for under these rules" and "only if it is necessary for the performance of the lawful contract between the [entity] and provider of information or where such person has consented to data transfer."

Finally, Rule 8 requires data collectors to implement documented "reasonable security practices and procedures" "that are commensurate with the information assets being protected." Rule 8 specifically incorporates the international standard IS/ISO/IEC 27001 ("Information Technology - Security Techniques - Information Security Management System - Requirements") as one such system. If the data collector wishes to use another set of best practices, it must have those practices approved by the Central Government. Data collectors must have their systems audited at least once per year, and whenever they "undertake significant upgradation of [their] process[es] and computer resource[s]."

Other nations in Asia that have enacted personal data privacy statutes include Hong Kong (Personal Data (Privacy) Ordinance of 1995), Japan (Act on the Protection of Personal Information of 2003), South Korea (Act on Promotion of Information and Communication Network Utilization and Information Protection of 2001), and Taiwan (Computer-Processed Personal Data Protection Law of 1995).

III. The Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR) System

The APEC CBPR System is a set of voluntary internal business rules concerning data privacy and security that was designed by APEC's member economies, including the U.S., "to create more consistent

privacy protections for consumers when their data moves between countries with different privacy regimes in the APEC region."[36] Companies wishing to take advantage of the APEC CBPR System must undergo an independent third-party certification process that ensures compliance with the privacy rules in the System.[37] In addition to creating a uniform system of data privacy and security across the APEC countries and its associated benefits to cross-border enforcement, the CBPR System has as its goals the free flow of information across borders and the creation of trust among both consumers *and* organizations that the entities with which they transact business involving personal information have robust data privacy and security policies.[38]

Once an organization has been certified as CBPR-compliant, the CBPR System privacy policies and practices become binding and enforceable by an appropriate enforcement authority.[39] For example, the U.S. FTC could bring an action under § 5(a) of the FTC Act for a company's failure to comply with the CBPR System, as an "unfair and deceptive business practice," because a CBPR-compliant company is representing that it complies with the System. While "[p]articipation in the CBPR System

---

[36] FTC Press Release, "FTC Welcomes a New Privacy System for the Movement of Consumer Data Between the United States and Other Economies in the Asia-Pacific Region" (Nov. 14, 2011). The 21 members are: Australia; Brunei Darussalam; Canada; Chile; the People's Republic of China and Hong Kong; Indonesia; Japan; the Republic of Korea; Malaysia; Mexico; New Zealand; Papua New Guinea; Peru; the Philippines; Russia; Singapore; Chinese Taipei; Thailand; the U.S.; and Viet Nam.

[37] Even before a company can participate in the APEC CBPR System, that company's APEC member economy must itself qualify for participation in the System, generally by: (1) having in place a mechanism to enforce data privacy and security within its borders; and (2) participating in the APEC Cross-Border Privacy Enforcement Arrangement, which is a multilateral arrangement enabling national privacy enforcement authorities to share information and provide assistance in cross-border data privacy and security enforcement. On July 26, 2012, the U.S. was confirmed as having met these conditions through the enforcement authority and activities of the FTC.

[38] APEC Cross-border Privacy Rules System – Policies, Rules and Guidelines, at 2-3.

[39] *Id.* at 4.

does not replace a participating organization's domestic legal obligations,"[40] these rules comprise many best practices in data privacy and security, and therefore likely will serve as a solid foundation from which to build-out additional privacy and security policies and practices as this dynamic legal landscape continues to change.

The requirements for APEC certification are exhaustive. The key elements of notice to individuals are:

- providing "clear and easily accessible statements" about practices and policies governing personal information, including specifically publication on the entity's website and stating an effective date of the policies and practices;
- describing how the personal information is collected;
- identifying the "type" of personal information collected, and the "categories or specific sources of all categories of personal information collected";
- describing "the purpose(s) for which personal information is collected";
- informing individuals "whether their personal information is made available to third parties and for what purpose," including identification of the "categories or specific third parties, and the purpose for which the personal information will or may be made available";
- providing "contact information regarding practices and handling of personal information upon collection";
- providing "information regarding the use and disclosure of an individual's personal information";
- providing "information regarding whether and how an individual can access and correct their personal information"; and
- providing notice to individuals that their information is being collected at the time it is being collected, including the purpose for which it is being collected and whether it may be shared with third parties and for what purpose.[41]

---

[40] *Id.* at 10.

[41] APEC Cross-border Privacy Rules System Program Requirements, at 2-5.

A business seeking APEC CBPR System certification must also document how:

- each type of data collected is collected only for the stated limited purpose(s) of collection;
- each type of data collected is used only for the stated limited purpose(s) of collection; and
- each type of data collected is disclosed or transferred only for the stated limited purpose(s) of collection.[42]

Additional requirements include: providing individuals with clearly worded, easily understandable, and conspicuous choice to prohibit or limit their disclosure of personal information;[43] and having in place reasonable procedures to maintain up-to-date, accurate, and complete information, including through procedures for individuals to correct the information and for the collector of the information to provide corrections to, and receive corrections from, third parties to whom the collector had previously disclosed or transferred the information.[44]

With respect to data security, the CBPR System requires physical, technical, and administrative safeguards "proportional to the probability and severity of the harm threatened," which safeguards may include password protections, encryption, firewalls, and monitoring.[45] Businesses are also required to train and oversee employees on data security issues.[46] Also required are measures for secure disposal of personal information, measures to detect, prevent, and respond to attacks, periodic risk assessments,

---

[42] *Id.* at 6-10.

[43] *Id.* at 11-14.

[44] *Id.* at 15-16.

[45] *Id.* at 17.

[46] *Id.* at 18.

and reasonable measures to require information processors, agents, contractors, or other service providers to whom personal information is transferred, to secure the information.[47]

Finally, the business must designate employees to be responsible for compliance with the CBPR System, including for procedures for receiving, investigating, and responding to complaints and for information processors', agents', contractors', or other service providers' compliance with the business's privacy and security policies and practices.[48]

IV. Best Practices for Compliance with U.S. and Asian Data Privacy Regimes

Beyond satisfying the need to comply with existing rules, robust and flexible compliance systems will lower the cost of compliance with foreseeable future rules. Characteristics of such systems include: internal awareness of, and procedures for, how individuals' personal data are collected, stored, used, disclosed, transferred, and sold; reasonable safeguards and handling procedures for the data; adequate data privacy and security policies and practices, both in terms of existing rules and in terms of anticipated areas of concern; up-to-date disclosure of data privacy and security policies and practices to individuals; continual monitoring of compliance with those policies and practices; and attention to how particular use and sale of personal information may be perceived by the public. In short, how are the data collected? Where are the data stored? How are the data used? Where do the data go? And are the individuals who provide the data given clear, unambiguous notice of all of this? This latter question is critical given the central role of informed consumer consent in all jurisdictions in both existing and proposed legislation, and in the public perception that drives such legislation. Moreover, because of widespread media and public attention to data privacy and security, privacy and security policies and

---

47 *Id.* at 19-20.

48 *Id.* at 24-28.

practices and their transparency to consumers are increasingly being perceived as a significant competitive element in service providers' offerings.

Three critical, foundational practices can readily be identified. First and foremost, designate a chief privacy officer: (a) to fully comprehend the flow of personal data in the company's IT and human infrastructure, in order to verify and regularly monitor compliance with the company's data privacy and security policies and practices; and (b) to keep those policies and practices current with the latest global legal and public developments. Second, incorporate privacy and security policies and practices into existing internal mechanisms and procedures for contract compliance, in order to ensure that data privacy and security compliance permeates all aspects of the company. Third, train all employees involved in the collection, storage, use, disclosure, transfer, or sale of personal data in company privacy and security policies and practices. Given the myriad ways in which data are collected, stored, used, disclosed, transferred, and sold, knowledgeable employees are the first, best, and most efficient line of defense against inadvertent data disclosure.

Below are three checklists of specific best practices. "Level 1: US" includes those practices that should go a long way to minimizing adverse data privacy events and minimizing litigation risk in the U.S. given the current legal landscape. "Level 2: India" includes those practices in addition to "Level 1: US" that are necessary for compliance with India's new data privacy and security rules. "Level 3: APEC" includes practices in addition to Level 1 and Level 2 that are necessary for APEC certification.

Level 1: U.S.

- Clear, unambiguous, non-legalese statement of data privacy & security policies and practices – can link to a more detailed legal statement
- Consent for every change
- Disclose precisely what data are collected and how they are used, and be especially vigilant about location tracking – precise disclosure also makes it easier for your own employees to follow and monitor compliance
- Disclose precisely to which third parties or categories of third parties data may be disclosed, sold, or transferred – again, also makes it easier for your own employees to follow and monitor compliance
- Access only data that the application needs (but you need not represent that to users)
- Permanently delete all of an individual's data when it is no longer necessary or when you've told the individual you would
- Take reasonable security measures: strong passwords; firewalls; encryption (how sophisticated/extensive/expensive depends on the potential damage from security loss)
- Have a system in place for regularly monitoring the security and integrity of your network, and keep it updated
- If you've had the misfortune of being hacked, find out exactly what happened and do everything you can to stop it from happening again
- Avoid putting large collections of personal data on portable computers or removable media that travel outside your offices, as these are easily stolen
- Require third parties to whom you disclose data to commit contractually to maintain the security of the data
- FOLLOW YOUR OWN RULES!!!
- Don't make promises you're not sure you can keep
- If you don't do these things, and the FTC sues you, you're going to have to do a LOT more

Level 2: India

- ID the purpose(s) of collection, use, sale, and transfer of data
- Opt-out AND option to withdraw prior consent
- For "sensitive personal data or information," obtain "consent *in writing* through letter or Fax or email from the provider of the sensitive personal data or information *regarding the purpose* of usage *before* collection of such information"
- While engaged in the process of collecting the information, inform the provider of the information of "the fact that the information is being collected," "the purpose for which the information is being collected," "the intended recipients of the information," and "the name and address of—the agency that is collecting the information" and "that will retain the information"
- Grant providers of information with access to their information upon request and with the ability to correct or amend their data "as feasible"

- Do NOT transfer to third parties unless you obtain consent AND the transferee will grant the same protections as India
- Data security: (1) international standard IS/ISO/IEC 27001 ("Information Technology - Security Techniques - Information Security Management System - Requirements") or (2) Central Government approval

Level 3: APEC

- Inform individuals (1) whether their personal information is made available to third parties, (2) which third parties or categories of third parties, (3) for what purpose, *and* (4) do so at the time the information is being collected
- Establish procedures for individuals to correct their information and for *you* to provide corrections to, and receive corrections from, third parties to which you previously disclosed or transferred the information
- Training and oversight of employees on data privacy & security
- Measures to detect, prevent, and respond to attacks, and periodic risk assessments
- Measures to ensure *third parties' compliance* with data privacy & security policies and practices