HOW TO NAVIGATE LANDSCAPE OF GLOBAL PRIVACY AND DATA PROTECTION

Paul Jones
Principal
Jones & Co.
Toronto, ON

and

Leita Walker
Partner
Faegre Baker Daniels LLP
Minneapolis, MN

November 2 – 4, 2016
Miami, FL

©2016 American Bar Association
# TABLE OF CONTENTS

| I. INTRODUCTION .................................................................................................................. | 1 |
| II. RECENT U.S. DEVELOPMENTS .......................................................................................... | 3 |
| A. The Wyndham Decision and Subsequent Settlement ..................................................... | 3 |
| B. The Spokeo Decision ..................................................................................................... | 7 |
| III. RECENT INTERNATIONAL DEVELOPMENTS ................................................................... | 8 |
| A. Introduction .................................................................................................................... | 8 |
| B. European Model ............................................................................................................. | 9 |
| C. United States Model ...................................................................................................... | 10 |
| D. Privacy laws in Some of Franchising’s Top Markets ...................................................... | 10 |
| 1. Canada ........................................................................................................................ | 11 |
| a. Laws – Federal ............................................................................................................ | 11 |
| i. Enforcement Tools under PIPEDA .............................................................................. | 11 |
| b. Laws – Provincial ........................................................................................................ | 12 |
| c. Canada’s anti-spam legislation: ................................................................................ | 12 |
| i. CASL and Franchising: ............................................................................................... | 13 |
| ii. Implied consent and existing business relationship ................................................. | 13 |
| iii. Express consent ....................................................................................................... | 15 |
| iv. Unsubscribe Mechanism ............................................................................................ | 15 |
| d. Private Right of Action ............................................................................................... | 16 |
| 2. Australia ....................................................................................................................... | 16 |
| a. Law .............................................................................................................................. | 16 |
| b. Enforcement ................................................................................................................ | 17 |
| c. Private Right of Action ............................................................................................... | 17 |
| 3. People’s Republic of China (“PRC”).... ........................................................................ | 18 |
| a. Regulatory ................................................................................................................... | 18 |
| i. 2013 MIIT Guideline ................................................................................................. | 18 |
| ii. 2011 / 2012 MIIT Decision and Regulation ............................................................. | 20 |
| iii. 2016 Cybersecurity Law ........................................................................................... | 20 |
| b. Practice tip ................................................................................................................. | 20 |
| 4. Indonesia ...................................................................................................................... | 20 |
| 5. Other countries ............................................................................................................ | 21 |
E. Developments in the European Union .................................................................22
  1. Background on the Safe Harbor.................................................................22
  2. Facts Giving Rise to Schrems.................................................................23
  3. The Decision of the Court of Justice of the European Union...............23
  4. Announcement of the Privacy Shield.......................................................24
  5. Criticism of the Privacy Shield...............................................................25
  6. Adoption of General Data Protection Regulation............................26
  7. New rights ..............................................................................................26
  8. New obligations ......................................................................................27
  9. New processes ......................................................................................28
F. Data localization .........................................................................................29
G. Payment security standards ........................................................................30

IV. Risk Assessment and Compliance Planning ................................................31
  A. What Personal Information Does Your System Collect and Use? ..........32
  B. What are the Damages in a Privacy Breach? ........................................34
     1. Private Actions by the Subjects of the Breach ....................................34
     2. Obligations to the Banks and Insurance ...........................................35
     4. How to Comply ..................................................................................39
        a. Appoint a Privacy Officer ............................................................39
        b. Prepare and Adopt a Privacy Policy ...........................................39
        c. Prepare for Breaches, and Breach Notification ..........................41

V. CONCLUSION .............................................................................................43

BIOGRAPHIES ...............................................................................................44
I. INTRODUCTION

Privacy and data protection issues affecting franchisors have evolved considerably in the past decade or so. Historically, many of the concerns about compliance with privacy laws were focused around providing proper notices, obtaining appropriate consent for the use of personal information and, sometimes, unwarranted requests for access to information. While Europe has enacted strict privacy and data protection laws, enforcement was not common, and in the United States the difficulty in proving significant damages resulting from a failure to obtain the correct consent limited private enforcement.

Data protection and the risk of potential security breaches have now become a primary concern for franchisors, particularly where payment information is implicated. In the past, many franchise systems have allowed their franchisees to develop their own privacy policies and compliance methods. But the recent settlement in the Wyndham\(^1\) case suggests that such an approach may no longer be viable.

As will be discussed in this paper, the regulatory penalties and damage awards potentially resulting from the breach of an IT system and the unauthorized disclosure of a customer’s credit card or other payment information are such that franchisors may be faced with the option of either becoming much more deeply involved in the monitoring of privacy compliance by their franchisees, or, alternatively, publically disclaiming responsibility for their franchisees’ data security practices.

International privacy issues have also evolved. The revelations of Edward Snowden have changed the attitude of many international jurisdictions regarding the collection of personal information by businesses based in the U.S. Some have responded by mandating that data collected that concerns their citizens and residents only be held in their own jurisdiction. In addition, authorities charged with data protection in many international jurisdictions have become more concerned about the level of consent required to authorize the transfer of personal information to the United States.

Thus, as a result of on the Schrems\(^2\) case discussed in this paper, the Safe Harbor Program that previously allowed U.S. businesses to self-certify as to their compliance with European privacy standards, has collapsed. In Germany, for example, there already have been fines levied on three separate companies based on their electronic transfer of personal information to the United States in reliance on the now invalidated Safe Harbor Program.\(^3\) These retailers did not switch over to the alternative methods for compliance with such transfers, principally standard contractual clauses, quickly enough. This also illustrates how the enforcement of data protection in Europe has strengthened over the last decade.

---

3 Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, Pressemitteilungen „Unzulässige Datenübermittlungen in die USA - Erste Bußgelder rechtsskräftig, weitere Verfahren noch offen,“ June 6, 2016 (Hamburg Commissioner for Data Protection and Freedom of Information, Press Release „Invalid Data transfers to the USA – First Fines in Law. Further Measures still Open,“) available in German at: https://www.datenschutz-hamburg.de/news/detail/article/unzulaessige-datenuebermittlungen-in-die-usa.html?tx_ttnews%5BbackPid%5D=1&cHash=f00d844fb3434a4d32451675b0c454a5.
A new program, the E.U.-U.S. Privacy Shield (the “Privacy Shield”), was quickly put in place and approved by the European Commission for implementation on August 1, 2016. However, many on both sides of the Atlantic already question whether the additional protections in the Privacy Shield are adequate to address concerns regarding access to the personal information by American national security agencies, and this is unlikely to change. It is anticipated that the Privacy Shield will be challenged in the courts in the near future.

In addition to the changes with respect to the transfer of personal information to the U.S., the EU has also decided to upgrade the 1995 Data Protection Directive (the “Directive”). To this end the EU has drafted and adopted the General Data Protection Regulation (the “GDPR”). Unlike the Directive, which provided a common baseline standard but left it to member states to implement the Directive through their own data protection laws, the GDPR is a Regulation that has direct effect on EU member states in its own right. It is scheduled to come into effect May 25, 2018.

Perhaps the most important development in international privacy affecting franchising is the increasing adoption by countries of general privacy laws modelled on those of Europe. The U.S. model of regulated sectors, breach notification laws and voluntary compliance is now found outside the U.S. less and less. The U.S. has become the outlier in global data protection and, accordingly, compliance with European style general privacy laws by U.S. based franchisors will become another impediment to international expansion.

A decade ago Singapore had decided to follow the U.S. model and declined to adopt a general privacy law. Things have changed. In 2012, Singapore adopted the Personal Data Protection Act 2012 which is enforced by the Personal Data Protection Commission. A decade ago Brazil had a general privacy protection clause in its Federal Constitution, the Civil Code and other sectoral laws. But a draft bill on Data Protection was prepared and released for consultation in 2015. On May 13, 2016 the draft law was submitted to the Brazilian Congress three days before President Dilma Rousseff was impeached.

At first glance, it appears that other jurisdictions are, like the U.S., addressing privacy regulations in a sectoral approach. But a closer look often reveals that the regulations are merely interim measures put in place as stopgaps while a general data protection law is being drafted and discussed. The People’s Republic of China is an example of such a jurisdiction. In

---


6 Personal Data Protection Act of 2012, Act No. 26 of 2012, passed by Parliament on 15th October 2012 and assented to by the President on 20th November 2012, available at: http://statutes.agc.gov.sg/aol/search/display/view.w3p;page=0;query=DocId%3Aea8b845-51b8-48cf-83bf-81d01478e50b%20Depth%3A0%20Status%3Ainforce;rec=0.

7 Constituição da República Federativa do Brasil, Text of October 5, 1988, as amended.

8 Projeto de Lei 5276/2016, que dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural (Bill 5276/2016, which provides for the processing of personal data to guarantee the free development of the personality and dignity of the natural person), available in Portuguese at: http://www.camara.gov.br/proposicoesWeb/propos_mostrarIntegra?sessionid=D1B8E2F7337B0C8CBE8DA957C67F11DC.proposicoesWeb1?código=1457459&filename=PL+5276/2016.
2003, the government commissioned a group of experts to prepare what became the 2005 draft Personal Information Protection Law. However the drafting process for laws in the PRC is very consultative, and thus slow. When a major dispute arose between two PRC internet service providers in 2011, the law still had not been finalized and presented to the State Council. Accordingly, the PRC adopted a number of interim regulations focused on privacy on the internet to address the immediate problems. To the casual observer, the PRC may seem to be following a sectoral regulatory approach. However, the intention to have a general privacy law is still very much alive in the PRC.

U.S. franchisors are likely to find it increasingly difficult to navigate both U.S. and global privacy and data protection laws. U.S. franchisors considering international expansion in the future would do well to analyze and evaluate the implications of the Wyndham case and design a franchise system and IT system that complies with the general data protection laws in effect, or being adopted, both domestically and abroad.

II. RECENT U.S. DEVELOPMENTS

A. The Wyndham Decision and Subsequent Settlement

In F.T.C. v. Wyndham Worldwide Corp., a case brought by the Federal Trade Commission (the “FTC”) after hackers breached Wyndham hotel’s computer systems on three separate occasions, the Third Circuit Court of Appeals held that the FTC had authority to regulate cybersecurity under the Federal Trade Commission Act, which prohibits “‘unfair or deceptive acts or practices in or affecting commerce.’” The Third Circuit affirmed the district court’s denial of Wyndham’s motion to dismiss, specifically holding that (1) the FTC had authority to regulate cybersecurity under the unfairness prong of 15 U.S.C. § 45(a), and (2) Wyndham had fair notice that its cybersecurity practices potentially could violate that provision.

Wyndham franchises and manages hotels and sells timeshares through its subsidiaries and licenses its brand name to independently owned hotels. Wyndham-branded hotels process consumer information, including consumer names, addresses, and payment card information, on their property management systems.

The Wyndham case concerned three separate data breaches that occurred in 2008 and 2009, when hackers accessed Wyndham’s network and the property management systems of Wyndham-branded hotels and obtained the payment card information for more than 619,000 consumers, resulting in at least $10.6 million in fraud loss. The first cyberattack occurred in April 2008, when hackers broke into the local network of a Phoenix, Arizona, hotel that was

---


11 799 F.3d 236, 240, 259.

12 Id. at 240.

13 Id. at 240, 242.

14 Id. at 241.
connected to Wyndham’s network and the Internet.\textsuperscript{15} The hackers guessed user login IDs and passwords to access an administrator account on Wyndham’s network, enabling the hackers to obtain consumer data for more than 500,000 accounts that the hackers then sent to a domain in Russia.\textsuperscript{16} In March 2009, hackers again accessed Wyndham’s network through an administrative account.\textsuperscript{17} Wyndham was unaware of this attack until consumers filed complaints about fraudulent charges, at which point Wyndham discovered that, during the first attack, the hackers had installed “memory-scraping malware” on more than thirty hotel computer systems.\textsuperscript{18} The hackers obtained payment card information for approximately 50,000 consumers in this second attack.\textsuperscript{19} Finally, in late 2009, hackers accessed an administrator account on a Wyndham network and obtained payment card information for approximately 69,000 customers.\textsuperscript{20} Wyndham was not aware of this third attack until customers complained in January 2010.\textsuperscript{21}

The FTC filed suit against Wyndham in June 2012, asserting that Wyndham had engaged in “unfair” and “deceptive” trade practices in violation of 15 U.S.C. § 45(a).\textsuperscript{22} The FTC’s Complaint alleged that Wyndham engaged in the following unfair cybersecurity practices:

\begin{enumerate}
  \item Wyndham allowed its branded hotels to store payment card information in “clear readable text.”\textsuperscript{23}
  \item Wyndham “allowed the use of easily guessed passwords to access the property management systems.”\textsuperscript{24}
  \item Wyndham failed to use “readily available security measures”—such as firewalls—to ‘limit access between [the] hotels’ property management systems . . . corporate network, and the Internet.”\textsuperscript{25}
  \item Wyndham “allowed hotel property management systems to connect to its network without taking appropriate cybersecurity precautions.” For instance, Wyndham did not ensure that the hotels had adequate security policies and procedures, and it allowed hotels to use out-of-date operating systems and default user IDs and passwords.\textsuperscript{26}
\end{enumerate}

\textsuperscript{15} \textit{Id.}
\textsuperscript{16} \textit{Id.} at 242.
\textsuperscript{17} \textit{Id.}
\textsuperscript{18} \textit{Id.}
\textsuperscript{19} \textit{Id.}
\textsuperscript{20} \textit{Id.}
\textsuperscript{21} \textit{Id.}
\textsuperscript{22} \textit{Id.}
\textsuperscript{23} \textit{Id.} at 240.
\textsuperscript{24} \textit{Id.}
\textsuperscript{25} \textit{Id.} at 241.
\textsuperscript{26} \textit{Id.}
(5) Wyndham “failed to ‘adequately restrict’ the access of third-party vendors to its network and the servers of Wyndham-branded hotels.”

(6) Wyndham did not employ “reasonable measures to detect and prevent unauthorized access” to its computer network or conduct security investigations.

(7) Wyndham did not follow proper incident response procedures after the hackers gained access.

The FTC’s complaint also included a deception claim, alleging that Wyndham’s published website privacy policy overstated the company’s cybersecurity measures.

After setting out the history behind the FTC Act, the Third Circuit held that § 45(n) of the FTC Act “requires [1] substantial injury that [2] is not reasonably avoidable by consumers and that [3] is not outweighed by the benefits to consumers or competition” but “acknowledges the potential significance of public policy and does not expressly require that an unfair practice be immoral, unethical, unscrupulous, or oppressive.”

In so holding, the Court rejected Wyndham’s arguments that its conduct fell outside the plain meaning of “unfair.” First, the Court rejected Wyndham’s argument that the unfair conduct must be unscrupulous or unethical in order to be actionable, noting that the Supreme Court had rejected this view. Second, the Court rejected Wyndham’s argument that a practice is only “unfair” if it is not equitable or “marked by injustice, partiality, or deception,” holding that these requirements were of little relevance in this case because “[a] company does not act equitably when it publishes a privacy policy to attract customers who are concerned about data privacy, fails to make good on that promise by investing inadequate resources in cybersecurity, exposes its unsuspecting customers to substantial financial injury, and retains the profits of their business.” The Court also rejected Wyndham’s assertion that it did not treat its customers unfairly for purposes of the FTC Act because it, too, was victimized by criminals. In response to this argument, the court stated, “that a company’s conduct was not the most proximate cause of an injury does not immunize liability from foreseeable harms,” further noting that Wyndham did not argue that the cyber intrusions were unforeseeable—an argument that would be particularly implausible as to the second and third attacks. The Court further chided Wyndham’s argument that if the FTC’s authority extends to Wyndham’s conduct, “then the FTC also has the authority to ‘regulate the locks on hotel room doors . . . to require every store in the land to post an armed guard at the door,’ . . . and to sue supermarkets that are ‘sloppy about

27 Id.
28 Id.
29 Id.
30 Id.
31 Id. at 244 (citing 15 U.S.C. § 45(n)).
32 Id. at 244, 247.
33 Id. at 244-45.
34 Id. at 245.
35 Id. at 246.
36 Id. (emphasis in original).
sweeping up banana peels.” The Court stated that this “alarmist” argument “invites the tart retort that, were Wyndham a supermarket, leaving so many banana peels all over the place that 619,000 customers fall hardly suggests it should be immune from liability under § 45(a). The Court was also not persuaded by Wyndham’s argument that even if cybersecurity was covered by § 45(a) as initially enacted, subsequent legislative acts have reshaped the provision’s meaning to exclude cybersecurity.

As to fair notice, the Court rejected Wyndham’s assertion that the FTC failed to give Wyndham adequate notice of the specific cybersecurity standards that Wyndham was required to follow. Wyndham had contended that, based on principles of agency statutory interpretation, it was entitled to “ascertainable certainty” of the FTC’s interpretation of what specific cybersecurity practices are required by § 45(a). But based on Wyndham’s own assertions that the FTC had not actually decided that unreasonable cybersecurity practices qualify as “unfair” trade practices under the FTC Act, the Court reframed Wyndham’s position as asking “not whether Wyndham had fair notice of the FTC’s interpretation of the statute,” but rather “whether Wyndham had fair notice of what the statute itself requires.” The Court determined that Wyndham was “only entitled to notice of the meaning of the statute and not to the agency’s interpretation of the statute.”

The Court further rejected Wyndham’s argument that it lacked notice of what specific cybersecurity practices were necessary to avoid liability. While recognizing that the language of § 45(n) was “far from precise” and could result in some “borderline cases,” the Court stated that the relevant inquiry was a “cost-benefit analysis” that required consideration of a number of factors, “including the probability and expected size of reasonably unavoidable harms to consumers given a certain level of cybersecurity and the costs to consumers that would arise from investment in stronger cybersecurity.” The Court held that Wyndham’s fair notice challenge fell short, given that the FTC’s complaint did not allege that Wyndham used weak firewalls, IP address restrictions, encryption software, and passwords. Instead, the FTC’s complaint was based on the absence of any firewall at critical network points, Wyndham’s failure to restrict specific IP addresses, its lack of any encryption for certain customer files, and its failure to require some users to change their default or factory-setting passwords. The Court found that given that Wyndham was hacked three times, “it should have been painfully

37 Id. at 246-47.
38 Id. at 247.
39 Id.
40 Id. at 249.
41 Id. at 252.
42 Id. at 249-54 (emphasis in original).
43 Id. at 255.
44 Id.
45 Id.
46 Id. at 256.
47 Id.
clear to Wyndham that a court could find its conduct failed the cost-benefit analysis.”48 In addition, the Court’s decision was reinforced by language regarding sound data security plans from the FTC Guidebook, as well as published FTC complaints and consent decrees from administrative cases that provided Wyndham notice of the FTC’s expectations with regard to cybersecurity.49

Following the Third Circuit’s decision, in December 2015, Wyndham settled with the FTC. Under the terms of the settlement, the company must establish a comprehensive information security program designed to protect cardholder data and is required to conduct annual information security audits that conform to the Payment Card Industry Data Security Standard and to maintain safeguards in connections to its franchisees’ servers. The settlement also requires that, in the event Wyndham suffers another data breach affecting more than 10,000 payment card numbers, it must obtain an assessment of the breach and provide that assessment to the FTC within 10 days. Wyndham’s obligations under the settlement continue for 20 years.50

B. The Spokeo Decision

On May 16, 2016, the U.S. Supreme Court decided Spokeo, Inc. v. Robins,51 a closely watched case by those who bring and defend consumer class actions—including those filed under privacy laws such as the Telephone Consumer Protection Act and the Fair Credit Reporting Act (FCRA). The Court vacated the decision of the Ninth Circuit and remanded to the Ninth Circuit to consider the “concrete-injury” requirement for standing under Article III of the Constitution.

The case arose after Spokeo, which operates an online search engine that people can use to search for information about other people, allegedly disseminated incorrect information about the plaintiff. Specifically, Spokeo disseminated information that the plaintiff was married, had children, was in his 50s, had a job, was relatively affluent, and held a graduate degree. In fact, none of these things were true and the reality, some might argue, actually made the plaintiff a less desirable job candidate, credit risk, etc.

Notwithstanding an apparent lack of actual damage, the plaintiff sued, alleging that Spokeo willfully violated the FCRA by publishing inaccurate information about him and that he was therefore entitled to either actual damages or statutory damages of $100 to $1,000 per violation (among other things). The district court dismissed the complaint, concluding that plaintiff had not suffered a sufficient injury in fact to satisfy the standing requirement of Article III of the Constitution. The Ninth Circuit then reversed on the theory that the plaintiff had adequately alleged standing because he alleged violations of his own statutory rights, and not just the statutory rights of others.

48 Id.

49 Id. at 256-57.


51 136 S. Ct. 1540, 194 L. Ed. 2d 635 (2016), as revised (May 24, 2016).
In an unsatisfying decision for those seeking a bright-line rule (and a reduction in the amount of class action litigation), the Supreme Court concluded that the Ninth Circuit’s standing analysis was incomplete, and accordingly vacated and remanded the case to the Ninth Circuit for further proceedings. However, in reaching this decision, it did shed some light on constitutional standing requirements. It explained that to show injury in fact, a plaintiff must show that he suffered a “concrete and particularized” invasion of a legally protected interest. The Court concluded that the Ninth Circuit addressed the requirement that injury be “particularized,” but not the additional requirement that injury be “concrete.”  

Plaintiff’s allegation that Spokeo violated his own statutory rights, and not just the statutory rights of other people, went to the particularization requirement. But concreteness is different. A concrete injury, the Court explained, “must actually exist” and must be “‘real,’ and not ‘abstract’” (though it can be intangible). “[I]t is instructive to consider whether an alleged intangible harm has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts,” the Court said.

The Court also explained that Congress could “elevate to the status of legally cognizable injuries concrete, de facto injuries that were previously inadequate in law.” But the Court clarified that a plaintiff would not necessarily satisfy the concreteness requirement whenever a statute grants a person a right to sue: a plaintiff must always show a concrete injury, even in the context of a statutory violation. In short, the Court concluded, Congress could not “erase Article III’s standing requirements by statutorily granting the right to sue to a plaintiff who would not otherwise have standing.”

As applied to the plaintiff in Spokeo, these rules meant that Congress could seek through the FCRA to curb the dissemination of false consumer information by adopting procedures designed to decrease that risk, but Robins could not satisfy the requirements of Article III simply by alleging a procedural violation.

III. RECENT INTERNATIONAL DEVELOPMENTS

A. Introduction

Privacy laws are becoming ubiquitous globally. Some countries have general privacy laws and other counties have privacy laws covering particular parts of the private sector, such as e-commerce, credit reporting, health information, etc.

According to a privacy study in 2015, there are 109 general privacy laws in countries around the world, specifically: EU (28); Other European (25); Africa (17); 13 Asia (12); Latin America (10); Caribbean (7); Middle East (4); North America (2); Australasia (2); Central Asia (2); Pacific Islands (0).

---

52 *Id.* at 1549-50.
53 *Id.* at 1549.
54 *Id.* at 1549, 1548.
Non-European countries generally are adopting provisions that are similar to European privacy laws. Recent examples include Chile, South Africa and Thailand. In this sense, the European privacy model has become the leading privacy model in the world.

B. European Model

The European model is based on the OECD Privacy Principles as set out in the OECD Guidelines ("Guidelines") adopted in 1980. The Guidelines provide eight principles regarding the protection of privacy and trans-border flow of personal data. These are:

Collection Limitation Principle. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Data Quality Principle. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

Purpose Specification Principle. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation Principle. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except: (a) with the consent of the data subject; or (b) by the authority of law.

Security Safeguards Principle. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

Openness Principle. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Individual Participation Principle. An individual should have the right: (a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; (b) to have communicated to him, data relating to him (1) within a reasonable time; (2) at a charge, if any, that is not excessive; (3) in a reasonable manner; and (4) in a form that is readily intelligible to him; (c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and (d) to challenge data

---


relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

**Accountability Principle.** A data controller should be accountable for complying with measures which give effect to the principles stated above.\(^{58}\)

### C. United States Model

In sharp contrast to the European model, the privacy legislation in the United States may be described as using the “sectoral approach”. There is no general comprehensive federal law regulating the collection and use of personal data. Instead, there is a mix of federal laws, state laws, self-regulatory guidelines and guidelines developed by governmental agencies to protect privacy.

For example, on the federal level, the Federal Trade Commission Act\(^ {59}\) (the “FTC Act”) provides consumer protection provisions that prohibit practices that breach online and off-line privacy and data security policies. The Federal Trade Commission (FTC) is the chief federal agency on privacy policy and enforcement. The FTC is also the primary enforcer of the Children’s Online Privacy Protection Act (COPPA),\(^ {60}\) which applies to the online collection of information from children, and the Self-Regulatory Principles for Behavioral Advertising.

On the state level, for example, California was the first state to enact provisions on security breach notification.\(^ {61}\)

### D. Privacy laws in Some of Franchising’s Top Markets

In May of 2016 the U.S. Department of Commerce released a report on the top 12 markets for American franchisors.\(^ {62}\) These were, in order: Canada, Australia, The People’s Republic of China, Indonesia, South Africa, Mexico, India, Vietnam, Colombia, Brazil, Argentina, and the United Kingdom.\(^ {63}\)

To illustrate the effect of privacy issues on international expansion by U.S. franchisors, the privacy laws in the top four markets are summarized below.

---


\(^{60}\) Children’s Online Privacy Protection Act (COPPA ) (15 U.S.C. §§6501-6506)

\(^{61}\) California Civil Code §1798.82


\(^{63}\) Note that this was prior to the June 23, 2016 referendum on U.K. leaving the European Union, known as the “Brexit”.
1. Canada

   a. Laws – Federal

   The Personal Information Protection and Electronic Documents Act ("PIPEDA") is a general federal privacy law, based on the European model, which applies to the private-sector's collection, use and disclosure of personal information in the course of commercial activities across Canada.\textsuperscript{64} It was adopted in 2000 to facilitate trade with Europe by bringing Canada into line with the EU Data Protection Directive. However, due to the structure of Canada’s Constitution and the division of powers between the federal government and the provinces, the implementation of PIPEDA was delayed.

   In addition to the private sector, PIPEDA also applies to federal works, undertakings and businesses with respect to employee personal information.

   PIPEDA requires an organization to appoint an individual as privacy officer to be responsible for the organization's compliance. Organizations also are required to prepare a privacy policy setting out specific rules concerning the organization's collection, retention, use and disclosure of personal information.

   The Office of the Privacy Commissioner of Canada (OPC) is responsible for oversight of Part 1 of PIPEDA - Protection of Personal Information in the Private Sector.

   i. **Enforcement Tools under PIPEDA**

      Complaint

      Individuals, including non-residents of Canada, can file complaints concerning privacy breaches under PIPEDA to OPC. Resolution of a privacy dispute may be facilitated by an early resolution officer when the complaint involves issues that may easily be resolved. If a resolution is not reached, the privacy commissioner will conduct an investigation and issue a report of findings.

      Audit

      If OPC has reasonable ground to believe that an organization has contravened PIPEDA, OPC may initiate an audit regarding the personal information management practices of the organization.

      Public Interest Disclosure

      If OPC considers it in the public interest to do so, OPC may make public any information related to the personal information management practices of an organization. To date, this has been the main enforcement mechanism used by the OPC, and, thus, is the enforcement penalty that a franchisor is most likely to encounter based on a PIPEDA violation.

\textsuperscript{64} Personal Information Protection and Electronic Documents Act S.C. 2000, c. 5.
Applying to the Federal Court

The Federal Court in Canada has the authority to award damages and issue mandatory compliance orders. A complaint is initiated directly by the complainant and an application made to the Federal Court for a hearing. OPC also has independent authority to apply for a court hearing and has done so in a limited number of cases.

Canadian courts have demonstrated an increasing willingness to protect privacy interests. For example, in 2012, Ontario recognized the tort of invasion of privacy, also called “intrusion upon seclusion”.65

In addition to private actions and OPC enforcement actions, class action law suits concerning privacy breaches can also be brought in the courts. However, it is worth noting that in Canada, as a “meaningful screening device”66, class action law suits require court certification.

Disclosure of Offences

If the OPC believes there is evidence, OPC also may disclose to the federal or provincial Attorney General information relating to the commission of an offense of a federal or provincial law by an officer or employee of an organization.

b. Laws – Provincial

Some provinces have enacted privacy laws that are deemed substantially similar to PIPEDA by regulation or exemption order. If the privacy law violation takes place entirely within these provinces, the provincial law will apply instead of PIPEDA. Accordingly, for foreign franchise systems that operate in Canada, PIPEDA typically will be the relevant law, although as between the local franchisee in Canada and its customer, the provincial law typically will apply.

c. Canada’s anti-spam legislation:

Spam accounts for 97% of all messages received by business email servers. Many of the illicit emails concern the sale of counterfeit or illicit goods.67 In fact, virtually all spam comes from malware-infected computers and causes a huge strain on company resources leading to lost productivity.68 Over 30% of all spam passed along by hacked computers worldwide originates from the United States, South Korea, Brazil and India.69

Canada’s anti-spam legislation, also known as CASL, came into effect on July 1, 2014 and is intended to protect Canadians while ensuring that businesses can continue to compete in

65 Jones v Tsige, 2012 ONCA 32.
66 Pro-Sys Consultants Ltd. v. Microsoft Corp. 2013 SCC 57.
68 Ibid.
69 Ibid.
the global marketplace.\textsuperscript{70} CASL bans the most deceptive forms of spam – such as identity theft, phishing and spyware.\textsuperscript{71} CASL prohibits businesses from sending commercial electronic messages (CEMs) without the recipient's consent or permission, including messages to email addresses, social networking accounts, and text messages sent to a cell phone. CASL also provides rules regarding the unauthorized installation of software on a computer in Canada.

According to the Memorandum of Understanding for Cooperation, Coordination and Information Sharing published on October 22, 2013\textsuperscript{72}, there are three departments responsible for enforcing CASL- the competition Bureau of Canada, the Office of the Privacy Commissioner of Canada and the Canadian Radio-television and Telecommunications Commission (“CRTC”).

The CRTC has enacted the primary regulation under CASL and on June 19, 2014 published a guideline to help businesses develop corporate compliance programs (“Guideline”).\textsuperscript{73} The Guideline highlights the importance of a corporate compliance program generally, as well as key elements including the involving of senior management in privacy compliance, conducting risk assessment of business activities, developing a written corporate compliance policy, record keeping, providing training programs to staff, auditing and monitoring, and developing a complaint-handling system and an organizational disciplinary code to address contraventions.

i. CASL and Franchising:

Foreign franchisors sending CEMs to Canada must comply with CASL.\textsuperscript{74} It should be noted that e-mails sent between franchisors and franchisees are CEM as defined under CASL but are not prohibited by CASL.

In addition to ensuring compliance concerning the collection, retention and disclosure of personal information under privacy laws (PIPEDA and provincial laws), a franchisor should consider obtaining proper consents for subsequent commercial communications between the franchisor and customers.

ii. Implied consent and existing business relationship

\textsuperscript{70} An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act (S.C. 2010, c. 23) available at: http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/03643.html.

\textsuperscript{71} Drapeau W and Racicot, Federal Access to Information and Privacy Legislation Annotated 2016, Carswell Page 12-81.

\textsuperscript{72} Supra Note 68.


CASL recognizes two types of consent, implied and express, and provides that consent could be implied when the person who sends the messages, the person who causes the message to be sent or the person who permits the message to be sent, has an existing business relationship or an existing non-business relationship with the recipient.75

CASL defines “existing business relationship” as a business relationship between the person to whom the message is sent and any person who sent or caused or permitted the message to be sent arising from:

a. the purchase or lease of a product, goods, a service, land or an interest or right in land, within the two-year period immediately before the day on which the message was sent, by the person to whom the message is sent from any of those other persons;

b. the acceptance by the person to whom the message is sent, within the period referred to in paragraph (a), of a business, investment or gaming opportunity offered by any of those other persons;

c. the bartering of anything mentioned in paragraph (a) between the person to whom the message is sent and any of those other persons within the period referred to in that paragraph;

d. a written contract entered into between the person to whom the message is sent and any of those other persons in respect of a matter not referred to in any of paragraphs (a) to (c), if the contract is currently in existence or expired within the period referred to in paragraph (a); or

e. an inquiry or application, within the six-month period immediately before the day on which the respect of anything mentioned in any of paragraphs (a) to (c).76

CASL provides for a transition period that allows for implied consent to send CEMs for a period of three years from July 1, 2014 to July 1, 2017 where there is an existing business or non-business relationship that includes the communication of CEMs. 77 However, if a customer/receiver withdraws his/her consent during that period, the sending of CEMs is prohibited.

Furthermore, franchisors and franchisees should note that in order for the three-year transitioning period to apply, an existing business or non-business relationship should have been created before CASL came into force, that is, before July 1, 2014. Accordingly, reliance on the implied consent exemption by a franchisor or a franchisee is potentially risky.

Franchisors and franchisees also should note that if a franchisee has an existing business relationship with the customers under CASL, and the business is sold, the person who

75 Supra Note 68, Section 9(a).

76 Supra Note 68, Section 10(10).

77 Supra Note 68, Section 66.
purchases the business is considered to have, in respect of that business, an existing business relationship with the customers.78

Franchisors also should be advised that the existing business relationship exemption does not automatically extend a franchisee’s business relationship with its customer to the franchisor. In other words, a franchisor sending a promotional e-mail directly to a customer must have a previous independent direct relationship or explicit consent from the customer.

iii. **Express consent**

Typically a franchisee obtains consent from its customer to receive promotional emails. For an express consent to be effective for both the franchisor and the franchisee, the franchisee needs to not only identify itself as the information collector, but also must inform the customer that it is collecting information for the franchisor and that the franchisor also may send out CEMs.79

After the identification information is provided, the sender of CEMs, is required to ensure that its identification and contact information is valid for a minimum of 60 days after the message has been sent.

iv. **Unsubscribe Mechanism**

CASL also requires that CEMs provide an unsubscribe mechanism for recipients. The unsubscribe mechanism must enable the recipients to indicate, at no cost, that they wish to no longer receive CEMs or no longer wish to receive specified class of messages. The unsubscribe mechanism can be part of the same electronic means by which the message was sent, or it can be made available by other practicable electronic means.

The unsubscribe mechanism must also specify an electronic address that can be accessed by a web browser, or provide a link to an Internet page, that permits the recipient to unsubscribe to future CEMs. CASL further requires that CEM senders ensure that the unsubscribe messages are processed without delay, and no later than 10 business days after the unsubscribe message was sent. In 2015, Porter Airlines paid a $150,000 settlement for failure to honor CASL unsubscribe requirements.80

Beginning July 1, 2017, CASL permits individuals to file private and class action lawsuits to collect statutory damages.81 Franchise systems in Canada that use e-mail to communicate with customers should implement a compliance systems well before that deadline.

At the present time, CASL generally is enforced by undertakings and the issuance of notices of violation. Under CASL, CRTC has the ability to seek or impose administrative

---

78 Supra Note 70, Section 10(12).
79 Supra Note 70, Section 10(1)(b).
monetary penalties as an enforcement tool and is able to impose administrative monetary penalties for violations of up to $1 million per violation for individuals, and $10 million per violation for corporations.

d. **Private Right of Action**

The Canadian common law torts coined “intrusion upon seclusion” and “publicity given to private life” are still developing. A recent Federal Court of Appeal decision, which reversed a lower court class action certification, has provided some guidance as to the standards applicable to the tort of “publicity given to private life”.82 The court noted that the tort requires a breach, or publicity, of a broad scope, and not merely a disclosure to a small group. In addition, the torts of “intrusion upon seclusion” and “publicity given to private life” both require bad faith or reckless conduct. An isolated administrative error is insufficient. In addition, it is likely that the torts would not be found to be applicable unless the subject matter of the breach is of a kind that would be highly offensive to a reasonable person and not a matter of legitimate public concern.

2. **Australia**


a. **Law**

In Australia, the federal Privacy Act83 and its Australian Privacy Principles (APPs), which are contained in schedule 1 of the Privacy Act, apply to private sector entities and not-for-profit organizations with annual revenues of more than $3 million. In addition, some businesses with annual revenues of less than $3 million, such as private health service providers; businesses that sell or purchase personal information; credit reporting bodies; etc. also are covered under the Privacy Act.

Due to the exemption of smaller businesses from the scope of the Privacy Act, Australia has been deemed by the E.U. to not have a substantially similar privacy law regime.

The thirteen APPs contained in the Privacy Act are based on the European model. They are:

- Australian Privacy Principle 1—open and transparent management of personal information
- Australian Privacy Principle 2—anonymity and pseudonymity
- Australian Privacy Principle 3—collection of solicited personal information
- Australian Privacy Principle 4—dealing with unsolicited personal information
- Australian Privacy Principle 5—notification of the collection of personal information
- Australian Privacy Principle 6—use or disclosure of personal information

---


Australian Privacy Principle 7—direct marketing

Australian Privacy Principle 8—cross-border disclosure of personal information

Australian Privacy Principle 9—adoption, use or disclosure of government related identifiers

Australian Privacy Principle 10—quality of personal information

Australian Privacy Principle 11—security of personal information

Australian Privacy Principle 12—access to personal information

Australian Privacy Principle 13—correction of personal information

In Australia, organizations are required to appoint a privacy officer and prepare a privacy policy. As a result of the amendment of the Privacy Act to include the above privacy principles, and their application to the private sector, an organization should ensure that it has a data transfer agreement in place if it is likely to disclose personal information to overseas recipients.

b. Enforcement

The Office of the Australian Information Commissioner (OAIC) has the authority to investigate privacy complaints under Privacy Act 1988. Individuals initially should direct complaints to the infringing organization and allow 30 days for the organization to respond. If the organization fails to respond or provides an unsatisfactory response, the complainant can then make a complaint to the OAIC.

c. Private Right of Action

In addition to being able to potentially obtain relief under the Privacy Act, a private right of action for privacy breaches may soon exist under Australian law. The Australian Law Reform Commission (“ALRC”) has recommended that breach of privacy to be recognized as a cause of action by the courts. In September 2014, the ALRC issued a report called “Serious Invasions of Privacy in the Digital Era.” The report proposed a statutory cause of action for serious invasions of privacy. However, to date, legislation specifically creating such a cause of action has not yet been introduced in Australia at the federal level.

At the state level, the New South Wales Legislative Council Standing Committee on Law and Justice (“Standing Committee”) released a report on March 3, 2016 that recommended


that any statutory cause of action established by the New South Wales government concerning privacy be based on the model outlined in ALRC’s 2014 report. The Standing Committee also recommended that a fault by governments and corporations should be included in the statutory cause of action, while limiting the fault element for natural persons.

The Standing Committee supported the ALRC’s recommendation that available remedies include:

i. compensatory damages, including damages for the plaintiff’s emotional distress;
ii. exemplary damages where exceptional circumstances have been proven;
iii. account of profits;
iv. injunction; and
v. an enforceable undertaking (including a public apology).

In addition, the South Australian Law Reform Institute issued its report in March 2016 titled “A statutory tort for invasion of privacy”89 in which it recommended that a statutory cause of action for serious invasions of privacy be created in South Australia.

Although some courts in Australia have recognized privacy breach as a tort90, it is still unclear at the present time if a general tort of invasion of privacy law exists under Australian law.

ALRC has also recommended that the Privacy Act be amended to include mandatory breach notification requirements. In December 2015, the Australian Government issued a discussion paper regarding mandatory data breach notification and asked for consultation.91 Once the motion is passed, the number of class actions brought in Australia regarding privacy breach may increase.

3. People’s Republic of China (“PRC”)

China was listed third among projected franchise markets on the 2016 Franchising Top Markets Report prepared by the U.S Department of Commerce.

a. Regulatory

There is no general privacy law in the PRC on either the national or provincial levels. A draft national law based on the European model has been in preparation for a number of years. But in 2011 a dispute between major internet companies led to the speedy adoption of a number of sectoral privacy regulations focusing on online behavior and e-commerce.

i. 2013 MIIT Guideline

---


In 2013, the Ministry of Industry and Information Technology ("MIIT") released Information Security Technology - Guideline for Personal Information Protection within Public and Commercial Services Information Systems (the “Guideline”). The Guideline provides the protection of personal information stored in computer information systems including mobile communications terminals and networks in the private-sector. The Guideline also sets out 8 basic principles for the handling of personal information by personal information administrators in China. They are:

1) Clear purpose principle – “handle personal information with certain, clear and reasonable purposes, do not expand the scope of uses and not change the purpose of handling personal information without the knowledge of the subject of personal information.”
2) Minimum & sufficiency principle – “only handle the minimal information that is relevant to the purpose of (information) handling. Once such a handling purpose is achieved, personal information should be deleted/removed in the shortest possible time period.”
3) Public notification principle – “In a clear, easily understandable and appropriate manner, truthfully inform the subject of personal information of the purpose of handling personal information, the scope of the collection and use of personal information, personal information protecting measures and other information.”
4) Personal consent principle – “before handling personal information, [a personal information administrator] shall obtain the consent from the subject of personal information.”
5) Quality assurance principle – “ensuring that the confidentiality, integrity and availability of personal information are all up to date.”
6) Safety guaranty principle – “Security measures are to be appropriate to ‘the likelihood and severity of damage’.”
7) Good faith fulfilling principle – This largely repeats principle 1 & 2 and the compliance with legal requirements as another requirement.
8) Clear responsibility principle – Requires clear definition of responsibilities, taking of appropriate measures, and recording processing so as to facilitate retrospective investigation.

While the principles are relatively broad and some terms are not defined, such as “express consent” or “implied consent,” the MIIT terms obviously are based on the main principles in the OECD Privacy Principles.


93 Article 1 “This Guidelines applies to all kinds of organizations and institutions other than the government agencies and other institutions which exercise public management responsibilities...” Article 3.1 defines Information system, Article 3.2 defines Personal information.  [Ibid].

94  [Ibid]. Article 3.4.

It is worth noting that the 2013 MIIT Guideline includes a data transfer rule that states that personal information cannot be transferred to a foreign individual or organization without consent.⁹⁶

ii. 2011 / 2012 MiIT Decision and Regulation

Prior to the Guideline, MiIT published two regulatory instruments: in 2012, the Decision of the Standing Committee of the National People’s Congress on Strengthening Internet Information Protection,⁹⁷ and in 2011 the Regulation on Standardizing Market Order for Inter Information Services.⁹⁸The two instruments were mainly focusing on the privacy protection that applies to Internet Information Service Providers, which was broadened by the 2013 Guideline.

iii. 2016 Cybersecurity Law

On July 5, 2016, the Standing Committee of the National People’s Congress of the People’s Republic of China (the “Standing committee of PRC”) published for comment the second draft of Cybersecurity Law (中华人民共和国网络安全法).⁹⁹ The deadline for receipt of comment on the Cybersecurity Law was August 4, 2016.

b. Practice tip

Privacy law in China is still developing. Foreign entities doing business in China should not only following the current Chinese privacy laws, but should also proactively consider and take steps to prevent the types of breaches commonly addressed in privacy laws in other developed countries that have not yet been specifically included into Chinese laws. Franchisors should also consider the personal information protection expectations of Chinese customers and be forward thinking on implementing steps to prevent possible privacy breaches.

4. Indonesia

Indonesia is the fourth country listed on the projected franchise markets list according to the U.S. Department of Commerce’s 2016 Franchising Top Markets Report.

Indonesia does not have a general privacy law but has enacted the Information and Electronic Transactions (“IET Law”) ¹⁰⁰ and formulated a regulation concerning Electronic Information Services.

⁹⁶ Article 5.4.5, supra note 81.
System and Transaction Operation (IET Regulation). The IET law and IET Regulation provide the framework for regulations governing privacy matters in Indonesia.

In addition, the Ministry of Communications and Informatics of the Republic Indonesia (MOCI) has proposed a draft ministerial Regulation on Data Protection and a draft Data Protection Law. The draft Data Protection Law also covers both electronic and non-electronic data and, thus, is broader in scope than the IET Law and the IET Regulation.

As of the time of writing, neither the draft Data Protection Law, nor the draft Regulation on Data Protection, has come into force.

5. Other countries

In Singapore, personal data is protected under the Personal Data Protection Act which was passed in 2012 and came into force on July 2, 2014. The Personal Data Protection Regulations also came into force in July 2014 and address the transfer of personal data outside Singapore. They require that transfers comply with the Act if the data is in transit or publicly available in Singapore, the transfer is necessary for a contract, or the transferring organization has obtained individual consent or is required to transfer the data pursuant to a law, contract, binding corporate rules, or other legally binding instrument. In April 2016, the Personal Data Protection Commission (“PDPC”) in Singapore published details of data enforcement actions taken against eleven companies and organizations including one action where a financial penalty of $50,000 was imposed on a karaoke chain company – K Box Entertainment Group. PDPC has also issued an Advisory Guideline on Enforcement of the Data Protection Provision.

Brazil does not yet have a general law for the protection of personal information. However, a draft bill for the Protection of Personal Data has been proposed by the Ministry of

---


103 Personal Data Protection Regulations 2014.


Justice of Brazil. The *Marco Civil Da Internet* came into effect in 2014 and constitutes privacy regulation, but is limited to protection of privacy on the Internet (Guideline).\(^{106}\)

**E. Developments in the European Union**

**Safe Harbor Gives Way to Privacy Shield**

In October 2015, the Court of Justice of the European Union ("CJEU") issued a landmark judgment in *Schrems v Data Protection Commissioner*.\(^{107}\) The CJEU’s decision invalidated the U.S. Federal Trade Commission’s Safe Harbor Framework. The decision has significant practical implications for some 4,000 U.S. companies that had self-certified and relied on the Safe Harbor scheme to transfer personal data from the EU to the United States.

In February 2016, several months after the *Schrems* decision, the U.S. Government and the European Commission (the EU's executive arm) announced a new scheme for data transfers: the EU-U.S. Privacy Shield ("Privacy Shield"). Although the Privacy Shield faced harsh criticism from the Article 29 Working Party\(^{108}\) and others, it was officially adopted in July 2016, opening the door for certifications by U.S. companies as early as August 1, 2016, and ending months of limbo for those seeking to transfer data across the Atlantic.

1. **Background on the Safe Harbor**

Under the European Union Data Protection Directive,\(^{109}\) personal data may only be transferred outside of the European Union to those countries that ensure an "adequate" level of protection of the data. While certain countries have been recognized as providing “adequate” levels of protection, the U.S. has not.

While both the EU and U.S. provide extensive protection for personal privacy, their approaches are very different. To bridge the gap, in the late 1990s, the U.S. Department of Commerce — in consultation with the European Commission (the EU's executive body) — developed the Safe Harbor framework to provide a method for U.S. companies to transfer personal data outside the European Union in a way that was consistent with the EU Data Protection Directive. In 2000, the EU Commission decided (in the "EU Safe Harbor Decision")\(^{110}\) that transferred data would be “adequately” safeguarded if a U.S. company undertook a self-certification process to comply with the Safe Harbor principles. Therefore, Safe Harbor was often a first choice option for U.S. companies.

Under Safe Harbor principles there have been three principal ways of ensuring “adequate” protection:

\(^{106}\) *Marco Civil Da Internet* Law No. 12,965.

\(^{107}\) Supra note 2.

\(^{108}\) The Article 29 Working Party is made up of a representative from the data protection authority of each EU Member State, the European Data Protection Supervisor and the European Commission.


\(^{110}\) Decision 2000/520.
a. Data transfer agreements incorporating standard contractual clauses mandated by the European Commission;
b. Binding Corporate Rules, a set of internal rules adopted by global companies to govern intra-group transfers between companies, which have been approved by European data protection authorities as offering an adequate level of protection for personal data;
c. Through the recipient’s Safe Harbor certification for transfers to the U.S.

As a result of the Schrems decision, the third option is no longer available. As for the fourth potential option, expressly obtaining the data subject’s consent, while a theoretical possibility, such consent is generally disfavored in situations involving systematic transfers of data. In addition, it is inadvisable for employers to rely solely on an employee’s consent to transfer personal data outside the EU because the unequal bargaining power between employer and employee means the employee’s consent typically cannot be freely given and therefore is viewed with skepticism by EU authorities.111 Finally, reliance upon consent as a transfer mechanism poses practical difficulties, as consent can be revoked.

2. Facts Giving Rise to Schrems

Like many U.S. corporations, Facebook, Inc. organizes its EU operations around its Irish subsidiary (“Facebook Ireland”). Facebook users in the EU enter into a contract with Facebook Ireland that permits personal data to be transferred for processing in the U.S. on the basis of the Safe Harbor principles.

In June 2013, following the Snowden revelations, an Austrian student, Max Schrems, requested that the Irish Data Protection Commissioner exercise statutory powers to prohibit the transfer by Facebook Ireland of his personal data to the U.S. — on the basis that U.S. law and practice did not ensure adequate protection against surveillance activities by public authorities. The Irish Data Protection Commissioner refused to intervene, asserting that the EU Safe Harbor Decision could not be overruled. Upon review, the Irish High Court referred the issue to the Court of Justice of the EU, which ensures that EU law is interpreted consistently in every EU member country.112

3. The Decision of the Court of Justice of the European Union

The CJEU held that the EU Safe Harbor Decision does not eliminate, or even reduce, the powers available to the national supervisory authorities, including the power to investigate the propriety of data transfers.113

Specifically, the CJEU found that, when looking at a claim brought by an individual, a national supervisory authority must be able to examine, with complete independence, whether

111 See, for example, the following documents issued by the Article 29 Data Protection Working Party: Opinion 8/2001 on the processing of personal data in the employment context (WP48, 5062/01/EN); Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995 (WP114, 2093/05/EN); and Opinion 15/2011 on the definition of consent (WP187, 01197/11/EN).


113 Maximilian Schrems v. Data Protection Commissioner, Case C-362/14, 6 October 2015.
the transfer of a person’s data to a third country complies with the Directive. In addition, the CJEU found that the EU Safe Harbor Decision was itself invalid.

The CJEU held that the EU Commission was required to assess whether the U.S. ensures, by reason of its domestic law or its international commitments, an adequate level of protection for privacy. In the CJEU’s view, the Commission did not make such a finding, but merely examined the Safe Harbor scheme.

In particular, the CJEU noted:

a. The Safe Harbor scheme only applies to U.S. companies which opt to comply with it; U.S. public authorities are not required to comply with Safe Harbor principles;

b. In case of any conflict between U.S. law and Safe Harbor principles, organizations must comply with U.S. law;

c. The Safe Harbor principles are subject to a broad derogation on the basis of national security, public interest or law enforcement requirements, which does not provide adequate protection for individuals’ fundamental privacy rights;

d. The EU Safe Harbor Decision does not refer to the existence of any rules intended to limit or protect against such interference;

e. There is nothing in the CJEU’s decision to indicate misuse by any of more than 4,000 companies that have signed up to the Safe Harbor principles. The decision relates solely to potential access by government bodies, which is usually outside of the control of commercial organizations.

4. Announcement of the Privacy Shield

Following the Schrems decision, the U.S. and EU governments faced significant pressure from companies that rely on international transfers of data to fix the problems with the Safe Harbor that the decision highlighted. That pressure increased substantially when EU data protection regulators issued a joint statement providing that if no appropriate solution was found by the end of January 2016, they would take action to coordinate all enforcement activities.

Thus, in early February 2016, the two governments announced the so-called Privacy Shield, which EU negotiators emphasized provides a very different level of protection than the Safe Harbor scheme adopted in 2000.

In particular, the Privacy Shield is intended to impose stronger obligations on the U.S. to protect personal data imported from the EU and provides for stronger monitoring and enforcement by the U.S. Department of Commerce and FTC, including through increased cooperation with European Data Protection Authorities.

According to the outline issued by the EU Commission at the time of announcement, the Privacy Shield would include:

a. Robust obligations for U.S. companies importing personal data with respect to how personal data is processed and individual rights are guaranteed;

b. Monitoring and enforcement of such commitments by the Department of Commerce which will be enforceable under U.S. law by the U.S. Federal Trade Commission;
c. Obligations to comply with decisions of European data protection regulators when importing human resources data from Europe;
d. Binding written assurances from the U.S. to the EU from the Office of the Director of National Intelligence that the access of public authorities for law enforcement and national security purposes will be subject to clear limitations, safeguards and oversight mechanisms;
e. An annual joint review by the European Commission and the U.S. Department of Commerce with input from national security experts from the U.S. and European Data Protection Authorities;
f. More effective redress mechanisms for individuals, and in particular:
   i. Strict deadlines will be imposed for companies to respond to complaints from data subjects;
   ii. European data protection authorities will be able to refer complaints from EU data subjects to the Department of Commerce and the Federal Trade Commission for resolution;
   iii. If such complaints are not resolved, there will be an arbitration mechanism;
   iv. A new Ombudsperson will be set up in the U.S. State Department to hear complaints on possible access by national intelligence authorities.

5. **Criticism of the Privacy Shield**

In April 2016, shortly after the announcement of the Privacy Shield, the Article 29 Working Party issued a non-binding opinion acknowledging that the Privacy Shield improves upon the Safe Harbor scheme but stressing that the new framework was complex and lacked clarity. In addition, the Working Party expressed concerns regarding whether the Privacy Shield would ensure a level of protection equivalent to that in the EU. In particular, the Working Party identified issues relating to data retention, purpose limitation, onward transfers, and EU individuals’ right of redress.

The Working Party also expressed concerns about the sort of government surveillance that gave rise to the Schrems decision. In particular, it pointed out that the Privacy Shield did not fully exclude the possibility of massive and indiscriminate collection of personal data originating from the EU by the U.S. authorities. The Working Party further observed that while the establishment of an Ombudsman was helpful, it was not clear whether the Ombudsman would have adequate powers to be effective. The Working Party implicitly acknowledged that government surveillance is something over which the companies that had relied on the Safe Harbor (and would be relying on the Privacy Shield) have little, if any control.

Others, including the European Parliament and the European Data Protection Supervisor have also criticized the Privacy Shield. Nevertheless, on July 8, 2016, EU representatives on the Article 31 Committee approved the final version of the Privacy Shield, and it was official approved on July 12, 2016. The U.S. Department of Commerce began accepting certification forms on August 1, 2016.

Companies already “Safe Harbor certified” likely will not find it overly difficult to comply with the new Privacy Shield principles. Although there are significant changes to the notice and onward transfer principles, most of these can be addressed by updates to company privacy policies and by revisiting agreements with vendors and ramping up, where necessary, data protection language therein. Tweaks to other principles were even more modest. Not
surprisingly, given the reasons for the invalidation of the Safe Harbor, many of the new protections embraced by the Privacy Shield relate to government surveillance and principle enforcement (which may be beyond the control of most companies seeking certification).

The Privacy Shield’s longevity is yet to be determined. It likely will face challenges from individuals such as Schrems and possibly from the Article 29 Working Party and others. In addition, in May 2018, when the General Data Protection Regulation (discussed below) goes into effect, further revisions to the Privacy Shield may be necessary. For now, however, the Privacy Shield provides a welcome reprieve to those companies eager to legitimize transfers of data from the EU to the U.S.

6. Adoption of General Data Protection Regulation

The General Data Protection Regulation (“GDPR”) \(^{114}\) was adopted by the European Parliament on April 14, 2016, and the final draft was signed on April 27, 2016. Its provisions will directly apply in all EU Member States on May 25, 2018.

The GDPR was drafted and negotiated over the course of four years and was one of the most heavily lobbied pieces of European legislation ever (with nearly 4,000 amendments). The GDPR will replace the existing 1995 Data Protection Directive (which required member states to adopt their own data privacy laws consistent with the Directive) and will increase the harmonization of data privacy laws across the member states.

The GDPR will also greatly expand the territorial reach of European data privacy laws. It will apply not only to companies established in the European Union but also to data controllers and processors based outside of the European Union that either offer goods or services to EU data subjects (whether for payment or for free) or monitor the behavior of EU data subjects (regarding the activities of data subjects within the EU). Penalties for violating the GDPR are potentially severe and include, for the most serious breaches, the greater of up to €10m or 4 percent of worldwide revenues.

The GDPR not only expands the territorial reach of EU data privacy law, it also creates new rights and imposes new obligations and will require many companies to adopt new internal policies and procedures. This section provides a brief overview of some of the most significant implications of the GDPR.

7. New rights

Among the rights created or enhanced by the GDPR is the “right of erasure,” a derivative of the so-called “right to be forgotten.” The GDPR codifies a right to request deletion of personal data where (1) the data is no longer necessary for the purpose for which it was collected or processed, (2) the individual withdraws consent, (3) there are no overriding legitimate grounds for retention, or (4) the data is otherwise unlawfully processed. The right of erasure/right to be forgotten makes allowances for freedom of expression and the retention of information for compliance with legal obligations, public interest tasks, and research and statistics. However, demands made pursuant to the right to are subject to a balancing test and will have to be assessed on a case-by-case basis.

Another new right involves data portability. The GDPR gives data subjects the right to obtain from data controllers who process personal data through automated means a copy of all personal data that the controller processes. The data controller must provide the data in a commonly used electronic and structured format that permits further use by the data subject or a third-party. Supporting explanatory materials must also be provided if relevant. As a practical matter, companies may need to re-structure their systems so they are able to comply with data portability requests. However, the right to data portability applies only when processing was originally based on a user's consent or on a contract.

Yet another new right is the right not to be subjected to “profiling.” Profiling is the automated processing of personal data to evaluate certain personal aspects relating to a natural person. Specific examples include analyzing or predicting aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements. Profiling is permitted when expressly authorized by law, carried out in the course of entering or performing a contract, or when the data subject has given his/her consent. Therefore, for example, franchisees operating automatic credit checks on customers or assessing employee performance purely on the basis of automatically collected metrics will need to provide advance notice and obtain consent to such profiling.

8. New obligations

Among the new obligations imposed by the GDPR are enhanced consent requirements. Although the Directive allowed for implicit or even opt-out consent in certain situations, the GDPR requires that consent be freely given, specific, informed, and unambiguous and provided either by a statement or by clear affirmative action. Thus, for example, ticking a box may be sufficient, but silence or apparent acquiescence to a pre-ticked box is not. Controllers must be able to demonstrate that consent was validly obtained and, before obtaining consent, they must make clear to data subjects that they have a right to withdraw it. For sensitive data, consent must be more than unambiguous, it must be explicit, and a parent's consent is needed to process children’s personal data (unless otherwise provided by a member state law, the age of consent is 16 years).

Companies will want to revisit their privacy policies to comply with the new consent/disclosure requirements. Among other things, privacy policies should identify the data controller; the categories of personal data held; the intended terms of the processing, including the entities to which personal data will be disclose and whether the data will be transferred to a third country; the data retention period; the existence of automated decision-making; the existence of the rights, such as the right to be forgotten and the right to data portability, and the right to lodge a complaint with the national data protection authority.

Franchisors will need to clearly allocate responsibility for data privacy policy compliance in franchise agreements. While the Data Protection Directive imposes primary liability on data controllers, the GDPR also imposes significant obligations directly on data processors. Franchisors may therefore be liable for data processing carried out on behalf of franchisees, even though the franchisee may be primarily responsible for determining the purposes and means of collecting personal data and may, legally and in the minds of customers, be primarily liable for data privacy compliance. Determining the respective roles will be the key practical issue. Franchisor and franchisee may play different roles with respect to personal data at different stages in the business' operations. For example, customer data collected by a franchisee and sent for back office processing carried out by the franchisor on behalf of all franchisees might suggest that the franchisor is simply acting as a data processor. However, if
the same data is used by the franchisor for customer analytics or combination with other data, the franchisor may well be acting as a data controller, with more significant compliance obligations.

Another new obligation that will harmonize wide variances in national laws relates to data breach notification and requires data controllers to report a breach to supervisory authorities without undue delay and no later than 72 hours after discovery. Any notification after 72 hours must be accompanied by a reason for the delay. This timeframe is significantly shorter than that imposed by U.S. data breach notification laws, and companies should prepare by reviewing their internal procedures, designating internal roles, and training employees on breach response. It is also important for data controllers to ensure that their data processors report all security incidents so that the controller can notify the supervisory authorities.

Companies may also be required to appoint a data protection officer ("DPO"). A DPO is required when the core activities of the controller or processor involve regular and systematic monitoring of data subjects on a large scale or consist of processing on a large scale special categories of data, such as sensitive personal data or criminal offenses. The DPO must have expert knowledge of data protection laws and practices and must be allowed to operate independently and report to the highest management level. DPOs cannot be dismissed or penalized by the controller or processor for performing his tasks, making the job attractive for anyone who prioritizes job security.

9. **New processes**

Under the GDPR, data controllers and processors must maintain (and make available to supervisory authorities on request) internal records that cover all of their data processing activities including: the purposes of the processing activities, categories of personal data and data subjects, details of recipients of the data, data retention policies, and security measures.

In addition, the GDPR expects data protection to be incorporated into products and services by design and by default. This means that as companies design new technologies, filing systems, and business model, they must be designed to limit the processing of data to that which is necessary to achieve the purpose for which it was collected and that default choices must minimize data collection. Access to personal data should be given only to those who need it within the organization. Companies will want to consider privacy implications at the inception of new products and services, for example franchise customer loyalty apps which capture geolocation. The GDPR does allow for a risk-based approach that allows consideration of the cost of implementation and the nature of the processing.

Anonymized data is not within the scope of the GDPR but pseudonymized data — data that cannot be attributed to a specific data subject without the use of additional information — must be kept separately and subjected to technical and organizational measures to ensure the personal data are not attributable to an identified or identifiable natural person.

Finally, data controllers will find it necessary to “up their game” in appointing data processors, as the GDPR expects them to select processors who offer adequate safeguards and enter into a written contract setting out the relationship. Processors who breach the written agreement may be held to be acting as a data controller. Processor contracts should make clear that the processor must act only on the documented instructions of the controller, ensure appropriate confidentiality of employees, take appropriate security measures and assist with security reporting obligations, delete or return all the personal data to the controller at the end of
the provision of services, and make available all information necessary to demonstrate compliance with the obligations on processors. As noted above, franchise agreements will need to allocate clearly the respective roles of franchisor and franchisee with respect to the processing of customer personal data.

F. Data localization

In addition to the effect on European privacy laws, the revelations of Edward Snowden have also lead to the development internationally of “data localization” laws and regulations. Data localization requires the retention of data collected or generated through the internet, i.e. the server, to be physically located at the jurisdiction where the data originated. Countries around the world have gradually started to implement data localization requirements in order to add another layer of privacy protection.

In Europe, countries such as Germany, Russia and Greece has data localization requirements.

In Russia, for example, the new rule on data localization was implemented on September 1, 2015. The data localization rule requires that the personal data of Russian citizens be processed via servers located within the territory of Russia. The data localization rule has been interpreted to apply to a foreign entity even if that entity has no physical establishment in Russia. This does not mean that personal data of Russian nationals can no longer be transferred abroad, but only means that the “primary” or “entry-level” should be inside Russia. Data transfer abroad will then be subject to compliance with Russian data cross-border transfer rules. On January 13, 2016, the Russian data protection regulator released a detailed plan, approved in December 2015, concerning data localization compliance audits schedule for later this year.

In in response to the October 2015 collapse of the EU-U.S. Safe Harbor Agreement many U.S. companies established EU-based data centers to process the information collected from EU citizens.

In Asia, counties such as Taiwan, Vietnam, Indonesia and Malaysia have rules on data localization. Australia has data localization requirement for health records and Brazil has the law – Marco Civil da Internet to protect the rights of Internet users.

China does not yet have a comprehensive law regulating cross-border transfer of information or data localization. Article 31 of the draft Cybersecurity Law, which passed second reading on June 27, 2016, provides that key information infrastructure operators should retain the personal information within China. In other words, this rule may not affect most of the franchisors doing private business in China. But it should be noted that there are some

---

115 The data localization law, Federal Law No. 242-FZ.
117 Supra Note 103.
118 Supra Note 97.
prohibitions on cross-border data transfer within certain industries in China. Franchisors entering into China should evaluate national rules and be prepared to conduct data segregation.

Interestingly, the Trans-Pacific Partnership (“TPP”) intends to prevent data localization in international business. The TPP text, released on January 2016 in Auckland, New Zealand, sets out the prohibition of data localization.\textsuperscript{119} Article 14.13 of TPP provides that subject to some exceptions, TPP prevents using data localization as a prerequisite for conducting business.\textsuperscript{120} TPP participating countries include the United States, Canada, Japan, Singapore, Australia, etc. While from a business aspect TPP provides greater opportunities for U.S. franchises to export their concepts,\textsuperscript{121} privacy concern under TPP should not be ignored.

G. Payment security standards

The Payment Card Industry Data Security Standard (“PCI”) provides a set of security standards to ensure that all companies accept, transmit, and retain cardholder’s data properly.\textsuperscript{122} In other words, any business that involves the transmission, process and retention of payment card data must comply with PCI standards.\textsuperscript{123} The PCI was launched in 2006 and has been having significant impact on payment security in all kinds of industry globally.

PCI is managed by the Payment Card Industry Security Standards Council\textsuperscript{124} and enforced by five payment card brands: Visa, MasterCard, American Express, JCB International and Discover. Under PCI rules, all businesses will fall into one of the four merchant levels according to the volume of transaction. Different levels of merchants must take different steps to satisfy PCI requirements.

Failure to comply with PCI standards can result in penalties. Such penalties are contractual and are not subject to proof of actual damage to a cardholder.\textsuperscript{125}

To mitigate the risks of privacy breaches, franchisors should encourage franchisees to achieve PCI compliance and discourage franchisees from delaying action. Although providing advice and guidance to franchisees concerning the compliance process entails some vicarious liability risk for the franchisor, it may be a greater risk to leave franchisees to fend for themselves. Franchisors should consider mandating PCI compliance by franchisees and clearly

\begin{itemize}
\item \textsuperscript{119} Text of Trans-Pacific Partnership \url{https://www.mfat.govt.nz/en/about-us/who-we-are/treaty-making-process/trans-pacific-partnership-tpp/text-of-the-trans-pacific-partnership/}.
\item \textsuperscript{120} Article 14.13 of the text of Trans-Pacific Partnership. \url{https://www.mfat.govt.nz/assets/_securedfiles/Trans-Pacific-Partnership/Text/14._Electronic-Commerce-Chapter.pdf}.
\item \textsuperscript{122} Payment Card Industry Security Standards. Available at: \url{https://www.pcisecuritystandards.org/pci_security/maintaining_payment_security}.
\item \textsuperscript{123} PCI Compliance Guide. Available at: \url{https://www.pcicomplianceguide.org/pci-faqs-2/#2}.
\item \textsuperscript{124} Payment Card Industry Security Standards Council. See at: \url{https://www.pcisecuritystandards.org/}.
\item \textsuperscript{125} \textit{Aldo Grp. Inc. v. Chubb Ins. Co. of Canada}, 2016 QCCA 554.
\end{itemize}
set out provisions regarding the franchisee’s responsibility to comply with PCI rules either in the franchise agreement or in a separate operations manual.

IV. Risk Assessment and Compliance Planning

Over the last decade, the focus of risk assessment with respect to compliance with privacy laws and data protection has shifted from an emphasis on obtaining appropriate consent for the collection, use and disclosure of information to implementation of security methods to protect the personal information stored on IT systems, and the prevention of and handling of data security breaches that could result in theft of the personal information.

The Wyndham case illustrates this well. The FTC’s concerns did not emanate from Wyndham’s use of customer personal information required for payment, but rather arose from the failure of Wyndham and its franchisees to adequately secure the personal information.

Non-compliance with privacy laws creates at least four types of risks:

1. Government action against the franchisor and/or its franchisees that results in compliance orders and/or fines;
2. Class action litigation that may result in an expensive settlement;
3. Claims for damages from credit card companies, banks and other participants in the electronic payment systems based expenses they had to incur as a result of a data security breach; and
4. Loss of sales and goodwill associated with negative publicity surrounding a data security breach affecting the system.

In the Wyndham case, no fine was imposed. However, Wyndham was required to establish a “comprehensive information security program” and conduct annual audits. With respect to franchisees, the settlement with the FTC requires Wyndham to:

- certify which franchisee networks were “untrusted” and need improvement to prevent future hackers from using the same method used in the company’s prior breaches;
- certify the extent of compliance with a formal risk assessment processes that will analyze the possible data security risks faced by the company; and
- certify that the auditor is qualified, independent and free from conflicts of interest.

Under the settlement, these requirements will remain in place for 20 years.

Perhaps the most significant requirement of the settlement is that Wyndham must annually obtain a third party assessment of it level of compliance with approved standards. According to the settlement, the third party assessor must:

- certify individually, as to each Wyndham-branded Hotel [independently owned managed or franchised hotel], whether Hotels and Resorts [the franchisor] treats

---

as an untrusted network any Wyndham-branded Hotel’s network that has a Cardholder Data Environment. 127

Essentially the FTC has mandated through the courts that the franchisor must audit the franchisees’ credit card payment systems and report the findings to the FTC for the next 20 years. The Wyndham settlement begs the question: “Why wasn’t the franchisor already monitoring the franchise systems levels of data security compliance? The potential problem for franchisors with respect to privacy compliance by franchisees was described in a 2004 ABA Forum on Franchising publication as follows:

“The most fundamental decision to be made by a franchisor in implementing a privacy compliance program is the decision about the breadth of the program. Will there be one privacy policy and compliance program for the franchise system (that is including franchisees) or will the franchisor’s privacy policy and compliance program be mandatory only for the franchisor, and franchisees will only be required to comply with the relevant privacy law. And if the privacy policy is system wide, will it be for customers only, or also for employees? In making these choices the franchisor will have to take into account the degree to which privacy is relevant to the customer satisfaction associated with brand, and the risk of the assumption of liability for non-compliance with the privacy policy by a franchisee. If a privacy policy is system wide, who will respond in the event of a complaint, and how will the costs of a defense be allocated? These issues would preferably be worked out in advance.

As a formula for a franchisor wishing to undertake such an analysis, the process might be described as balancing (a) the marketing benefits likely to be derived from having a uniform system wide policy; against (b) the costs associated with implementing and policing a system wide policy; and (c) the risks of liability for franchisee conduct (vicarious liability) arising out of a system wide policy.” 128

The following part of this paper will consider the second and third parts of the equation, namely what is required to develop, implement and police a system wide policy, and how to assess the risks of franchisee conduct, particularly in light of the Wyndham case.

A. What Personal Information Does Your System Collect and Use?

Essentially franchisors need to conduct a privacy audit. Initially, this does not need to be a major undertaking. It simply requires an assessment of how the system operates, and what personal information is collected, used and disclosed.

For example, do the franchisees communicate with potential customers by e-mail or other forms of social media? Are payments made by credit card? Is personal information


128 Supra Note 55.
exchanged between individual franchisees and the franchisor and/or between franchisees themselves? Is any of this done internationally?

In the 2004 paper mentioned above, the authors suggested that the amount of personal information collected by a hamburger franchise might be limited and privacy would not be considered part of the service features of such a system.  

Things have changed. The hamburger is probably now purchased with a wave of a credit card over a terminal. In that instant significant personal financial information enters the franchisor’s system and is delivered to a third party supplier. And increasingly the personal financial information may cross a national boundary when doing so.

Most franchisors should know how their system operates to immediately identify areas where significant personal information is collected and used. However, the person tasked with the actual privacy audit should collect the following information:

1. The type of data being collected, such as payment information, customer preferences, or personal contact details.
2. The functional purpose within the organization for collecting the data.
3. Is any of the data from individuals under the age of majority in their jurisdiction?
4. Is any of the data from individuals in other countries?
5. Where physically (i.e. server address, laptops) and how (electronically, paper) is the data stored?
6. Is encryption used when transferring or storing the data?
7. Who within the organization is responsible for the data?
8. Is access to the data provided to third parties outside the organization, such as suppliers?
9. Is there a contract governing such third party access and requiring appropriate privacy protection?
10. What is the retention schedule (if any) applied to the data.

The responses to the privacy audit should provide some answers as to the extent and nature of the privacy non-compliance risk that must be managed. For example:

1. If the personal information is being collected in other countries, is your organization in compliance with the privacy laws in those countries, and who is responsible for monitoring privacy law developments in those countries?
2. If some of the personal information is being collected from persons under the age of majority, do you need to comply with COPPA?
3. Are there supplier standards, such as with respect to the processing of credit card payments that your organization has agreed to adhere to?

---

129 ibid.


131 Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle branded credit cards from the major card schemes including Visa, MasterCard, American Express, Discover, and JCB. The PCI Standard is mandated by the card brands and administered by the Payment
4. Based on the privacy cases in the relevant jurisdictions is any type of data that your organization has particularly subject to complaints and/or theft?132
5. Is any of the personal information that your organization collects considered particularly sensitive information in one of the jurisdictions that you operate?133
6. Is insurance available with respect to these risks?
7. Should encryption of some of the data be considered?

B. **What are the Damages in a Privacy Breach?**

1. **Private Actions by the Subjects of the Breach**

When assessing the risks associated with failure to comply with privacy laws, regulations and standards, one of the questions that needs to be considered is the damages that individuals whose personal information is leaked may suffer.

Plaintiffs in privacy actions have had difficulty proving that they suffered actual harm. For example on May 16, 2016 the U.S. Supreme Court ruled in *Spokeo, Inc. v Robins*134 that plaintiffs in a class action alleging a breach of the Fair Credit Reporting Act135 based on the sale of inaccurate personal information, must show more than just a violation of the statute in order to collect damages. They must be able to prove “injury in fact.”

On the other hand, the Court of the Appeals for the Seventh Circuit the month before had ruled that in the class action brought by a customer of P.F.Chang’s who was the victim of a data breach had suffered sufficient harm in that he had had incurred:

1. The increased risk of fraudulent credit- or debit- charges; and
2. The increased risk of identity theft.136

This followed the earlier 7th Circuit decision in *Remijas v. Neiman Marcus Grp., LLC*137 Where the Court held that the injuries associated with resolving fraudulent charges and protecting oneself against injury were sufficient to grant standing. The question now is whether the decision in *Spokeo*, where the injuries claimed were potentially distinguishable, has effectively nullified these decisions recognizing standing in data breach cases.

---

132 The use of laptops loaded with personal information by employees outside the organization has proven to be particularly problematic. They are frequently lost or stolen for the value of the laptop rather than the data.

133 In the United States health information is considered to be particularly sensitive and is protected the Health Insurance Portability and Accountability Act of 1996 (HIPAA; Pub.L. 104–191, 110 Stat. 1936, enacted August 21, 1996). But the notion of sensitivity varies by culture, and in Europe the concept includes participation in political and other community organizations.


137 794 F.3d 688 (7th Cir. 2015).
In other jurisdictions, the courts have had similar difficulties in determining how to evaluate if a simple breach of privacy provides standing for a private right of action. Privacy developments in each relevant country need to be monitored to conduct a valid risk assessment.

2. **Obligations to the Banks and Insurance**

For P.F. Chang’s, the worst was yet to come. Banks protect credit card holders from fraudulent charges arising from theft of credit card information by providing reimbursement and issuing new cards.

The contractual obligations amongst the banks and the credit card company provide that the retailer’s bank is liable for the fraudulent charges, and the costs.\(^{138}\) In this case, there was about $1.7 million in fraudulent charges, and about $200,000 in notification, card replacement costs and administrative fees. In all the assessed liability that P.F. Chang’s had to its bank was $1.9 million.

P.F. Chang’s had a “CyberSecurity by Chubb Policy” that it claimed provided coverage for the data security breach. The insurer disagreed and a lawsuit followed. The Arizona District Court held based on the wording of the policy that the so-called “Privacy Injury” coverage actually only applied to cover damage incurred by the person whose data was illegally accessed, and did not cover damage directly incurred by P.F. Chang.

The Court also identified two policy exclusions that barred P.F. Chang’s claim for fraudulent charges and administrative costs. One exclusion precluded coverage for contractual liabilities that the retailer had assumed. P.F. Chang’s obligations to its bank under its Master Service Agreement were deemed to fall within this exclusion.

In addition, the Court rejected the P.F. Chang’s claims under the “reasonable expectations of privacy” doctrine.

This case emphasizes the need for franchisors to carefully evaluate the policy provisions and exclusions of the cyber insurance they plan to purchase, particularly with respect to obligations to franchisees.

Cyber coverage typically covers:

1. Information security and privacy (standard coverage for damages resulting from the unauthorized disclosure or theft of confidential information)

2. Breach response services (forensic computer experts, customer notification of breaches, attorneys retained to determine compliance with breach notice laws, public relations, and costs for credit monitoring)

3. Regulatory Defense and Penalties for violations of privacy laws

4. Business Interruption

5. Data Protection

6. Cyber Extortion

7. Breach Preparedness

PCI compliance is required by contract, not by regulation. In Canada, Aldo Group Inc. c. Chubb Insurance Company of Canada provides that the fines imposed by MasterCard are unrelated to any damages which may have been suffered by cardholders and that the $4.9 million in penalties assessed by MasterCard due to the cyber-attack was not covered under Aldo’s policy with its insurer.

When purchasing insurance, a franchisor should consider negotiating with its insurer to include coverage for penalties assessed due to the non-compliance with PCI standards which can be considerable.

3. Fines

In the Wyndham case no fines were levied. However, Wyndham does bear the cost of 20 years of third party compliance audits and reporting to the Federal Trade Commission.

Still the fines can be significant. The International Association of Privacy Professionals has on its web site a chart showing the top government imposed fines for privacy breaches worldwide.


<table>
<thead>
<tr>
<th>Rank/Fined entity</th>
<th>Amount of fines and penalties</th>
<th>Year</th>
<th>Country</th>
<th>Privacy principles violated</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Apple</td>
<td>$32.5M</td>
<td>2014</td>
<td>U.S.</td>
<td>Choice and Consent</td>
</tr>
<tr>
<td>2. Google</td>
<td>$22.5M</td>
<td>2012</td>
<td>U.S.</td>
<td>Collection</td>
</tr>
</tbody>
</table>

---


140 Aldo, 2016 QCCA 554.

141 Web Site: https://iapp.org/.

3. Google $17M 2013 U.S. Collection and Notice
5. Hewlitt-Packard $14.5M 2006 U.S. Collection
7. TJ Maxx $9.8M 2009 U.S. Security
8. Dish Network $6M 2009 U.S. Choice and Consent
9. DirecTV $5.3M 2005 U.S. Choice and Consent
10. HSBC $5M 2009 UK Security
12. Craftmatic $4.3 2007 U.S. Choice and Consent
15. Certegy Check Services $3.5M 2013 U.S. Accuracy
17. The Broadcast Team $2.8M 2007 U.S. Collection
18. Equifax, TransUnion and Experian $2.5M 2000 U.S. Access
19. CVS Caremark $2.3M 2009 U.S. Security and Disposal
The chart clearly demonstrates that fines associated with poor data security practices are something that a franchisor should be concerned about, especially in the United States. While the United States does not have the equivalent of a general privacy law with single specialized enforcers that potentially could serve to discourage privacy complaints, when privacy cases are enforced in the United States, the results are more likely to have serious consequences for the party that breached.\textsuperscript{143}

The \textit{Schrems} case\textsuperscript{144} referenced above led to the invalidation of the “Safe Harbor” framework developed by the U.S. Department of Commerce and the European Commission. This required U.S. companies doing business in Europe to develop another legal mechanism to transfer personal data from Europe to the United States. On June 16, 2016 the Hamburg State Data Protection Office announced that it had fined three multi-national corporations (two of which are based in the United States) a total of 28,000 Euros (about $32,000 USD) for continuing to rely on the Safe Harbor system to transfer personal data from Europe to the United States even after it was no longer applicable.\textsuperscript{145}

More importantly, going forward the E.U., as mentioned earlier, is in the process of updating its privacy regulations, moving from a “Directive” to a much greater level of harmonization and higher substantive legal standards under the General Data Protection Regulation.\textsuperscript{146} Not only has breach notification been added to the regulation, but the right to private actions and compensation against the individual company and the member state regulator have been expanded.\textsuperscript{147}

\begin{flushleft}

\textsuperscript{144} \textit{Supra} note 2.

\textsuperscript{145} Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, „Pressemittelungen: Unzulässige Datenübermittlungen in die USA“ (Hamburg Office for Data Protection and Freedom of Information, „Press Release: Illegal Data Transfers to the USA“), June 6, 2016, available online at (in German): https://www.datenschutz-hamburg.de/news/detail/article/unzulaessige-datenuebermittlungen-in-die-usa.html?tx_ttnews%5BbackPid%5D=170&cHash=d21026cc72d2a53525c7c40d6cbaa6e2; Fioretti, Julia, “German privacy regulator fines three firms over U.S. data transfers,” Reuters, June 6, 2016, available online (in English) at: http://www.reuters.com/article/us-germany-dataprotection-usa-idUSKCN0YS23H.


\textsuperscript{147} \textit{Ibid}, see Articles 78 to 84.
\end{flushleft}
4. **How to Comply**

a. **Appoint a Privacy Officer**

As the magnitude of the risks for non-compliance with the privacy laws and regulations increase, one of the more obvious actions a company can take is appoint a senior level executive to oversee compliance. In Canada the privacy laws require the appointment of a privacy officer, and one of the ways to quickly distinguish a compliant U.S. privacy policy from one that is non-compliant is to see if the privacy policy provides for a privacy officer.

In the E.U. privacy officers are known as Data Protection Officers (“Datenschutzbeauftragter” in German) and are mandated under the Federal Data Protection Law.\(^\text{148}\)

There are few guidelines concerning what qualifications a privacy officer should have. However, obvious qualifications would include significant experience with IT systems and data management, knowledge of the privacy laws and regulations, experience in training and in change management.

The person appointed as privacy officer should be responsible for assessing risks and determining what actions the franchisor should take to ensure that data security omissions by franchisees do not subject the franchise system to an FTC compliance order, as occurred with Wyndham.

b. **Prepare and Adopt a Privacy Policy**

What should a franchisor put in a privacy policy?

If the franchisor operates only in the United States, and in an unregulated sector,\(^\text{149}\) it has some leeway concerning the content of its privacy policy. However all other franchisors should reference the relevant laws, regulations, and guidelines promulgated by the enforcement authority in the jurisdictions in which it operates.

A U.S franchisor that operates only in the U.S. still may wish to consider implementing broad privacy protection in its system, and may, as a starting point, consult the privacy guidelines and policies of foreign jurisdictions where the franchisor may wish to expand in the future.

In Canada, one of the foreign countries where U.S.-based franchisors are most likely to expand, privacy policies should follow the general outline contained in the law that sets out the privacy principles. For reference they are:

**Principle 1 – Accountability**


\(^{149}\) Sectors that are regulated in the United States with respect to privacy include the financial sector (Gramm–Leach–Billey Act (GLBA), also known as the Financial Services Modernization Act of 1999), the health sector (Health Insurance Portability and Accountability Act of 1996), services for children under 13 (Children’s Online Privacy Protection Act of 1998), video rental (the Video Privacy Protection Act of 1988).
An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization’s compliance with the following principles.

**Principle 2 – Identifying Purposes**

The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

**Principle 3 – Consent**

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

**Principle 4 – Limiting Collection**

The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

**Principle 5 – Limiting Use, Disclosure, and Retention**

Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.

**Principle 6 – Accuracy**

Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

**Principle 7 – Safeguards**

Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

**Principle 8 – Openness**

An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

**Principle 9 – Individual Access**

Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.
Principle 10 – Challenging Compliance

An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization’s compliance.\(^{150}\)

The FTC Fair Information Practice Principles, namely *Notice, Choice, Access, and Security*,\(^{151}\) is an admirably succinct statement of the same ideas, but it would be more prudent to use a more comprehensive set of principles, especially if the franchise system operates outside of the United States.

Australia has a slightly different set of ten privacy principles,\(^{152}\) and the OECD has a set of eight principles that match the E.U. regulations.\(^{153}\)

It is important to use plain language in drafting a privacy policy, and to use what is called “layering” in setting out the principles when communicating with customers. An example of layering would be initially setting forth the general Canadian principles on a web site, with an invitation to the reader under each principle to click through to a more detailed description of the policy or the governing wording.

The policy should be regarded as a long-term relational contract, and should contain provisions for what happens to the personal information on the sale of the business, and for how changes to the privacy policy are introduced. The policy should also carry the date of its adoption.

Most importantly, the wording in the policy should track how personal information is actually handled by the entire franchise system, especially with regard to security. The draft policy should be evaluated against actual practices before being posted on the system web site.

c. Prepare for Breaches, and Breach Notification

While concept of privacy laws of general application emanates from Europe, the United States currently is a leader in privacy enforcement. In 2003 the California legislature enacted S.B. 1386, which requires any resident of California whose unencrypted personal information

\(^{150}\) As set out on the web site of the Office of the Privacy Commissioner of Canada, at: https://www.priv.gc.ca/leg_c/p_principle_e.asp.


\(^{153}\) The OECD Privacy Principles are part of the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, which was developed in the late 1970s and adopted in 1980. They are available online here: http://oecdprivacy.org/.
was, or is reasonably believed to have been, acquired by an unauthorized person to be notified.  

In the absence of a federal privacy law, the notification requirement has been adopted across the U.S. As of January, 2016 forty-seven out of the fifty states had adopted breach notification laws. The idea has also spread internationally, aided in part with the increased focus on security breaches with respect to payment systems, since they are the privacy issue most likely to directly affect individuals.

The elements typically include in such laws are:

1. Who must comply – a franchise system that holds personal information would usually qualify.

2. What constitutes personal information – is a business e-mail address personal information, even if it is available on a business related web site? Is a personal e-mail address personal information?

3. What constitutes a breach – So the data on a USB flash drive has been lost, does that mean that it has been acquired by an unauthorized person, or is it simply just lost?

4. Notice requirements – How soon must the individuals be notified that the USB flash drive has been lost? Precisely who must be notified?

5. Exemptions – if the data on the USB flash drive was encrypted, has there been a breach of security?

When drafting a response plan for a security breach it is very important to know the content of the laws and regulations in the jurisdictions in which the franchise system operates, or more narrowly, the jurisdictions from which personal information is collected and used.

Some regulations call for an assessment as to the real risk of significant harm arising from the breach. This, in turn, requires an assessment of the sensitivity of the personal information lost, and the probability that such personal information is being misused (as opposed to sitting on a USB flash drive that has been lost down between the cushions on a couch or car seat). There also may be requirements to report the breach to a government authority in addition to the affected individuals.

154 California S.B. 1386 was a bill passed by the California legislature that amended civil codes 1798.29, 1798.82 and 1798.84, the California law regulating the privacy of personal information. The text is available online at: http://www.leginfo.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.pdf.


156 In 2015 the Canadian Personal Information Protection and Electronic Documents Protection Act (PIPEDA) was amended by the Digital Privacy Act (S.C. 2015, c. 32, Assented to 2015-06-18) to include breach notification requirements.
V. CONCLUSION

The time when franchisors could afford to simply delegate privacy matters to their franchisees or local country master franchisees may be ending, at least with respect to electronic payment systems. Certainly the *Wyndham* case settlement has increased the risks and disadvantages of taking that course. In addition, recent developments confirm that data security, not the obtaining of appropriate consent, has become “the” privacy and data protection issue.

Because the United States remains an outlier in international privacy and data protection law, U.S. franchisors would be well advised to consider international models for privacy protection, even if international expansion has not become part of their business plan.
Paul Jones ● Principal ● Jones & Co.

Paul's practice is broadly focused on the national and international distribution of goods and services. Specifically he practices franchising, licensing, distribution, intellectual property, competition, e-commerce and privacy law.

Paul is familiar with both common law and civil law systems and jurisprudence. He has studied French, Spanish, German, Russian and Mandarin Chinese, and as required (and with some assistance) reads law in these languages.

Leita Walker ● Partner ● Faegre Baker Daniels LLP

Leita Walker is a member of the Faegre Baker Daniels intellectual property group. She splits her practice between dispute resolution and client counseling, focusing on three substantive areas: media, advertising and privacy law.

Leita's litigation experience includes litigating copyright and false advertising claims, defending libel and invasion of privacy lawsuits, and obtaining access to government records.

Outside the litigation context, Leita regularly counsels clients on the intersection of marketing initiatives and privacy laws, and is knowledgeable on the rules that govern social media and mobile marketing campaigns, online behavioral advertising, e-commerce, outsourcing, trans-border data flows, and security breaches. She routinely reviews and writes terms of use and privacy policies for the websites of major corporations and helps these clients understand and comply with the Digital Millennium Copyright Act, Communications Decency Act, TCPA, COPPA, FTC Act and CAN-SPAM Act.