American Bar Association
36th Annual Forum on Franchising

DATA PROTECTION AND PRIVACY IN FRANCHISING: WHO IS RESPONSIBLE?

Michael K. Lindsey
Paul Hastings LLP
Los Angeles, California

and

Mark S. Melodia
Reed Smith LLP
Princeton, New Jersey

October 16-18, 2013
Orlando, Florida

Table of Contents

Page

DATA PROTECTION AND PRIVACY IN FRANCHISING:

WHO IS RESPONSIBLE?[1]

I. INTRODUCTION

In the United States, improving the privacy and security of personal information has been established as a national priority. Yet the details of that national program remain very much in debate. This legal uncertainty and growing risk has profound implications for franchise systems and their counsel.

In 2012, when introducing the Department of Commerce's Consumer Privacy Bill of Rights, President Barack Obama noted:

> Americans have always cherished our privacy… Citizens who feel protected from misuse of their personal information feel free to engage in commerce, to participate in the political process or to seek needed health care. This is why we have laws that protect financial privacy and health privacy, and that protect consumers against unfair and deceptive uses of their information. This is why the Supreme Court has protected anonymous political speech, the same right exercised by the pamphleteers of the early Republic and today's bloggers. Never has privacy been more important than today, in the age of the Internet, the World Wide Web and smart phones.[2]

In 2013, in responding to revelations of the National Security Agency's domestic surveillance programs, the President remarked:

> You can't have 100 percent security and also then have 100 percent privacy and zero inconvenience. We're going to have to make some choices as a society.[3]

Regardless of one's opinions on the Commerce report or the NSA's programs, these statements demonstrate the constant tension at work between the legitimate interests of privacy, security and convenience. Consumers want their privacy to be respected, but also for companies to be able to quickly identify them and service them appropriately. Businesses are being pushed at the same time to be more transparent about the information they keep, but also to lock down that information with ever-greater security. As detailed below, the legal framework for privacy and security of personal information has become ever more complex, draconian and enforcement-minded.

Part II of this paper will detail how this developing area of law impacts the compliance risk and bottom line of franchisors, despite their traditional business-to-business role. Part II includes two case studies in which franchisors have been entangled in franchise-level privacy and/or data security controversies.

---

[1] The authors wish to thank Christine Nielsen, an associate in the Chicago office, and Paul Bond, a partner in the Princeton office, of Reed Smith LLP for their assistance in the preparation of this paper.

[2] U.S. Dep't of Commerce, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY, Introduction (Feb. 23, 2012), http://www.whitehouse.gov/sites/default/files/privacy-final.pdf (hereinafter, "Consumer Data Privacy Report").

[3] President Barack Obama, Statement by the President at the Fairmont Hotel, San Jose, California (June 7, 2013), http://www.whitehouse.gov/the-press-office/2013/06/07/statement-president.

Part III of this paper will explain, at a high level of detail, the legal landscape for privacy and data security in the United States. While a full treatment of this complex area is beyond the scope of this paper, our goal will be to help orient the franchisor to the dominant themes and controversies.

Part IV of this paper will provide more specific advice as to how franchisors can improve their own privacy and information security practices, and those of their franchisees.

II. WHY AM I, AS A FRANCHISOR, IN THE DATA PRIVACY AND SECURITY BUSINESS?

For the most part, the work of promoting personal information privacy and security has been imposed on corporate America. Businesses operating in the franchise form constitute an important part of the economy and, hence, an important part of the privacy and security effort. More than 453,000 businesses operate under a franchise model, with total sales of nearly $1.3 billion per year.[4] Franchised businesses employ nearly 8 million Americans, and account for almost 10% of private sector payroll.[5] Any national conversation on the treatment of personal information has to factor in the economic and business realities of this distribution model.

A question as basic as "Who is responsible for the vast amounts of personal information collected, stored, analyzed, shared, used and discarded through franchised businesses on a daily basis?" is not easily answered in the highly decentralized context of most franchise systems.

In its purest form, "[f]ranchising is a method of expanding a business by licensing independent business men and women to sell the franchisor's products or services or to follow a format and trade style created by the franchisor using the franchisor's trademarks, trade names and other intellectual property."[6] If the franchise relationship were simply a licensing of intellectual property, the franchisor would have very little to worry about with respect to the franchisee's day-to-day operations.

But the reality of a franchise relationship is not so simple. For example, the Federal Trade Commission defines the franchise relationship as involving, in part, an element of franchisor control. To be a franchise means, *inter alia*, that the franchisor "will exert or has the authority to exert a significant degree of control over the franchisee's method of operation, or provide significant assistance in the franchisee's method of operation."[7] State law is generally in accord that a franchise, by definition, includes a contractual requirement that a franchisee operate "under a marketing plan or system prescribed in substantial part by a franchisor."[8]

Privacy and data security concerns arise most directly where the franchisor is providing "significant control" and/or "significant assistance."[9] For example, franchisor control over site

---

[4] U.S. Census Bureau, U.S. Dep't of Commerce, 2007 ECONOMIC CENSUS FRANCHISE STATISTICS, *http://www.census.gov/econ/census/pdf/franchise_flyer.pdf*.
[5] *Id*.
[6] 1 GLADYS GLICKMAN, FRANCHISING §1.01 (2013).
[7] Disclosure Requirements and Prohibitions Concerning Franchising and Business Opportunity Ventures, 16 C.F.R. §463.1(h)(2)(2007).
[8] GLICKMAN, *supra* note 6, §2.02 n. 50 (2013)(surveying state laws on definition of franchise).
[9] FED. TRADE COMM'N, FRANCHISE RULE COMPLIANCE GUIDE 2-4 (May 2008), http://business.ftc.gov/documents/franchise-rule-compliance-guide.

design and operation can touch on issues of physical security of data. As employees are among the most frequent sources of data loss, theft or misuse, franchisor control over franchisee personnel policies and practices can impact administrative security. Franchisor control over franchisee participation in promotional campaigns may require the franchisor to make decisions about how and when to use customer data, and how and when to do outreach. Likewise, franchisor assistance to franchisees in the form of management of locations, personnel advice or training, providing operating manuals or centralized reservations or credit card systems can involve the franchisor in operational decisions about personal information.Whether couched as franchisor assistance or franchisor control, pervasive franchisor involvement in franchisee activity has been a traditional ground for plaintiffs to seek to hold franchisors liable for alleged franchise-level problems.[10]

To the extent that a franchise relationship vests in the franchisor contractual and/or practical control over franchise operations, plaintiffs may seek to impute legal liability for alleged data privacy and security issues at the franchise level to the franchisor. The most concrete example of potential franchisor liability to date is the Federal Trade Commission's suit against franchisor Wyndham, discussed in the case study below.

Also below is a case study in which the franchisor – Papa Johns International, which had no direct liability – undertook great expense to negotiate a legal settlement for a franchisee alleged to have violated a marketing privacy law. This second case study illustrates that aside from legal liability, franchisee-level privacy and security issues can present reputational or brand management risks for franchisors.

A. Case Study #1: FTC v. Wyndham Worldwide

In 2012, the FTC filed an action pursuant to its authority under Section 5 of the Federal Trade Commission Act[11] against Wyndham Worldwide Corporation ("Wyndham Worldwide"), Wyndham Hotel Group ("Hotel Group"), Wyndham Hotels and Resorts ("Hotels and Resorts") and Wyndham Hotel Management ("Hotel Management").[12] In its Complaint, the FTC alleged that Defendants':

> failure to maintain reasonable security allowed intruders to obtain unauthorized access to the computer networks of Wyndham Hotels and Resorts, LLC, and several hotels franchised and managed by Defendants on three separate occasions in less than two years. Defendants' security failures led to fraudulent charges on consumers' accounts, more than $10.6 million in fraud loss and the

[10] *See*, *e.g.*, *Goodyear Tire & Rubber Co. v. Washington*, 719 So. 2d 774, 777 (Ala. 1998)(affirming, in relevant part, decision that a Goodyear service outlet acted as an agent of the manufacturer Goodyear where there was evidence "(1) that Goodyear knowingly allowed and encouraged Tire Pro to use Goodyear signs and to sell Goodyear products; (2) that Goodyear knowingly allowed Tire Pro to represent to customers, through logos on its invoices, that it was a 'Goodyear Certified Auto Service' center; (3) that Goodyear's dealer sales manager testified that Goodyear intended for Tire Pro's customers to believe they were dealing with a Goodyear establishment; (4) that the tires sold to Washington's daughter were 'Goodyear Eagles'; and (5) that the repairs effected on Washington's daughter's car were performed by Tire Pro as a 'Goodyear Certified Auto Service" center'); *Nichols v. Arthur Murray, Inc.*, 248 Cal. App. 2d 610, 614 (Cal. App. 1967)(affirming trial court's determination that "[a] reading of the contract here involved leads me to conclude that rigid effective controls over almost every aspect of the operation were retained by the licensor to the extent that for all intents and purposes it should be regarded as the operator of the business").

[11] Federal Trade Commission Act, 15 U.S.C.A. § 45.

[12] *FTC v. Wyndham Worldwide Corp.*, Complaint for Injunctive and Equitable Relief, No. 2:12-cv-1365 (D. Ariz. August 9, 2012).

export of hundreds of thousands of consumers' payment card account information to a domain registered in Russia.[13]

The FTC's Complaint made specific allegations about the Defendants' control of franchise-level operations. For example, the FTC alleged:

- That the franchise agreements "require each Wyndham-branded hotel to purchase, and configure to their specifications, a designated computer system, known as a property management system;"[14]

- that these property management systems "store personal information about consumers, including names, addresses, email addresses, telephone numbers, payment card, account numbers, expiration dates and security codes;"[15]

- that all of these property management systems "are part of Hotels and Resorts' computer network, and are linked to its corporate network;"[16]

- that "[o]nly Defendants, and not the owners of the Wyndham-branded hotels, have administrator access that allows Defendants to control the property management systems at the hotels;"[17]

- that "Defendants set the rules, including all password requirements, that allow the Wyndham-branded hotels' employees to access their property management systems;"[18] and

- that for those hotels that Hotel Management directly operates under management agreements, Hotel Management controls "information technology and security functions and the hiring of employees to administer the hotels' computer networks."[19]

The FTC also cited to the privacy policy of the central reservation website allegedly operated by Hotel and Resorts as allegedly deceptive.[20]

The Defendants successfully transferred the case from the District of Arizona to the District of New Jersey,[21] and subsequently moved to dismiss the action. Defendants' motion asserted that the FTC does not have authority to prescribe or enforce data security standards; that it has not done so with sufficiently fair notice; that the FTC specifically has no enforcement authority with respect to the security of payment card information; and that, in any event, the Complaint (as amended) does not sufficiently allege any facts which would make plausible the Defendants' liabilities for franchisee-level failures. While, as of this writing, no decision has yet been made on the sufficiency of the FTC's Complaint, the case demonstrates the danger of franchisor liability in this uncertain area.

---

[13] *Id*. at ¶ 2.
[14] *Id*. at ¶ 15.
[15] *Id*.
[16] *Id*. at ¶ 16.
[17] *Id*. at ¶ 17.
[18] *Id*.
[19] *Id*. at ¶ 18.
[20] *Id*. at ¶ 20-21.
[21] Docketed at 2:13-cv-01887-ES-SCM.

B. Case Study #2: Papa John's

Even if a franchisor is not legally liable for a data privacy or security failure at the franchisee level, the risk of franchise bankruptcy may prompt the franchisor to volunteer and intervene.

In May 2010, a putative class action was filed against Papa John's International, as well as several Papa John's franchisees, for violations of the Telephone Consumer Protection Act ("TCPA") and the Washington Consumer Protection Act.[22] Statutory damages under the TCPA are $500 per violation, or $1,500 per willful violation.[23] The plaintiffs alleged that they had received commercial text messages sent from Papa John's without the recipient's prior express consent, actions that violate the TCPA and the state consumer protection law.[24] Plaintiffs argued that the franchisor and franchisees, as well as their third party vendor who actually sent the messages, acted in concert to approve, ratify and further direct the illegal marketing campaign.[25] Though the defendants argued, among other things, that the franchisor was not liable for the acts of the franchisee, the case dragged on for three years before settling. The nationwide litigation class that was certified in November 2012 included all persons who had received at least one unsolicited text message that marketed a Papa John's branded product, good or service.[26] The brand mattered – not an individual defendant's status as a franchisor or franchisee. In May 2013, the court approved a proposed class action settlement valued at $16.5 million.[27] The proposed settlement includes a free pizza coupon for all class members notified of the settlement and $50 for each class member who files a claim, as well as administrative costs and plaintiffs' attorneys' fees.[28]

The Papa John's plaintiffs arguably did not understand the difference between Papa John's the franchisor and each Papa John's franchisee. All plaintiffs apparently understood was that they received text messages advertising Papa John's pizza deals, and that was enough for them to try to pin liability on all named defendants. Statutory damages for TCPA violations add up quickly, as the calls or texts at issue can sometime be part of a large-scale marketing campaign. Even if a franchisor successfully shows that a franchisee engaged in its own marketing campaign without direction or authority from the franchisor, and the franchisor is thus not liable, the franchisor and brand can suffer. The franchisee may not be able to remain solvent when faced with statutory damages or a settlement. Public perception of the entity at "fault" may not change with a franchisor "win" in court – the public may still view the brand as having acted badly in the marketplace.

---

[22] *Agne v. Rock City Pizza, LLC*, Case No. 10-2-19384-1, Kings County Superior Court (WA)(May 28, 2010). The action was subsequently removed July 14, 2010. *Agne v. Rock City Pizza, LLC*, Case No. 2:10-cv-01139-JCC (W.D. Wash.)(hereinafter, "*Agne Docket*").
[23] Telephone Consumer Protection Act, 47 U.S.C. § 227(b)(3).
[24] *Agne Docket,* Docket Entry #2, Verification of State Court Records, Attachment #4, Complaint.
[25] *Id*.
[26] *Id.*, Docket Entry #366, Order Granting Motion for Class Certification (Nov. 9, 2012).
[27] *Id*., Docket Entry #371, Motion for Preliminary Approval of Class Action Settlement, p. 6 (May 17, 2013)
[28] *Id*.

III. WHAT IS THE LEGAL LANDSCAPE FOR PRIVACY AND SECURITY IN THE UNITED STATES?[29]

The Federal Trade Commission, in articulating privacy principles discussed in more detail below, found that "many consumers are concerned about the privacy of their personal information" but "generally lack full understanding of the nature and extent of this data collection and use."[30] Likewise, the Department of Commerce emphasized that "[p]rivacy protections are critical to maintaining consumer trust," but that "[n]either consumers nor companies have a clear set of ground rules to apply in the commercial arena."[31]

The general confusion is easy to understand. In the United States, there is no one law that governs the privacy and security of personal information. There is not even a single authority. Instead, there is a patchwork of laws, regulations, private contractual regimes, industry standards and common law obligations, none, some or all of which might apply to a given business activity. Those sources of obligation are almost always additive, and very rarely preemptive. That a particular action does not violate one standard usually is not determinative of whether the action passes muster under another standard.

For example, two of the most prescriptive federal laws of privacy and security are the Gramm-Leach Bliley Act ("GLBA") and the Health Insurance Portability and Accountability Act ("HIPAA"). Each federal standard provides that it does not preempt more stringent state law, barring a direct conflict making compliance with both federal and state law impossible.[32]

Because consumer privacy, at least in the abstract, is politically popular, these ad hoc standards seem likely to continue to multiply. Other than sector-specific regulators, the most important movers of this legal landscape for franchisors and franchisees to consider are:

- The Federal Trade Commission
- State Attorneys General
- Payment Card Industry Security Standards Council
- Private Class Action Attorneys

A. The Federal Trade Commission

For most United States businesses, for most purposes, the FTC is the primary federal authority for enforcement of privacy and data security requirements.

---

[29] The laws of nations other than the United States, such as the European Union's Data Protection Directive (95/46/EC), will not be discussed in this paper. Such laws can add significantly to the complexity of privacy and data security compliance.

[30] Fed. Trade Comm'n, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (March 2012) (hereinafter, "Final Report"), *http://ftc.gov/opa/2012/03/*privacy framework.shtm.

[31] Consumer Data Privacy Report, *supra* note 2, at Foreword.

[32] 15 U.S.C.A. § 6807(a)(providing preemption of state law "inconsistent with" GLBA) and (b)("For purposes of this section, a State statute, regulation, order, or interpretation is not inconsistent with the provisions of this subtitle if the protection such statute, regulation, order, or interpretation affords any person is greater than the protection provided under this subtitle"); 45 C.F.R. §160.203 (preempting state laws "inconsistent with" HIPAA, unless the state law is, for example, "more stringent").

The FTC is empowered and directed under Section 5 of the Federal Trade Commission Act to prevent persons from using "unfair" or "deceptive" acts or practices in or affecting commerce.[33] The FTC has several investigative powers at its disposal, including issuing subpoenas, civil investigative demands ("CIDs") and more informal inquiry letters. Following an investigation, the Commission may initiate an enforcement action if it has reason to believe that the law is being or has been violated. Unless the alleged violation contravenes a specific rule or a standing Consent Order, the FTC cannot impose a civil penalty.

Under the FTC Act, the FTC has authority to prescribe rules which define with specificity acts or practices which are unfair or deceptive acts or practices in or affecting commerce.[34] The Commission may commence a civil action, in federal district court, to recover a civil penalty against any person, partnership or corporation which violates any rule respecting unfair or deceptive acts or practices.

With respect to matters of privacy and data security, the FTC has interpreted its mandate as extending to situations where neither physical nor economic harm is at hand. In its Final Report, the Commission said it was willing to act whenever a company's practices "unexpectedly reveal previously private information *even absent physical or financial harm, or unwarranted intrusions*."[35] The division most active in enforcement of these standards is the Division of Privacy and Identity Protection in the FTC's Bureau of Consumer Protection.

The FTC has made extensive use of its Section 5 authority with respect to the privacy and security of consumer information. The primary record of this activity has been in Consent Orders that companies enter into to resolve FTC investigations.

For example, the FTC and responding companies entered into the following Consent Orders to resolve investigations concerning allegedly deceptive conduct. While the specifics differ from case to case, these examples show that any representation about privacy or security of consumer information can result in FTC attention:

- ***Guess?*** and ***Life is good, Inc***., in each case alleging that the payment card information collected on the company's respective website was not as secure as claimed by its online disclosures.[36]

- ***Toysmart***, which had promised in its privacy policy never to resell consumer information, but which attempted to sell its consumer database as a standalone asset in the context of its bankruptcy.[37]

- ***Google***, in connection with its Google Buzz program, for misrepresenting how registration information would be used, failing to adequately explain options for opting out and falsely claiming compliance with the European Union – United States Safe Harbor Program.[38]

---

[33] 15 USC § 45(a)(1), *et seq*.
[34] 15 USC §57a(a)(1)(B).
[35] Final Report, *supra* note 30, at 8 (emphasis added).
[36] *In The Matter of Guess?, Inc., and Guess.com, Inc*., Complaint and Decision and Order, FTC File No. 022 3260 (Jul. 30, 2003); *In the Matter of Life is good, Inc. and Life is good Retail, Inc.*, Complaint and Decision and Order, FTC Matter No. 072-3046 (Apr. 18, 2008).
[37] *FTC v. Toysmart.com, LLC*, Stipulated Consent Agreement and Final Order, No. 00-11341-RGS (D. Mass. Jul. 10, 2000).
[38] *In The Matter of Google, Inc*., Decision and Order, FTC File No. 10231236 (Oct. 13, 2011).

- ***Liberty Financial Companies***, following allegations that the company's website, which provided financial literacy information for young investors, claimed that information about minor users would be stored anonymously but actually keep identifying information.[39]

- ***GeoCities***, to resolve claims that it provided registration information about website users to third parties, including for marketing purposes, in contravention of its posted privacy policy.[40]

While any statement a company makes concerning privacy and data security can be held against that company by the FTC, the FTC has also prosecuted allegedly unfair practices even where the company has said nothing. For example:

- ***BJ's Wholesale Club***, alleging that the chain had failed to encrypt credit card information in transit throughout its stores, resulting in millions of dollars of credit card fraud.[41] While there was no allegation that the company had promised to encrypt the card information, the FTC stated that failure to do so was still unfair to consumers.

- ***DSW, Inc.***, for an alleged failure to adequately secure its database of payment card information from unauthorized access.[42] Again, there was no allegation that any consumer disclosure made by the retailer had been inaccurate or misleading.

In March 2012, the FTC issued its most comprehensive statement of policy yet in the privacy arena, its Final Report entitled "Protecting Consumer Privacy in an Era of Rapid Change."[43] The FTC emphasizes that the Final Report only sets forth industry best practices and was "not intended" to serve as a new template for enforcement. However, this line is not exactly clear, as the FTC identifies in the report existing law and enforcement actions that form the basis for its advice (and could be the basis for Section 5 enforcement actions).

In addition to providing a review of Commission action in these areas to date, the Final Report calls on companies to build in privacy protections – including data security, data minimization, focused data retention and data hygiene – at every stage in product development (from conceptualization to end-of-lifecycle). The Final Reports stresses that companies should give consumers the ability to make choices about their data collection and use "at a relevant time and context," including developing more automated choice functions such as a "Do Not Track" mechanism. The Final Report also states that companies should make their data practices more "consumer friendly" and accessible by streamlining privacy policies, providing consumers with access to data collected about them and engaging in consumer education campaigns to promote information-age literacy. Several of the Commission's more specific recommendations are detailed in Part IV below.

Perhaps the most remarkable statement in the Final Report is that the Commission intends to extend privacy protection to information which does not name a consumer or provide sufficient information to directly contact him or her. The framework applies to all businesses

[39] *In the Matter of Liberty Financial Companies, Inc*., Decision and Order, FTC File No. 982 3522 (Aug. 12, 1999).
[40] *In the Matter of Geocities*, Decision and Order, FTC File No. 982 3015 (Feb. 5, 1999).
[41] *In the Matter of BJ's Wholesale Club Inc*., Decision and Order, FTC File No. 0423160 (Sept. 20, 2005).
[42] *In the Matter of DSW, Inc*., Decision and Order, FTC File No. 052 3096 (Mar. 7, 2006).
[43] Final Report, *supra* note 30.

that collect or use consumer data that can be "reasonably linked to a specific consumer, computer or other device."[44] Thus, for example, if a franchisor develops and supports a mobile application by which its franchisees will connect with retail customers, and that mobile application collects the unique device identifier of the devices that use it, the FTC framework would apply. That would be the case even if the device never collects name, address, phone number or anything else traditionally considered personally identifiable information.

Of importance in this era of Big Data, the FTC even intends its guidance to apply to deidentified data sets if there is a prospect of reidentification. The FTC noted in its Final Report:

> There is significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead to identification of a consumer, computer or device even if the individual pieces of data do not constitute PII. Moreover, not only is it possible to re-identify non-PII data through various means, businesses have strong incentives to actually do so.[45]

In the Final Report, the FTC identified a number of areas as enforcement priorities in privacy and data security. In the time since March 2012, the FTC has sustained consistent focus on these areas, through enforcement actions, workshops and guidance to business. They include the privacy of information collected via mobile applications, improved disclosure of information sharing and enhancement and improving the ability of consumers to access and correct information held about them.

While the FTC's enforcement authority under the FTC Act is wide-ranging, the FTC also has specific authority in this area by means of other statutes. For example, the FTC has authority to interpret and enforce the Fair Credit Reporting Act ("FCRA"). The FCRA regulates the use of credit report information for credit and insurance eligibility decisions, and also in background checks and other investigative reports. One category of companies, called "consumer reporting agencies," is subject to especially burdensome obligations under the FCRA. While "consumer reporting agencies" was initially intended to refer most precisely to national brokers of consumer information such as Experian, Equifax and TransUnion, the FTC staff has recently taken an increasingly broad view of this definition. The FTC has, for example, pursued enforcement actions against companies which offered criminal background information or rental histories for sale.[46]

To the extent that franchisors support franchisees in collecting or analyzing information about individuals that will be used to determine whether or on what terms to provide credit, insurance or employment, franchisors must be aware of the potential application of the FCRA. Because the franchisees are independent businesses, if the franchisor shares information with them it may all the more easily fall into the definition of a consumer reporting agency and accrue the associated burdens.

While the FTC is the primary federal regulator for most businesses on most privacy and data security issues, it is by no means the only such regulator. Financial institutions have their own federal regulators on this issue, as do telecommunications companies, government

---

[44] Final Report, *supra* note 30, at p. 18.
[45] *Id*. at p. 20.
[46] *In the Matter of Filiquarian Publishing, LLC; Choice Level, LLC; and Joshua Linsk*, Decision and Order, FTC File No. 112 3195 (Apr. 30, 2013); and Press Release, Fed. Trade Comm'n, FTC Warns Data Brokers That Provide Tenant Rental Histories They May Be Subject to Fair Credit Reporting Act (Apr. 3, 2013), http://www.ftc.gov/opa/2013/04/tenant.shtm.

contractors, health care providers and insurance plans. Each, however, will articulate some variant on the same standards – in this context, what is deceptive to say or not say with respect to the company's treatment of individual information? What is unfair to do or not do? And, in each of these cases, the answers will tend to be highly context-specific.

B. State Attorneys General

Justice Louis Brandeis once noted:

> It is one of the happy incidents of the federal system that a single courageous state may, if its citizens choose, serve as a laboratory; and try novel social and economic experiments without risk to the rest of the country.[47]

But for companies attempting to comply with, or even understand, the legal requirements to protect the privacy and security of personal information, the multiplicity of state laws has been far from a happy incident.

State Attorneys General waded into the breach enforcement waters early on, after a security breach at the data broker ChoicePoint compromised Social Security numbers and consumer credit reports. ChoicePoint notified California residents who were affected by the breach, but did not intend to notify residents in other states because California was the only state in 2005 to have a law mandating such notification. In February 2005, nineteen Attorneys General sent a letter to ChoicePoint demanding notification to residents in their states. The Attorneys General then commenced an investigation, which culminated in a settlement agreement that was announced in May 2007.[48] The state settlement, which included injunctive relief and a civil penalty in the amount of $500,000, was in addition to an FTC settlement that included $5 million in consumer redress and a $10 million civil penalty for alleged violations of the FCRA.[49]

Since that time, there has been a rollout of security breach notification laws in state after state across the nation. At this time, 46 states and multiple other United States jurisdictions have laws requiring some form of notification after the loss, theft or misuse of certain types of personal information.[50] These laws share certain core characteristics, but differ from one another in material ways that make compliance in a breach situation complex. All, for example, consider social security numbers information within the scope of their concern, but some can also be triggered by other identifiers, such as tribal identification numbers, biometrics, mother's maiden name, etc. Some cover paper records, while many only relate to electronic records. Some require a risk of actual harm before compelling companies to send notices; some do not. Moreover, many of the statutes now require notice to specific state officials prior to, or at the same time as, notice is provided to the affected individuals. The states routinely follow up on these notices with additional questions, investigations or even enforcement actions.

But the states' role in this area is hardly limited to breaches. For example, Massachusetts issued "Standards for the Protection of Personal Information of Residents of the

---

[47] *New State Ice v. Liebmann*, 285 U.S. 262, 311 (1932)(Brandeis, J., dissenting).
[48] *See* Press Release, Illinois Attorney General, Attorney General Madigan Reaches Agreement With Choicepoint (May 31, 2007), http://www.illinoisattorneygeneral.gov/ pressroom/2007_05/20070531.html.
[49] *See* Press Release, Fed. Trade Comm'n, ChoicePoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress (January 26, 2006), http://www.ftc.gov/opa/2006/01/ choicepoint.shtm.
[50] *See* 1-22 BENDER ON PRIVACY AND DATA PROTECTION § 22.01 (2012).

Commonwealth."[51] This sweeping regulation on data security nominally applies to all companies that "own, license or maintain personal information about a resident of the Commonwealth."[52] The regulation requires all such companies to maintain a "comprehensive written information security policy," with certain specifically required elements, and to require by contract that all vendors who will obtain personal information about Massachusetts will do the same.[53] Because of the last of these requirements, the requirements of the Massachusetts regulation have "gone viral." Companies are requiring vendors to contractually agree to compliance and vendors are requiring it of subvendors, far beyond the borders of Massachusetts.

In addition to issues of security and breach, the States have been active in investigating and prosecuting perceived overreach with respect to collection or use of personal information. For example, California's Online Privacy Protection Act ("CalOPPA") requires companies to disclose their information-collection practices to California consumers. California Attorney General Kamala Harris has interpreted this act to apply not only to websites, but also mobile applications. On December 6, 2012, Attorney General Harris filed an action under California's Unfair Competition Law based upon the alleged failure of Delta Air Lines to comply with CalOPPA in providing a mobile application to the public.[54]

Delta was one of many entities that received a letter from the attorney general's office in late October 2012 notifying the company of non-compliance with CalOPPA. Attorney General Harris, asserting that Delta had not cured the legal deficiencies of its mobile application, sued the company two months later. The primary allegations are twofold. First, the complaint alleged that Delta's mobile application did not include a privacy policy, either available in the application itself, or available to review at the time of download from the application platform. In addition, though Delta had a privacy policy for its website, the complaint alleged that the website disclosure was insufficient to cover the mobile application. Critically, the complaint alleged that "while the privacy policy on Delta's website describes some of the PII collected on their website, Delta does not disclose anywhere several types of PII that the Fly Delta app collects, but the Delta website does not collect."[55]

In May 2013, Judge Marla Miller of the San Francisco Superior Court sided with Delta and sustained a demurrer to the complaint without leave to amend.[56] The court found that the claims against Delta were preempted by the Airline Deregulation Act and the court declined to rule on the arguments pertaining to the substantive reach of CalOPPA. Attorney General Harris declared that she was undeterred by the ruling and intended to continue to protect the California public from what she perceives as violative corporate practices.[57]

Separately, several States announced a settlement with Google for its collection of data through its Street View vehicles. On March 12, 2013, Connecticut Attorney General George

---

[51] *Standards for the Protection of Personal Information of Residents of the Commonwealth*, 201 CMR 17.00 *et seq*.
[52] 201 CMR 17.01(2).
[53] 201 CMR 17.03(1).
[54] *People v. Delta Air Lines Inc.,* No. CGC 12-526741, Cal. Super. Ct., San Francisco Cty. (Dec. 6, 2012).
[55] *Id*., Complaint at ¶ 17, http://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-files-suit-against-delta-airlines-failure.
[56] *Id*., Order Sustaining Defendant Delta Air Lines, Inc.'s Demurrer to Complaint (May 9, 2013).
[57] Erin Coe, *Calif. AG Poised To Ratchet Up Privacy Enforcement Efforts*, Law360 (May 20, 2013), http://www.law360.com/articles/443322/calif-ag-poised-to-ratchet-up-privacy-enforcement-efforts.

Jepsen announced a $7 million settlement with Google.[58] The investigation stemmed from the Street View vehicles' alleged collection of data over unsecured wireless connections as those vehicles drove from street to street snapping photos for the Google Street View website.

It is likely that the future will see additional enforcement actions by State Attorneys General in the privacy and data security arena. For example, the National Association of Attorneys General ("NAAG") adopted "Privacy in the Digital Age" as the organization's 2012–2013 initiative.[59] Noting that the Internet is "challenging our ability to control how and with whom our private information is shared, and changing our very understanding of privacy,"[60] NAAG articulated its goals for this initiative in the following terms:

> This initiative will explore the best ways to manage [privacy] risks – from geo-location tracking to cyberbullying, from data collection to data breaches – bringing the energy and legal weight of this organization to investigate, educate, and take steps necessary to ensure that the Internet's major players protect online privacy and provide meaningful options for privacy control, while continuing to enhance our lives and our economy.[61]

C. PCI-DSS

For many franchisors whose franchisees sell goods and services to the public, arguably the most important rules are not those set forth by any legislature or agency at all, but rather those set forth by the Payment Card Industry Security Standards Council ("PCI-SSC" or "Council"). The Council is an industry association comprised of several leading credit card companies. The Council has established technical criteria, the Payment Card Industry Data Security Standard ("PCI-DSS"), that are designed to minimize the risk of theft or misuse of credit card data. With respect to PCI-DSS, the Council has represented that the standard "applies to all entities involved in payment card processing – including merchants, processors, acquirers, issuers and service providers, as well as all other entities that store, process or transmit cardholder data."[62]

The Council not only develops these standards, but continues to refine them and promote education and awareness. However, because the Council is a consortium of non-governmental entities, it does not have the innate power to pass laws or impose federal or state regulations. Instead, retailers are bound by PCI-DSS by means of agreements with merchant banks or with the brands themselves. By means of these agreements, retailers agree not only to comply with PCI-DSS, but to be liable to penalties and fines for any violation.

For example, these standards, and associated guidance from specific brands, may require notice of an alleged breach within 24 hours of it being discovered or suspected. If fines are levied, the fine amounts for violations can be quite large. For example, MasterCard has the

---

[58] *See* Press Release, Connecticut Attorney General, Attorney General Announces $7 Million Multistate Settlement With Google Over Street View Collection of WiFi Data (Mar. 20, 2013), http://www.ct.gov/ag/cwp/view.asp?Q=520518.

[59] NAAG, Press Release, New NAAG President Is Maryland Attorney General (June 22, 2012), http://www.naag.org/new-naag-president-is-maryland-attorney-general.php.

[60] NAAG, Privacy in the Digital Age (Jun. 21, 2012), http://www.naag.org/privacy-in-the-digital-age.php.

[61] *Id*.

[62] PAYMENT CARD INDUSTRY (PCI) DATA SECURITY STANDARD: REQUIREMENTS AND SECURITY ASSESSMENT PROCEDURES VERSION 2.0 at 5 (Oct. 2010), https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf; *see also* AT A GLANCE: STANDARDS OVERVIEW: PAYMENT CARD INDUSTRY SECURITY STANDARDS at 1, https://www.pcisecuritystandards.org/pdfs/pcissc_overview.pdf ("The PCI-DSS applies to any entity that stores, processes, and/or transmits cardholder data").

discretion to impose fines of $25,000 per day for noncompliance.[63] Visa has tiered violations of $50,000 for the first violation, $100,000 for the second violation and third or subsequent violations of $200,000.[64] American Express assesses fines up to $100,000 for each data security incident.[65] These fines can be taken from merchant reserves, or compelled to be paid on penalty of termination of the ability to keep processing transactions.

Class action plaintiffs' attorneys increasingly look to PCI-DSS as establishing a standard of care with respect to cardholder data.[66] In addition, failure to protect cardholder data at a standard consistent with PCI-DSS "may provide the basis for a governmental enforcement action or private class action against the violating party under a more general statute," such as the Federal Trade Commission Act's prohibition on unfair practices.[67]

D. Private Class Actions

In the past several years, hundreds of class actions have been filed in the United States against businesses, alleging that those businesses violated the law with respect to individual privacy. For the most part, these putative class actions can be lumped into two categories: (1) cases that allege that the company permitted the loss, theft or misuse of personal information and (2) cases that allege that the company intentionally undertook some action with respect to consumer information – collection, transfer, analysis, retention or destruction – with a purpose or in a manner that violated privacy law.

1. Cases Concerning the Loss, Theft or Misuse of Information Safeguarded by the Company

Hundreds of class action suits arising from data security breaches have been filed in the U.S., fueled by tens of millions of breach letters sent.[68] Most privacy class actions seek millions or billions in statutory penalties, although nearly every such case fails to point to any out-of-pocket harm to consumers. Legal liability theories range from simple negligence to breach of contract to unjust enrichment to consumer fraud.

To date, class action counsel have been mostly unsuccessful in these actions. The fact that information has been lost or stolen does not mean that that anyone described by that information will actually become the victim of identity theft or financial fraud. Courts routinely hold that "threat of identity theft" allegations are not sufficient to plead legally cognizable tort claims.[69] In *Krottner v. Starbucks*, a laptop containing the names, addresses and Social Security numbers of some 97,000 Starbucks employees was stolen.[70] In the case of one

---

[63] MASTERCARD SECURITY RULES AND PROCEDURES, MERCHANT EDITION at § 10.2.6 (Feb. 22, 2013) , http://www.mastercard.us/merchants/security/data-security-rules.html.

[64] VISA INTERNATIONAL OPERATING REGULATIONS at p. 722 (April 15, 2013), http://usa.visa.com/merchants/operations/op_regulations.html.

[65] AMERICAN EXPRESS MERCHANT REFERENCE GUIDE – U.S. at § 12.2.4 (April 2013), https://www260.americanexpress.com/merchant/singlevoice/dsw/FrontServlet?request_type=dsw&pg_nm=merchinfo&ln=en&frm=IDC.

[66] *See, e.g.*, John P. Hutchins and Renard C. Francois, *A New Frontier: Litigation Over Data Breaches*, 20 Prac. Litigator 47 (July 2009).

[67] *See* James Cowing and Stephen S. Wu, *Implementing Security Standards: What Businesses Need to Know About the Payment Card Industry (PCI) Data Security Standard,* 935 PLI/Pat 341, 354 (July 2008).

[68] The Privacy Rights Clearinghouse has documented almost 4,000 breaches made public, concerning more than 600 million records. *See* Privacy Rights Clearinghouse, CHRONOLOGY OF DATA BREACHES SECURITY BREACHES 2005 - PRESENT, http://www.privacyrights.org/data-breach.

[69] *See, e.g., Krottner v. Starbucks Corp.*, 406 F. App'x 129, 132 (9th Cir. 2010).

[70] *Id.*

employee, there was even a subsequent attempt by an unauthorized person to open a bank account in his name. The Ninth Circuit Court of Appeals found that plaintiffs stated no claim under Washington law.

> The mere danger of future harm, unaccompanied by present damage, will not support a negligence action… The alleged injuries here stem from the danger of future harm. Even Shamasa, the only plaintiff who claims his personal information has been misused, alleges no loss related to the attempt to open a bank account in his name.[71]

The *Krottner* decision was in accord with an earlier decision by the Seventh Circuit.[72] In *Pisciotta v. National Bankcorp.*, plaintiffs claimed that defendants:

> had solicited personal information from applicants for banking services, but had failed to secure it adequately. As a result, a third-party computer 'hacker' was able to obtain access to the confidential information of tens of thousands of ONB site users. The plaintiffs sought damages for the harm that they claim to have suffered because of the security breach; specifically, they requested compensation for past and future credit monitoring services that they have obtained in response to the compromise of their personal data through ONB's website.[73]

The trial court dismissed the case on the pleadings. The Court of Appeals for the Seventh Circuit affirmed, holding that it had no indication that Indiana law would permit a suit based on "increased risk" following a data security breach.[74] In fact, court after court has considered and rejected the theories of recovery advanced by plaintiffs. Dismissal of "increased risk of identity theft" suits has become a sufficiently obvious result across the country that one federal court *sua sponte* dismissed a *pro se* complaint arising from a data security breach.[75] This complaint alleged that plaintiff's credit card information had been stolen from defendant, a credit processing company. The complaint further alleged that the theft had put plaintiff at "increased risk of fraud and identity theft."[76] "[I]t appearing that Hinton's allegations of injuries amount to nothing more than mere speculation," the court dismissed his case for being "frivolous and for failure to state a claim."[77]

Plaintiffs typically claim that they now "need" to buy credit monitoring to protect themselves from increased risk of identity theft. Courts have typically rejected that attempt to

---

[71] *Id.* at 131.
[72] *See Pisciotta v. Old Nat'l Bancorp*, 499 F.3d 629 (7th Cir. 2007).
[73] *Id*. at 631.
[74] *Id*.
[75] *Hinton v. Heartland Payment Sys., Inc*., Case No. 09-594 (MLC), 2009 WL 704139 (D.N.J. March 16, 2009).
[76] *Id*. at *1.
[77] *Id.* In addition to the cases cited above, the authorities for Rule 12(b)(6) dismissal of claims of "increased risk of identity theft" are abundant. *See, e.g., Cherny v. Emigrant Bank*, Case No. 08 Civ 5359, 2009 WL 690248 (S.D.N.Y. March 12, 2009) (dismissing data security class action for lack of injury under New York law); *Pinero v. Jackson Hewitt Tax Serv., Inc*., Case No. 08-3535, 2009 WL 43098 (E.D. La. Jan. 7, 2009) (same, under Louisiana law); *Belle Chasse Auto. Care, Inc. v. Advanced Auto Parts, Inc*., Case No. 08-1568, 2009 WL 799760 (E.D. La. Mar. 24, 2009) (same); *Melancon v. La. Office of Student Fin. Assistance*, 567 F.Supp.2d 873 (E.D.La. 2008) (same); *Shafran v. Harley-Davidson, Inc*., Case No. 07 Civ. 01365, 2008 WL 763177 (S.D.N.Y. Mar. 20, 2008) (dismissing all claims from data security breach); *Ponder v. Pfizer, Inc*., 522 F.Supp.2d 793, 798 (M.D.La. 2007) (dismissing claim for credit monitoring under Louisiana law, holding that "injury accrues when the compromised data are actually used by a third party to steal someone's identity").

accrue an "injury" that is not yet actual or imminent.[78] In *Giordano v. Wachovia Securities, LLC*, the plaintiff alleged that a copy of information about her, including her financial information and Social Security number, had been lost in shipping by the defendant.[79] The plaintiff claimed she suffered from "increased risk of identity theft" and would be "compelled" to buy credit monitoring for the rest of her life.[80]

The *Giordano* court, in making its finding that Giordano could not sue, commented with approval on a line of earlier cases on this point.[81] As the *Giordano* court noted:

> In all three cases, the district courts rejected a plaintiff's argument that he or she was entitled to reimbursement for credit monitoring services or for the time and money he or she spent monitoring his credit. In all three cases, the district court has held that, because the plaintiff's injuries were solely the result of a perceived risk of future injury, plaintiff had failed to show a present injury or reasonably certain future injury to support damages for any alleged increased risk of harm.[82]

In light of the courts' virtual unanimity on these points,[83] plaintiffs have started to look more and more to finding some class members who allege actual identity theft following a breach.[84] *Anderson v. Hannaford* arose from the alleged theft of targeted payment card data by a sophisticated criminal enterprise, a theft committed for the purpose of accomplishing identity theft. The complaint alleged that many of the class members, including named plaintiffs, had suffered actual or attempted identity theft as a result. The court in *Hannaford* reinstated the post-breach claims of certain plaintiffs who alleged that they had procured replacement cards and credit insurance in response to that breach. However, even in *Hannaford*, the Court concluded that "where neither the plaintiffs nor those similarly situated have experienced fraudulent charges resulting from a theft or loss of the data, the purchase of credit monitoring services may be unreasonable and not recoverable."[85]

In fact, despite this limited win, the *Hannaford* plaintiffs still floundered on class certification. The court found that the plaintiffs satisfied the Rule 23(a) factors – numerosity, commonality, typicality and adequacy.[86] With respect to the predominance and superiority factors in Rule 23(b)(3), the court found that the plaintiffs' lack of an expert was fatal to their argument that questions of law or fact common to the class predominated over any questions affecting individual class members.[87] Class certification was therefore denied.[88]

---

[78] *See, e.g., Giordano v. Wachovia Securities, LLC*, Case No. 1:06-cv-00476, 2006 WL 2177036 (D.N.J. July 31, 2006).
[79] *Id*.
[80] *Id*.
[81] *Id*. at *5, citing with approval *Forbes v. Wells Fargo Bank, N.A*., 420 F. Supp. 2d 1018 (D. Minn. 2006); *Guin v. Brazos Higher Educ. Serv. Corp., Inc*., Case No. 05-cv-668, 2006 WL 288483 (D. Minn. 2006); *Stollenwerk v. Tri-West Healthcare Alliance*, Case No. 03-cv-0185, 2005 WL 2465906 (D. Ariz. 2005), *aff'd in relevant part*, 254 Fed. App'x 664 (9th Cir. 2007).
[82] *Id*.
[83] Support for these points may also be found in the U.S. Supreme Court's 2013 decision in *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138 (2013) (plaintiffs relying on the risk of future harm to establish standing – in this case, the potential for future warrantless electronic monitoring under 2008 amendments to the Foreign Intelligence Surveillance Act of 1978 – must show that the risk is "certainly impending").
[84] *See, e.g., Anderson. v. Hannaford Bros. Co.,* 659 F.3d 151 (1st Cir. 2011).
[85] *Id*. at *11, n. 10.
[86] *Id*.
[87] *Id*.
[88] *Id*.

Despite the general success of the defendant companies in breach litigation,[89] such cases continue to be filed, and defendants in certain circumstances choose to agree to settlements. The following table shows the settlement terms entered into in five different clusters of breach litigation, amounting to more than seventy class actions. As shown, these settlements often involve providing or making available credit monitoring or another form of identity theft protection, providing a means to make claims of identity theft and have them fairly resolved, and reimbursement for losses actually shown.

A defendant in a class action may have any number of reasons to settle, including a desire for finality, to lower the amount of unquantified litigation risk, to maintain customer relations or to avoid the cost of defense. For franchisors, the important takeaway is that the loss, theft or misuse of individual information is an area to which significant litigation risk still attaches, and preventing such loss events should be a goal of any privacy and data security plan.

Case (*** denotes case was not MDL)	**Class Certified Prior to Settlement?**	**# of Suits Resolved in Settlement**	**Consideration per class member**	**Plaintiff Atty Fees**
In re: Countrywide Financial Corp. Customer Data Security Breach Litig., 3:08-MD-01998 (W.D. Ky.) (MDL 1998)	No	37	• 2 yrs of CM and ID theft insurance • Reimbursement up to $50k for ID theft loss aggregate cap of $5m • Reimbursement for out of pocket expenses up to $350; aggregate cap of $1.5m • Dispute resolution through JAMS – award of additional 10% if successful • Individual mail notice; website; toll free number	$3.5m
In re: The TJX Companies, Inc., Customer Data Security Breach Litig., 1:07-cv-10162 (D. Mass.) (MDL 1838)	No (motion denied, 11/29/07)	26	• 3 yrs of CM and ID theft insurance • Reimbursement for cost of replacing driver's license • Reimbursement for losses > $60 if certain criteria met • Vouchers of $30/$60 for out of pocket expenses • One-time special event sale of 15% of all items • Individual mail notice; website; toll free number	$6.5m

[89] *But see*, *e.g.*, *Resnick v. AvMed, Inc.*, 693 F.3d 1317 (11th Cir. 2012) (reversing dismissal of a privacy class action complaint stemming from theft from a health plan of two laptops containing unencrypted sensitive information; court accepted plaintiffs' unjust enrichment claim that because the customers' data was allegedly not properly secured, the insurer "cannot equitably retain their monthly premiums – part of which were intended to pay for the administrative cost of data security.").

Case (*** denotes case was not MDL)	**Class Certified Prior to Settlement?**	**# of Suits Resolved in Settlement**	**Consideration per class member**	**Plaintiff Atty Fees**
In re Heartland Payment Sys., Inc. Customer Data Security Breach Litig., 851 F.Supp. 2d 1040 (S.D.Tex. 2012).	No	17	• Reimbursement for out of pocket expenses and/or identity theft up to $10k, up to $2.4m • Dispute resolution though third party arbitrator – award of additional 10% if successful • Publication notice; website; toll-free number • Potential for *cy pres*	$725k
Lockwood v. Certegy Check Services, Inc., 07-CV-01434 (M.D. Fla.)	No	6	• 1 yr of CM to credit card customers; 2 yrs of Bank Monitoring to bank customer members • Reimbursement up to $20,000 for ID theft loss; cap of $4m • Reimbursement for out of pocket expenses up to $220; aggregate cap of $1m • Dispute resolution through JAMS • Individual mail notice; website; toll free number	$2.35m
In re: Department of Veterans Affairs (VA) Data Theft Litig., 1:06-mc-00506 (D.D.C.) (MDL 1796)	No	3	• Lump sum of $20m to Plaintiffs, inclusive of fees and costs • Reimbursement min. payment $75, not to exceed $1,500	$3.6m
Rowe v. UniCare Life and Health Insurance Company, 09-CV-02286 (N.D. Il)	No	1	• 1 yr of CM, ID theft insurance, Internet Monitoring • Reimbursement up to $20,000/person if certain criteria met; aggregate cap of $2m for all claims • Reimbursement for out of pocket expenses; no cap per claimant; aggregate cap of $1m for all claims • Dispute resolution through JAMS – award of additional 25% if successful • Individual mail notice; website; toll free number	$500k

2. Privacy Cases Based on What Companies Intentionally Did With Consumer Information

Even perfect security – if that were possible – would not provide a guarantee against consumer class actions based on alleged privacy or data security violations. Increasingly, plaintiffs' lawyers bring consumer class actions asking not "why did you lose the consumer's information?" but "why did you have it in the first place?"

When companies are seen profiting from the collection or use of consumer data, consumers have sometimes sued for compensation.[90] In *In re DoubleClick*, more than a decade ago, the court rejected a class action brought by consumers who alleged that by using web cookies to track online activity, the defendants were unjustly enriching themselves. The court noted:

> [A]lthough demographic information is valued highly… the value of its collection has never been considered a [*sic*] economic loss to the subject. Demographic information is constantly collected on all consumers by marketers, mail-order catalogues and retailers. However, we are unaware of any court that has held the value of this collected information constitutes damage to consumers or unjust enrichment to collectors.[91]

The *DoubleClick* decision, while influential, marked the start and not the end of litigation between companies and the individuals whose information they collect and share. In the course of national programs against terrorism, many companies have shared consumer information with the government. These actions, too, have drawn consumer class actions.[92] In *In re Jetblue*, airline passengers sued an airline for "unlawfully transferring their personal information …for use in a federally-funded study on military base security."[93] The passengers sued for, *inter alia*, breach of contract and trespass to chattels. As to each claim, New York law applied. The *Jetblue* court dismissed both of these counts. As to the breach of contract claim, the court found that there was "no support for the proposition that an individual passenger's personal information has or had any compensable value in the economy at large," and hence plaintiffs stated no actual damages.[94] In dismissing the claim for trespass to chattels, the court added that the passengers had at all times retained access to their own respective individual information, and hence were deprived of nothing.[95]

Cases based purely on the value of data have foundered because plaintiffs have – so far – failed to produce any evidence that but for the company's actions, the consumer could and would have sold the same information.[96] In *Todd Murphy v. Walgreen Corporation*, plaintiffs sued a pharmacy for creating and selling an ancillary data set derived from de-identified activity of pharmacy patients. The court dismissed the complaint with prejudice, in part noting that "the sale of de-identified prescription data does not carry a compensable value to consumers, and thus plaintiff had not shown that he was harmed by defendants' actions."[97] This line of defense, of course, depends, at least in part, on consumer information not being an economic commodity on the individual level. That assumption may be eroding as consumers find additional opportunities to sell their personal information on the retail level through exchanges or online bazaars.

---

[90] *See, e.g., In re DoubleClick Inc. Privacy Litigation*, 154 F.Supp.2d 497, 525 (S.D.N.Y. 2001).
[91] *Id.* at 525. For a more recent variant on this phenomenon, *see Klayman v. Obama*, Case 1:13-cv-00881-RJL (D.D.C.). The *Klayman* suit was filed in connection with public disclosure of the NSA's national surveillance programs. It names as defendants all of the following companies and their top executives, alleged data sources for the NSA: Facebook, Google, Yahoo, YouTube, Skype, AOL, Sprint, AT&T, Apple, Microsoft, and PalTalk. The complaint demands $20 billion in punitive damages, a cease and desist order, and a full accounting.
[92] *See, e.g., In re Jetblue Airways Corp. Privacy Litigation*, 379 F.Supp.2d 299 (E.D.N.Y. 2005)(hereinafter, "*Jetblue*").
[93] *Id*. at 303.
[94] *Id*. at 327.
[95] *Id*. at 329.
[96] *See*, *e.g., Todd Murphy v. Walgreen Corporation*, No. 37-2011-00087162-CU-BT-CTL, Cal. Super. Ct., San Diego Cty. (Minute Order of May 9, 2012).
[97] *Id*. at p. 2.

Plaintiffs have been more successful in privacy-based suits where they have been able to pair their complaint with a specific statute, especially one which provides a statutory penalty. For example, the California Song-Beverly Credit Card Act prohibits retailers in California from requiring customers to provide personal information as a condition for using a credit card as payment.[98] In *Pineda v. Williams Sonoma*, the California Supreme Court held that "personal information," as it was used in the Song-Beverly Credit Card Act, included a consumer's ZIP code.[99] The court reasoned that "[t]he statute's overriding purpose was to protect the personal privacy of consumers who pay for transactions with credit cards," according to legislative history.[100] "[A] ZIP code is readily understood to be part of an address," and, according to the California Supreme Court, "the word 'address' in the statute should be construed as encompassing not only a complete address, but also its components."[101]

Because a violation of the Song-Beverly Credit Card Act provides for statutory damages, and because the practice of asking for a ZIP code in connection with credit card purchases was so widespread among retailers, the *Pineda* decision has set off an avalanche of privacy class actions. In fact, these ZIP code cases have spread to other jurisdictions, as plaintiffs try to find similar statutes to sue under across the country.

These ZIP code class actions are just one of a host of non-breach class action types that have proliferated across the country, with respect to topics as diverse as SMS text messaging,[102] storing subscriber rental history[103] or sharing subscriber lists,[104] and using Adobe® Flash® Locally Stored Objects.[105]

IV. SPECIFIC ACTIONS FOR FRANCHISORS TO TAKE AND ENCOURAGE THROUGHOUT THE FRANCHISE SYSTEM

A. Know What Personal Information You Collect and Keep It Secure

Arguably all businesses, especially consumer-facing entities like retailers and a multitude of service providers, are vast warehouses of data that include personal information. Personal information is generally thought of as data that can, on its own or in conjunction with other information, identify an individual, such as name, address, email address, Social Security number, driver's license number and credit card or bank account number. All employers gather this information, to one extent or another, on their employees, independent contractors, consultants and vendors. Entities that sell or provide products or services to consumers collect and store this data in order to provide those products or services, and also to market new products, verify an individual's identity, investigate an allegation of fraud, respond to a complaint and make other important business decisions.

[98] Cal. Civ. Code § 1747.08(a).
[99] *Pineda v. Williams-Sonoma Stores, Inc*., 51 Cal.4th 524 (2011).
[100] *Id*. at 534.
[101] *Id*. at 531.
[102] *See Sterk v. Path, Inc*., Case No. 1:13-cv-02330 (N.D. Ill., March 28, 2013).
[103] *See In re: Netflix Privacy Litigation*, Case No. 11-cv-00379 (N.D. Cal., Jan. 26, 2011).
[104] *See In re: Hulu Privacy Litigation*, Case No. 11-cv-03764 (N.D. Cal.)
[105] *See Vecchio v. Amazon.Com, Inc*., Case No. 11-cv-366 (W.D. Wash).

The FTC has published a practical guide for businesses on taking reasonable and appropriate steps to secure the personal information in their possession.[106] The guide is built on five key principles for data security:

1. Take stock. Know what personal information you have in your files and on your computers.

2. Scale down. Keep only what you need for your business.

3. Lock it. Protect the information that you keep.

4. Pitch it. Properly dispose of what you no longer need.

5. Plan ahead. Create a plan to respond to security incidents.[107]

The FTC guide recognizes that before a business can appropriately protect the information in its possession, it must know what it collects. This step is certainly easier said than done. Knowing what personal information comes into the business, through all of the possible channels and routes, and (as is important in step number 2) figuring out how it is used and whether it is necessary, can be incredibly time consuming and complex.

1. Data and Heat Mapping

The process of determining "what personal information you have in your files and on your computers" begins with asking the right people the right questions. This process may vary broadly depending on industry, jurisdiction and data profiles, but essentially begins by identifying those people who are likely to have access to, and use on a semi-regular basis, personal information. There are several generic "likely candidates," and many other specific possibilities that the business can identify. In order to create a data map, these individuals should be interviewed regarding how they collect, use, maintain, disclose, transfer and dispose of personal information.

The interviews will help to establish the lifecycle of personal information residing within the corporation. If a customer provides a credit card number at the point of sale, for example, there are certain business units, individuals and systems that will interact with that credit card number throughout its lifecycle in the business. The card number may be collected at point of sale and transmitted for processing. The number may be stored in servers on site for 30 days to allow for merchandise return and refund back to the card. Data from the card, including customer name, may be stored in separate servers and used for another purpose. When the information is no longer needed, it may be securely deleted from servers. Understanding where the credit card number comes into the business and how it is used once it arrives helps a business take the most appropriate methods to protect it.

Of additional importance is the ability to update the data map with changes in data collection and use practices. The interviews can therefore be not just a one-time event but part of an ongoing process that requires reporting on the privacy and security aspects of new projects, preferably before those projects are finalized and rolled out.

---

[106] Fed. Trade Comm'n, PROTECTING PERSONAL INFORMATION: A GUIDE FOR BUSINESS (Nov. 2011), http://www.business.ftc.gov/documents/bus69-protecting-personal-information-guide-business.

[107] *Id*.

2. Information Management

This lifecycle analysis is essential to the additional steps in the FTC's five-step guide for protecting personal information, and therefore essential to establishing a culture of compliance, important should the FTC or a state Attorney General ever come knocking. For example, a privacy audit may reveal that a business unit collects consumer Social Security numbers for no reason other than there is a blank on the form for it and that is what they have always done. That knowledge allows an entity to scale down and stop the practice of unnecessarily collecting Social Security numbers. If an entity does not maintain SSNs, the entity cannot lose SSNs, and the entity does not have to notify consumers regarding the loss of those SSNs. It only makes practical sense to stop collecting what is no longer necessary.

The process also allows an entity to determine who in the organization has access to the information as it is collected and used. Those without a legitimate business need to access and use personal information should not have such access. Similarly, the lifecycle analysis allows an entity to establish data security policies to lock up the information at various points as it travels or is transmitted across the company, and to determine the best way to destroy the information when it is no longer needed.

3. Policies, Procedures, and Training Around Privacy and Data Security

The lifecycle analysis reveals areas of risk, places where company practice can and should change, and informal policies that should be documented and formally implemented. The next step is therefore to draft, adopt, and thereafter maintain policies, procedures, and employee training around data security. Information management is a key component to regulatory investigations of data security incidents, and the way to demonstrate that an entity has built privacy protections in from conceptualization to end-of-lifecycle is by documenting policies and holding employees accountable.

Businesses may decide to create a Data Privacy Committee whose job it is to draft and approve all relevant data privacy and security policies, and to provide training and conduct compliance audits. All of the policies and procedures relating to data privacy and security may collectively be part of a company's Data Privacy Program. Such a program is one that the FTC routinely requires of entities that settle charges under Section 5 for unfair or deceptive acts or practices.[108] Establishing a program voluntarily, while free from scrutiny of a federal or state regulator, will allow an entity to customize the provisions.

Relevant internal policies and procedures that are a part of a Data Privacy Program include: corporate privacy policy; comprehensive written information security program; policy for physical protection of information; remote access use policies; access profile and periodic audit policies; policy to respond to law enforcement demands for personal information; breach incident response plans; vendor data security policies, vendor data transfer procedures, vendor data security audits, vendor indemnification for breaches and vendor management in general; and training programs for employees.

---

[108] *See In the Matter of Google, Inc*., *supra* note 38, Agreement Containing Consent Order, FTC File No. 102 3136 (Mar. 30, 2011) (requiring Google to "establish and implement, and thereafter maintain, a comprehensive privacy program that is reasonably designed to: (1) address privacy risks related to the development and management of new and existing products and services for consumers, and (2) protect the privacy and confidentiality of covered information").

How can a company be sure that its Data Privacy Program is being understood and followed? The process by which new data security procedures are implemented can help to emphasize the importance of adhering to the requirements. To that end, the follow steps can provide the appropriate emphasis:

- initial roll-out memo should come from senior management;
- provide plain text privacy training materials;
- obtain employee attestation;
- develop signage reminders as appropriate;
- help supervisors get involved;
- determine disciplinary measures appropriate for infractions;
- respond to individual infractions.

Audits are necessary to review, analyze and verify employee compliance with policies to secure personal and private information; internal communication of compliance standards; privacy compliance training; corporate policies regarding acceptable use of social media; employee support when privacy issues arise; and disciplinary process for violations of privacy policies and procedures.

4. Identifying and Responding to Data Breaches

Breach response policies and procedures can be implemented only if breaches are detected and accurately identified as breaches. Though some breaches are easily and fairly obvious to detect, others may be harder to identify. Breach response is a "team sport" that involves corporate communications, line of business, regulatory relations, privacy compliance and legal.

Once it has been determined that a security incident has occurred, a business must decide, based on the facts of the situation, the most appropriate first step. In some cases, the most appropriate first step will be to involve law enforcement. In others, it will be to conduct an internal investigation. If the breach is actively ongoing, an entity should ask itself it there is something that can be done to arrest the outflow of information. Oftentimes these technical fixes, *e.g.*, unplugging the compromised server, are undertaken in conjunction with a law enforcement agency investigation.

Next, entities must take steps to determine if the incident constitutes a "security breach" under state law for purposes of notifying affected individuals. These inquiries are very fact-specific, in part because each state's law is slightly different.[109] In addition, there may be many instances in which giving notice is still the right thing to do for reasons other than that the state compels notice. For example, giving notice may be the right business move, for keeping customer, counterparty or employee trust about an incident that may later come to light anyway. Further, giving notice may be legally required under a common law theory of negligence to keep someone from coming to foreseeable harm. Lastly, giving notice may be required by the Company's core corporate values.

[109] *See* discussion *infra* Part III.B.

The relevant facts for purposes of determining whether notification to individuals affected is required, or recommended, include whether the information was encrypted; the specific type of information accessed, e.g. whether it was name plus Social Security number, or first name and email address; whether the information was computerized or reduced to paper; and whether any unauthorized person may have accessed the information. Some jurisdictions do not require notice to be sent unless the breach is a "material compromise" of the system in which the information is kept, or unless there is reason to believe that the breach has harmed or will harm the person described by the information. This "risk of harm" analysis is only relevant in some states. Important questions in this notification analysis may include:

- What kind of information has been lost or stolen?
- Is the information in question particularly personal?
- Is it U.S. or non-U.S. data?
- Would the information in question help a would-be identity thief accomplish a crime?
- Who is described by the information stolen?
- How many people?
- Where do those people live?
- What relationship do they have to the company?
- What notice is owed to the persons whose information was stolen, either under the current 46 state laws or the laws of the non-U.S. country?

Some state laws require notification to the Attorney General, the credit reporting agencies, the state insurance regulator, or some other entity.

An entity should have a coordinated public response if the breach is reported in the media, or once breach notification letters go out. The statements made following announcement of a breach are scrutinized, and may form the basis for a class action complaint under state unfairness law.

Businesses that suffer security breaches also must assess whether to offer credit monitoring services or identity theft protection services to affected individuals. Such services are not mandated by law, but consumers affected by breaches have come to expect one or two years of free credit monitoring. Credit monitoring is not appropriate in all breaches, and can be expensive, so should be considered carefully. Companies that offer credit monitoring services and identity theft protection services also often offer call center capabilities to handle consumer inquiries and complaints. Depending on the nature and size of the breach, this is also a consideration.

Notification of the breach is only one response. A business must also assess how to prevent such an occurrence in the future, which might mean an audit of policies, procedures, training and enforcement. Such lessons learned can help a company work toward preventing a recurrence. This may mean physical fixes, e.g., changing locks on the burgled office; or administrative fixes, e.g., suspending or firing personnel involved in the incident.

B. Know What Representations You Make to Consumers and Do What You Say

As part of determining how it collects, uses, discloses, maintains and discards personal information, an entity should also consider investigating and conducting interviews that focus on privacy and security representations made to consumers and how those representations stand up to each business unit's dissemination and use of customer private information (especially for non-personal marketing efforts such as by e-mail, phone, direct mail or targeted advertisement).

When an entity suffers a security breach, and federal and state regulators roll in to investigate what happened, those regulators scrutinize not only the internal policies and procedures in place for data security, but also the representations made to consumers about what information would be collected, how it would be used and how it would be protected. The two inquiries go hand-in-hand — the representations made must be backed up by the documented policies.

Representations about how personal information is collected and used are made in website privacy policies, and also in terms of use, end user license agreements and other agreements and contracts which consumers and customers may enter in order to use a business' products or services. These documents should be compared against the data map to ensure that what a business says it does with personal information comports with the reality on the ground.[110]

V. THE EFFECT OF ALTERNATE DATA CAPTURE METHODS AND THIRD PARTIES

The most transparent manner in which to collect personal information, and the one dealt with in the preceding portions of this paper, is to ask an individual to provide such information directly. For example, a customer's address, credit card data, age or preferences may be provided directly by the customer on a website. The data and heat mapping processes discussed in Part IV of this paper can become quite complex when such information is gathered indirectly and the roles of alternate data collection techniques and third parties are taken into account.

A. Data Capture Through Technology

A method of collecting personal information that is less transparent than the direct approach is through the use of "cookies," which are small computer files stored on the customer's computer or other device when browsing the website. These cookies usually store and use information about a customer (e.g. user names, recent Internet searches, passwords, etc.) to customize what is seen by the customer when he or she returns to the website. While most Internet browser software allows for a systematic or selective refusal to accept cookies, many Internet users are unaware of the existence or use of cookies or their ability to configure their browser software so as to refuse the placing of cookies on their personal computer. Interestingly, the *DoubleClick* decision briefly discussed above[111] dismissed a purported class

[110] *See, e.g.*, *In the Matter of Snapchat, Inc.*, Complaint, Request for Investigation, Injunction, and Other Relief (May 26, 2013), http://epic.org/privacy/ftc/EPIC-Snapchat-Complaint.pdf, in which the Electronic Privacy Information Center alleges that statements to users by Snapchat, the publisher of a widely used mobile application that encourages users to share intimate photos and video, that the images they send using the app will "disappear" after a period of time of the user's choosing are incorrect, as the images may be easily restored on a recipient's device and thus such statements constitute actionable misrepresentations under Section 5 of the FTC Act.

[111] *In re DoubleClick Inc. Privacy Litigation*, *supra* note 75.

action against DoubleClick, Inc., an Internet advertising agency, stating that the placing of cookies on a computer user's hard drive is not an invasion of privacy. The reasoning underlying this decision was that a visit to a website constitutes communication between the website and the computer user visiting the website, and that DoubleClick, Inc. gained legitimate access to the communication when it obtained the authorization of the website operator, as one of the participants to the communication, to place cookies on the computer user's hard drive.[112]

Subsequently, Google Inc. agreed to pay a record $22.5 million civil penalty to settle FTC charges that it misrepresented to users of Apple Inc.'s Safari Internet browser that it would not place tracking cookies or serve targeted ads to those users,[113] thereby violating the 2011 privacy settlement between the company and the FTC.[114] According to the FTC's complaint, Google specifically told Safari users that because the Safari browser is set by default to block third-party cookies, as long as the users did not change their browser settings, this setting would effectively accomplish the same thing as opting out of the Google advertising tracking cookie. In addition, Google represented that it was a member of an industry group called the Network Advertising Initiative, which requires members to adhere to its self-regulatory code of conduct, including disclosure of their data collection and use practices. The FTC alleged that despite these assurances to site visitors, Google had exploited an exception to the browser's default setting to place a temporary cookie from Google's DoubleClick advertising network. Due to the unique operation of the Safari browser, that initial temporary cookie opened the door to all cookies from the DoubleClick domain, including the Google advertising tracking cookie that Google had represented would be blocked from Safari browsers. This settlement further demonstrates the wisdom of the comment in Part IV.B above that any collection of data, whether transparent or less so, should comply with the restrictions stated to website visitors and others whose personal information is collected.

One of the least transparent methods for collecting personal information is through what has become known as "click-stream data," which Internet users carry with them and of which traces are left on the various websites they visit. As Internet users browse a website, the website operator may collect such information as the user's IP address, the name of their Internet service provider, the type of computer and Internet browser used by the site visitor and how long they have stayed on the website in which pages have been visited.

Of course, as technology develops there appears to be an ever-increasing number of less transparent methods by which information can be collected, including e-mail wiretapping and "web bugs" (tiny hidden images that can embed in web pages to track users as they surf the web and read e-mail) which can be used to develop detailed profiles of individual users. In addition, many smartphones emit a steady stream of locational information which can be used to track customers and potential customers without their knowledge.[115] Opting out of such tracking – about which many consumers may be completely unaware – requires either powering down the device or opting out through a complex and time-consuming process.[116]

---

[112] Compare *Chance v. Avenue A, Inc*., 165 F.Supp.2d (W.D.Wash.2001)(accord with *DoubleClick*); and *In re Intuit Privacy Litigation*, 138 F.Supp.2d 1272 (C.D.Cal.2001) (accessing the cookies on a user's hard drive, even those placed there by the accessing party, could be found to be an unauthorized access under the Computer Fraud and Abuse Act, 18 U.S.C. §§ 1030 *et seq*.)

[113] *U.S. v. Google Inc*., Order Approving Stipulated Order for Permanent Injunction and Civil Penalty Judgment, No. CV 12-04177 SI (N.D. Cal. Nov. 16, 2012).

[114] *See In the Matter of Google, Inc*., *supra* note 38.

[115] Ken Dilanian, *The NSA is watching. So are Google and Facebook*, LOS ANGELES TIMES 1 (Jun. 30, 2013).

[116] *Id*.

While most consumers may have acquiesced in, or at least are generally unaware of, the latest techniques for harvesting their personal information, apparently not all have yet accepted the almost 15-year-old comment by a technology company CEO that "You have zero privacy anyway .... Get over it."[117] As one current commentator has noted, privacy-aware individuals are frustrated by such intrusions:

> "How do I express my privacy requirements? Increasingly, it means I have to shut off my phone and become a digital hermit," said Ian Glazer, a vice president at Gartner Inc., an information technology research and advisory company.
>
> In addition to privacy threats, he said, "there is a fundamental problem with fairness, in the sense that I am generating all this data about me through my devices, and these organizations are harvesting it and making a profit off it."[118]

The full extent of the legal obligations of companies surreptitiously gathering such information, or the companies which have engaged the data gatherers to do so, is at best unclear, as the pace of technological development has far outstripped the pace of legal development and of regulators to address the new technologies. At a minimum, though, some of the practices appear to be inconsistent with the FTC's 2012 statement of policy for the privacy arena,[119] and that policy statement should be read as a harbinger of regulation or enforcement actions yet to come.

B. Role and Effect of Third Party Data Activities

Third parties play an increasingly important role in the information technology systems and operations of many businesses, including franchise businesses. In a franchise system, franchisees may collect from their customers and maintain valuable personal information, and they may also use that information for promotional or other purposes. The potential for franchisor liability arising out of such franchisee activities is addressed in Part II above. To the extent that franchisees do engage in such collection, storage, use or disposition of personal information, the franchisor should have in effect policies or procedures – perhaps as part of the franchise system's operating manual – addressing the parties' respective rights and responsibilities with respect to such information. Because of the potential impact on the franchise brand of franchisee missteps with such information, such policies and procedures should at a minimum require compliance with privacy and data security laws but should be reinforced with training and procedural guidance[120] on such subjects as how to respond to a data security breach.

Third parties separate from the franchise system may also deal with franchise system-related personal information in their provision of a variety of data processing or data management functions, including accounting, invoicing, point of sale, human resource management, customer relationship management, management information systems, enterprise resource planning, content management and service desk management. These functions tend to be performed by application service providers in a "software as a service" or "on-demand software" role, generally in a location remote from the originating business or in the

---

[117] Polly Sprenger, *Sun on Privacy: 'Get Over it'*, WIRED NEWS (Jan. 26, 1999), http://www.wired.com/politics/law/news/1999/01/17538.
[118] Ken Dilinaian, *supra* note 114.
[119] Final Report, *supra* note 30.
[120] For additional discussion of privacy policies, procedures and related training, *see* Part IV.A.3 of this paper.

"cloud."[121] Providers are typically accessed via a web browser using a thin client, computer hardware used solely for economical access to the cloud.

In performing these functions, the third parties obviously have access to information of the originating business, which in many cases consists of personally identifiable information protectable under privacy and data security laws. Other third parties may be engaged to seek out or compile personal information for the contracting business to use for marketing, product research and development, customer support and other purposes.

It is clear under state and federal law that the illegal or inappropriate actions of third parties can result in liability for the owner of the data that is mishandled.[122] For example, CalOPPA – which is discussed in Part III.B above – applies to any operator of a commercial website or online service that collects personal information through the Internet about individual consumers residing in California that use or visit the operator's commercial website or online service.[123] Under the statute, the owner of the website is deemed to be the operator regardless of whether the owner has contracted actual operation of the site to a third party.[124] Thus a website owner is responsible for the failure of any third party operator of the site to comply with CalOPPA if the noncompliance is either knowing and willful or negligent and material.[125]

The same is true under data security breach notification laws. For example, the California statute requires "[a]ny person or business that conducts business in California, and that owns or licenses computerized data that includes personal information" to make the required disclosures when that person or business discovers a security breach affecting any California resident "whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person."[126] Although the statute also obliges a third party that maintains computerized data containing personal information to notify the owner or licensee of that data whenever such a security breach occurs,[127] the owner or licensee of the data is primarily responsible under the statute.

Even parties remote from the data owner can create liability. For example, in *Satterfield v. Simon & Schuster, Inc.*,[128] the Ninth Circuit reversed summary judgment in favor of publisher Simon & Schuster in connection with an unsolicited text message allegedly sent in violation of the Telephone Consumer Protection Act ("TCPA").[129] Although the plaintiff had consented[130] to the receipt of text messages from Nextones.com ("Nextones") in order to receive a free ringtone, that consent was not unlimited. In fact, the Nextones sign-up form authorized promotional messages only "from Nextones affiliates and brands." Despite this limitation, Simon

---

[121] *See* Part VI.C of this paper for additional discussion of cloud computing.

[122] *But see Shefts v. Petrakis*, No. 1:10-cv-01104, 2013 WL 3187971 (C.D. Ill. 2013) (an individual who directed others to intercept a colleague's private e-mails cannot be pursued in a civil action for procuring others to engage in violations of the Electronic Communications Privacy Act.)

[123] Cal. Bus. & Prof. Code § 22575.

[124] Cal. Bus. & Prof. Code § 22577(c) defines the term "operator" to mean "any person or entity that owns a Web site located on the Internet or an online service that collects and maintains personally identifiable information from a consumer residing in California who uses or visits the Web site or online service if the Web site or online service is operated for commercial purposes. It does not include any third party that operates, hosts, or manages, but does not own, a Web site or online service on the owner's behalf or by processing information on behalf of the owner."

[125] *See* Cal. Bus. & Prof. Code § 22576.

[126] Cal. Civ. Code § 1798.82(a).

[127] *Id*. § § 1798.82(b).

[128] *Satterfield v. Simon & Schuster, Inc.*, 569 F. 3d 946 (9th Cir. 2009),

[129] 47 U.S.C. § 227.

[130] The TCPA expressly exempts calls "made with the prior express consent of the called party," 47 U.S.C. § 227(b)(1)(A), from its prohibition on calls made using an automatic telephone dialing system .

& Schuster's promotional agent obtained 100,000 individuals' cell phone numbers from Nextones' licensing agent. The court found that Simon & Schuster was not a Nextones affiliate, that the text message promoting a new Simon & Schuster book was not a Nextones branded message and accordingly that the plaintiff had not consented to receive that text message from Simon & Schuster.

Because of the potential impact of third party provider actions, the owners of personal information who release such information to providers or contract with them to obtain such information should carefully consider liability issues in entering into such contracts. Depending upon the specific circumstances, a wide range of issues, including those summarized in the checklist appearing in Appendix A, should be analyzed and perhaps explicitly addressed in the parties' services contract.

VI. IMPACT OF NEW BUSINESS TECHNOLOGIES

A. Telecommuting and BYOD

Two related workplace technological developments have created additional threats to the integrity and security of an employer's data, and have added rich new complexity to the management of personally identifiable information maintained by an employer and protected by privacy and data security laws. Those two developments are telecommuting and bring your own device ("BYOD") practices.

Telecommuting involves employees' remote access to an employer's computer system as well as the confidential, proprietary and other sensitive information maintained in that system. Phrased in that manner, telecommuting suggests that its practice could well raise a host of privacy and security concerns. Despite that suggestion, many companies[131] have enthusiastically adopted such policies to encourage worker productivity while away from the office and to accommodate employees' personal, family or lifestyle needs. Even a traditional company such as IBM virtually gushes about telecommuting, suggesting that telecommuting makes IBM a better corporate citizen, as demonstrated by the following excerpt from its corporate website:

> IBM was one of the first global companies to pioneer programs to reduce employee commuting. It has sustained these programs for nearly two decades. Two key aspects are its (a) work-at-home program and (b) mobile employees program. Today, more than 128,000 (29 percent) of employees globally participate in one of these programs. In 2011, in just the U.S. alone, IBM's work-at-home program conserved approximately 6.4 million gallons of fuel and avoided more than 50,000 metric tons of CO2 emissions.[132]

While good for the individual employee and, as IBM suggests, potentially good for the environment, telecommuting can pose a range of privacy and data security problems beyond the ever-present risk of improper employee data-sharing or misappropriation. Such risks may include malicious hacking of the employee's home computer (which likely does not enjoy the same level of intrusion protection as the employer's network does) or of data in transit; access to corporate data by spouses, children or other nonemployees; unauthorized access of data transmitted over unsecured broadband or wireless networks, including public Wi-Fi hotspots; the

[131] With the notable exception of Yahoo Inc. *See* Rachel Emma Silverman, *At Yahoo, Working from Home Doesn't Work*, THE WALL STREET JOURNAL (Feb. 25, 2013).

[132] International Business Machines Corporation, *Supporting alternate employee commute options*, http://www.ibm.com/ibm/environment/climate/commuting.shtml).

risk of security breaches of information through misplacement or theft of an employee's laptop, tablet, smartphone or other device; and potential failures to recognize or discharge employer obligations under state data breach notification laws.

Many of the same risks are present with BYOD programs, which permit employees to use their personal electronic devices, including laptops, tablets and smartphones, in the workplace for work purposes. Such programs in general reflect the acquiescence by employers to employees' desire to carry a single mobile device – usually their own smartphone – to have the most up-to-date such device available and never to be separated from that device. While BYOD programs provide benefits in enhancing employees' convenience and perhaps reducing the employer's budget for hardware, monthly service fees and ongoing support, they create additional risks by permitting the deployment of devices – many of which may be quite attractive to thieves – that are full of confidential employer information. As noted by Larry Ponemon, chairman and founder of the Ponemon Institute, these risks appear to be increasing:

> "[H]ackers are starting to understand and take advantage of employees' privacy issues and objections to having their company control their personal mobile device. We're starting to see … a wave of sophisticated attacks — it's easier for bad guys to slip into a mobile device, access an account and steal money and resources from that account…. There's evidence that suggests this is happening in part because … employees have access to sensitive or regulated data on insecure devices."[133]

Because of these potential risks, a telecommuting or BYOD program should be implemented only after a thorough assessment of potential risks and development of a set of comprehensive policies and procedures to address those risks. An employer's human resources, legal and information technology staff will usually be called upon to participate in the development of such policies and procedures as well as the addition of any technological tools which may be appropriate under the circumstances. Such policies and procedures should address the following subjects as well as others particular to the employer's business and the nature of the employer's information that could be placed at risk:

- Employee confidentiality agreements creating an obligation to safeguard employer data and to return that data to the employer upon request. Any employee with access to confidential and proprietary information should be required to execute such an agreement, which should be tailored to the circumstances.

- A separate agreement concerning use of the employee's home computer or other device, allowing the employer access to the device in order to inspect it and, at least upon termination, to delete company information from it. Such an agreement should contain the employee's acknowledgement that the confidentiality agreement's restrictions apply to the employer's information wherever located, and that the employer's information does not lose protection merely because it may reside on the employee's device.

- Monitoring electronic equipment. In order to remove any expectation of privacy with respect to employer information housed in the employee's home computer or other

[133] Penny Crosman, *Mobile Leaks Make Banks Wary of 'Bring Your Own Device' Trend*, AMERICAN BANKER (Jul. 1, 2013), http://www.americanbanker.com/issues/178_126/mobile-leaks-make-banks-wary-of-bring-your-own-device-trend-1060319-1.html.

device,[134] the employee should acknowledge in writing that the employer will monitor and inspect, without notice, their use of the employer's computer system, virtual private network or other access means, and other equipment and systems, as well as documents and communications prepared or accessed by the employee.

- Technological safeguards. A variety of safeguards could be implemented, ranging from firewalls to an ability to remotely "wipe" a device, advanced logging and monitoring to detect unusual behavior, and other security-focused technologies. The employer's information technology staff may be detailed to telecommuters' homes or require access to employees' other devices in order to install such safeguards. To complement these protections, an employer might require that remote access be permitted only through a secure connection or other encrypted access and that data transfer be permitted only through a secure network rather than portable media.

The potential for employer liability arising out of telecommuting or BYOD programs should be obvious. The *Cbr Systems* case[135] is an instructive example. In that case, the FTC alleged that CBR, a leading cord blood bank, failed to protect the security of customers' personal information and that its inadequate security practices led to a breach that exposed the Social Security numbers and debit and credit card information of nearly 300,000 consumers. According to the FTC's complaint, Cbr failed to provide reasonable and appropriate security for consumers' personal information, contributing to a December 2010 security breach during which unencrypted backup tapes containing consumers' personal information, a Cbr laptop, a Cbr external hard drive and a Cbr USB drive were stolen from a backpack in a Cbr employee's personal vehicle in San Francisco, California. According to the complaint, the unencrypted backup tapes included, in some cases, the names, gender, Social Security numbers, dates and times of birth, drivers' license numbers, credit and debit card numbers, card expiration dates, checking account numbers, addresses, email addresses, telephone number and adoption type (e.g., open, closed, or surrogate) of approximately 298,000 Cbr customers. Further, the Cbr laptop and Cbr external hard drive, both of which were unencrypted, contained enterprise network information, including passwords and protocols, which could have facilitated an intruder's access to Cbr's entire network, including additional personal information contained on the Cbr network.[136]

As part of the settlement announced on January 28, 2013, Cbr agreed to establish and maintain a comprehensive information security program. The company must also submit to security audits by an independent auditor every other year for the next 20 years. The settlement order also bars misrepresentations about the privacy, confidentiality, security or integrity of personal information collected from or about consumers.

[134] In *City of Ontario v. Quon*, 130 S. Ct. 2619, 560 U.S. __ (2010), the U.S. Supreme Court held that an employer's search of personal text messages on an employer-owned device was reasonable because it was conducted for a work-related purpose and was not excessively intrusive. For non-employer owned devices, where privacy might more reasonably be expected, the parties should enter into an agreement clearly establishing the employer's rights to monitor.

[135] *In the Matter of Cbr Systems, Inc*., Decision and Order, FTC File No. 112 3120 (Apr 29, 2013).

[136] *Id*., Complaint at ¶¶ 9-12.

A. Social Media

1. User Information

Social networking sites thrive on personal information, and the more personal the better. This is especially true for the younger users of the sites. Thus sites such as Facebook provide its younger members with "the ability to flirt, diarize, post pictures, share videos, creative artwork, and meet new people."[137] With this abundance of personal information, social networking sites would appear to be a target for abuse of such information, or candidates for such abuse themselves, and particularly so with respect to information obtained from their youngest members. Indeed, among the many actions that the FTC has brought since 2001 against companies that allegedly failed to provide reasonable protections for sensitive consumer information in both online and offline settings[138] is one action against an immensely popular social media site, Twitter, which was accused of deceiving consumers and putting their privacy at risk by failing to safeguard their personal information.[139] According to the FTC, these lapses "allowed hackers to obtain unauthorized administrative control of Twitter, including access to non-public user information, tweets that consumers had designated private, and the ability to send out phony tweets from any account including those belonging to then-President-elect Barack Obama and Fox News, among others."[140] Under the terms of the FTC's settlement, Twitter is barred for 20 years from misleading consumers about the extent to which it protects their privacy, and it must establish and maintain a comprehensive information security program which will be assessed by an independent auditor every other year for 10 years.

Twitter is not alone in facing scrutiny for its privacy practices. In May 2010, some 14 privacy rights organizations filed a complaint with the FTC,[141] requesting the agency to open a formal investigation into Facebook's privacy practices. The complaint alleged that Facebook disclosed users' personal information to Microsoft, Yelp and Pandora without first obtaining users' consent; disclosed users' information – including details concerning employment history, education, location, hometown, film preferences, music preferences, and reading preferences – to which users had previously restricted access; and disclosed information to the public even when users had elected to make that information available to friends only.[142] Following an investigation and extensive public commentary, the FTC in August 2012 accepted a settlement[143] requiring Facebook to take several steps to make sure it lives up to its privacy promises in the future, including by giving consumers clear and prominent notice and obtaining their express consent before sharing their information beyond their privacy settings, by maintaining a comprehensive privacy program to protect consumers' information, and by obtaining biennial privacy audits from an independent third party.

The settlement announced by the FTC in 2006 with the social networking site Xanga.com ("Xanga") illustrates the nature of the risks associated with the personal information

---

[137] Susan B. Barnes, *A Privacy Paradox: Social Networking in the United States*, FIRST MONDAY (Sept. 4, 2006) , http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1394/1312.
[138] *See* Fed. Trade Comm'n, FTC STAFF REPORT: SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING 11, note 8 (2009), http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf.
[139] *In the Matter of Twitter, Inc*., Decision and Order, FTC File No. 092 3093 (Mar. 2, 2011).
[140] Fed. Trade Comm'n, *Twitter Settles Charges that it Failed to Protect Consumers' Personal Information*, http://www.ftc.gov/opa/2010/06/twitter.shtm.
[141] *In the Matter of Facebook, Inc*., Complaint, Request for Investigation, Injunction, and Other Relief (May 5, 2010), http://epic.org/privacy/facebook/EPIC_FTC_FB_Complaint.pdf.
[142] *Id.* at 1.
[143] *In the Matter of Facebook, Inc.*, Decision and Order, FTC File No. 092 3184 (Jul. 27, 2012).

obtained by social media sites.[144] According to the FTC, Xanga had collected, used and disclosed personally identifiable information associated with approximately 1.7 million members under the age of 13. The federal Children's Online Privacy Protection Act[145] and related rules (collectively, "COPPA"), protect personally identifiable information collected from children under age 13, any other information that permits the identification or contacting of a child, as well as certain other information collected through cookies or otherwise (including hobbies and other interests). Anyone who operates (i) a commercial website or online service directed at children under age 13 that collects individually identifiable information from children or (ii) a general audience website but with knowledge that it collects personal information from children, must comply with COPPA.

Although Xanga's terms of use stated that "[c]hildren under 13 are not permitted to join Xanga or participate in the Xanga community" and users were required to check a box confirming an age of at least 13 during the course of their registration, actual birthdates were generally entered, leading the FTC to conclude that Xanga had actual knowledge that it was collecting information from children under the age of 13. Under its consent decree with the FTC, Xanga agreed to pay a $1 million civil penalty and also agreed to delete all personally identifiable information obtained from children in violation of COPPA.

Both individual litigants[146] and government agencies[147] have continued to raise privacy concerns relating to the use social networking sites make of personally identifiable information. In June of 2009, an independent European advisory body on data protection and privacy adopted an opinion on online social networking advising social networking service providers on how they could better comply with EU data protection requirements.[148] Similarly, the Privacy Commissioner of Canada has questioned whether Facebook's privacy policies can be considered in compliance with Canadian law. For its part, Facebook has vowed to cooperate by implementing various privacy safeguards, including efforts to help users better understand Facebook's privacy policy, and to limit the ability of third-party application developers to use personal information without consent.[149]

What does all this mean for franchising? Obviously, to the extent that a franchisor obtains access to personally identifiable information through any social media site – such as through a fan or similar page – the franchisor should not use that information in a manner inconsistent with its own privacy policy or the policy of the social media site from which the information was obtained. In addition, franchisors and franchisees alike should be alert to the potential for acquiring, from one or more social media sites, information from children protected by COPPA. While the privacy policies of most social networking sites preclude the collection of personal information from minors, the experience of Xanga.com clearly demonstrates that a mere policy is insufficient to protect a company when it knows or should know that it has obtained children's information.

---

[144] *U.S. v. Xanga.com*, No.: 06-CIV-6853 (SHS), Consent Decree and Order for Civil Penalties, Injunction, and Other Relief, (S.D.N.Y. Sep. 7, 2006).
[145] 15 U.S.C. §§ 6501 *et seq*.
[146] *See, e.g*., Jessica Vascellaro, *Facebook Faces Privacy Lawsuit*, The WALL STREET JOURNAL (Aug. 18, 2009).
[147] *See, e.g*., Office of the Privacy Commissioner of Canada, *Facebook needs to improve privacy practices, investigation finds* (Jul. 16, 2009), http://www.priv.gc.ca/media/nr-c/2009/nr-c_090716_e.cfm.
[148] Article 29 Data Protection Working Party, *Opinion 5/2009 on online social networking* (Jun. 12, 2009), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf.
[149] Office of the Privacy Commissioner of Canada, *Facebook agrees to address Privacy Commissioner's Concerns* (Aug. 27, 2009), http://www.priv.gc.ca/media/nr-c/2009/nr-c_090827_e.cfm).

Finally, franchisors should make no use of information obtained from social networking sites that would exceed the scope of what is authorized by the sites' terms of use. In particular, without the consent of individuals that conforms to the requirements of the federal CAN-SPAM Act[150] that regulates the use of electronic mail to send commercial messages, franchise businesses should not use such information for commercial email marketing messages.

2. Employee Information

Separately, in their role as employers, franchise companies should be aware that a dozen states[151] presently have laws restricting employers' access to employees' and employment applicants' personal password-protected social media accounts, and 25 other states[152] considered similar legislation during this year's legislative session.[153] While some employers have argued that "access to personal accounts is needed to protect proprietary information or trade secrets, to comply with federal financial regulations, or to prevent the employer from being exposed to legal liabilities,"[154] the states as a public policy matter have generally rejected that position in adopting these laws, which typically prohibit employers from requiring or requesting that an employee or applicant do any of the following:

- Disclose authentication information, such as a username or password, needed to gain access to the individual's personal social media account;[155]

- Add the employer to the list of "friends" or other contacts associated with his or her social media account;

- Access a personal social media account in the presence of the employer in order to enable the employer to view contents of the account; or

- Divulge any personal social media.

Many of the statutes also prohibit an employer from discharging, disciplining, threatening to discharge or discipline, or otherwise retaliating against an employee or applicant for not complying with a request or demand by the employer that would violate any of the other statutory provisions. Exceptions are frequently provided for electronic devices furnished by the employer, social media accounts established or maintained for the benefit of the employer and personal social media reasonably believed to be relevant to an investigation of allegations of

---

[150] Controlling the Assault of Non-Solicited Pornography and Marketing Act, 15 U.S.C. § 7701 *et seq*.

[151] Arkansas, California, Colorado, Illinois, Maryland, Michigan, Nevada, New Mexico (applicable to prospective employees only), Oregon, Utah, Vermont and Washington

[152] Arizona, Connecticut, Georgia, Hawaii, Iowa, Kansas, Louisiana, Maine, Massachusetts, Minnesota, Mississippi, Missouri, Montana, Nebraska, New Hampshire, New Jersey, New York, North Carolina, North Dakota, Ohio, Pennsylvania, Rhode Island, Texas, West Virginia and Wisconsin.

[153] *See generally* National Conference of State Legislatures, EMPLOYER ACCESS TO SOCIAL MEDIA USERNAMES AND PASSWORDS 2013, http://www.ncsl.org/issues-research/telecom/employer-access-to-social-media-passwords 2013.aspx.

[154] *Id*.

[155] California's statute goes farther, extending its protection to all "social media," broadly defined to include "an electronic service or account, or electronic content, including, but not limited to, videos, still photographs, blogs, video blogs, podcasts, instant and text messages, email, online services or accounts, or Internet Web site profiles or locations." Cal. Labor Code § 980(a). Through its use of the term "electronic content," the California statute extends its reach to information housed on a wide range of media not traditionally considered to be social media sites, such as web-based email and file-sharing accounts; online banking, shopping and other accounts; and data that is completely off-line, such as information stored on local and external hard drives, USB flash drives, CDs, DVDs and other media.

employee misconduct or employee violation of applicable law or regulation, so long as the social media is used solely for purposes of that investigation or a related proceeding.[156]

These new statutes may have widespread and as yet not fully understood implications for employers' relations with their employees. Among other things, the statutes suggest that employers should carefully review their personnel and electronic communications policies for consistency with the legislation, and keep the statutes and their scope in mind whenever conducting internal investigations. Changes in policies may be required, such as closely looking at whether, when and for what purposes social media access will be permitted from the employer's network. Consideration should also be given to restricting managers working in the affected jurisdictions from sending "friend" or similar requests to subordinates or other employees. Additional or enhanced monitoring of the employer's computer network may be useful in order to reduce the potential for internal network security breaches and other employee misconduct. Finally, as a result of the statutory restrictions and in order to preserve the integrity of the employer's network, some employers may find it prudent to block employee access from company networks to social networking, file sharing, Internet mail and other potentially problematic web sites that are not used for business purposes.

A. Cloud Computing

1. What Exactly is Cloud Computing?

Although "cloud computing" encompasses a variety of business arrangements and the term has no single universally agreed definition, the National Institute of Standards and Technology[157] in late 2011 defined it as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or cloud provider interaction." Thus cloud computing is a manner of delivering software over the Internet via a web browser rather than installation directly onto the user's computer.[158] A more colloquial definition follows:

> Cloud computing is a fancy way of saying stuff's not on your computer. It's on a company's server, or many servers, possibly all over the world. Your computer becomes just a way of getting to your stuff. Your computer is an interface, but not where the magic happens.[159]

Cloud computing is therefore akin to other arrangements in which an off-site, third party provider furnishes information technology services. In fact, after studying the practice, six U.S. federal agencies that make up the Federal Financial Institutions Examination Council ("FFIEC") issued a guidance document in 2012 concluding that cloud computing should be characterized as "another form of outsourcing with the same basic risk characteristics and risk management

---

[156] *See, e.g.*, Cal. Labor Code § 980(c) - (e).

[157] NAT'L INST. OF STANDARDS AND TECHNOLOGY, Special Publication 800-144, GUIDELINES ON SECURITY AND PRIVACY IN PUBLIC CLOUD COMPUTING vi (Dec. 2011), http://www.nist.gov/manuscript-publication-search.cfm?pub id= 909494).

[158] AMERICAN BAR ASSOCIATION, CLOUD ETHICS OPINIONS AROUND THE U.S., http://www.americanbar.org/ groups/ departments_offices/legal_technology_resources/resources/charts_fyis/cloud-ethics-chart.html (hereinafter, "Cloud Ethics Opinions").

[159] Quinn Norton, *Byte Rights*, MAXIMUM PC (Sept. 2010). *See also* Penn. Bar Ass'n, Committee on Legal Ethics and Professional Responsibility, Formal Opinion 2011-200: *Ethical Obligations for Attorneys Using Cloud Computing/Software as a Service While Fulfilling the Duties of Confidentiality and Preservation of Client Property* (2011)(hereinafter, "Pennsylvania Opinion").

requirements as traditional forms of outsourcing."[160] Although this characterization may be viewed as too simplistic, the FFIEC guidance document suggests that cloud computing is anything but simplistic and proceeds to identify a series of due diligence questions that all companies utilizing cloud computing should consider.[161]

2. Opportunities and Risks

Although most Internet users have only recently become aware of the term "cloud computing," it is far from a new concept. By 2008, the Pew Internet & American Life Project found that "[s]ome 69% of online Americans use webmail services, store data online, or use software programs such as word processing applications [the] functionality [of which] is located on the web."[162] The attraction for most users has been the ease and flexibility of using cloud services. Most users report that they like how cloud services permit them to share data easily with others and also permit them to access their data from any computer.[163] In summary, therefore, the generally perceived attractions of cloud computing are modest upfront costs, flexibility, mobility and ease of use.[164]

As more expansively summarized by the Pennsylvania Bar Association's Committee on Legal Ethics and Professional Responsibility, the benefits of cloud computing may include:

- Reduced infrastructure and management;
- Cost identification and effectiveness;
- Improved work production;
- Quick, efficient communication;
- Reduction in routine tasks, enabling staff to elevate work level;
- Constant service;
- Ease of use;
- Mobility;
- Immediate access to updates; and
- Possible enhanced security.[165]

In addition, the cloud user need no longer own any technology, apart from the modest technology needed to access the web. Thus, "computer services are now available from the network in the same way that electricity is available from an outlet."[166]

---

[160] FED. FIN. INSTS. EXAMINATION COUNCIL, OUTSOURCED CLOUD COMPUTING (Jul. 10, 2012), http://docs.ismgcorp.com/files/external/062812_external_cloud_computing_public_statement.pdf.
[161] *Id*. at 2-4.
[162] PEW RESEARCH CENTER, USE OF CLOUD COMPUTING APPLICATIONS AND SERVICES (Sept. 12, 2008), http://pewinternet.org/Reports/2008/Use-of-Cloud-Computing-Applications-and-Services/Data-Memo.aspx).
[163] *Id*.
[164] Cloud Ethics Opinions, *supra* note 157.
[165] Pennsylvania Opinion, supra note 158, at 3.

The risks concerning cloud computing relate primarily to the privacy and security of the data located in the cloud.[167] That is because data may be stored in jurisdictions with different laws and procedures concerning access to or destruction of electronic data, most of the control over that data and its security is left with the service provider, and because "[t]he cloud client is . . . rarely in a position to be able to know in real time where the data are located or stored or transferred."[168]

Based upon the nature of the service and the technology involved, all of the issues related to third party provision of information technology services, summarized in Part V.B of this paper, are applicable to cloud computing services. In particular, the issues summarized in Appendix A to this paper should be considered carefully in connection with any decision to move data or data processing to the cloud.

3. Ethical Considerations

Professional ethical issues may be triggered by the use of cloud computing by an attorney, including a franchise company's in-house attorney. That is so for several reasons, principally because client documents, correspondence, contacts, notes, billing information and more may be stored on remote servers rather than on the attorney's own computer. As a result, the attorney may not have complete control of the client materials and may not even know where they are located. On one hand, since one of an attorney's key duties is to safeguard client confidentiality, attorneys are understandably wary about sending client files offsite to a vendor's servers, particularly if such servers are located in remote jurisdictions. The attorney's duties extend beyond confidentiality, though, as attorneys must take appropriate precautions to prevent destruction or degradation of client files, and they must also be able to retrieve client data in a format that is usable in a system other than the vendor's own product.

Balanced against these worries is the fact that, in many cases, files stored on a vendor's servers may more secure than those located on a typical attorney's computer or a typical law firm's computer system, as cloud service vendors often use security measures not regularly found in the legal industry and may also operate with multiple redundant backups in their data centers.

These circumstances create issues under several ethical principles, including the following:

- ABA Model Rule 1.1, which provides that "A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation."[169] Comment 8 to that Rule, revised in 2012, provides as follows: "To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, *including the benefits and risks associated with relevant technology*, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject."[170] Applying its version of Rule

---

[166] Paul M. Schwartz, *Information Privacy in the Cloud*, 161 U. PENN. L. REV. 1632 (2013).
[167] *Id*. at 1623.
[168] Article 29 Data Prot. Working Party, Opinion 05/2012 on Cloud Computing 17, (EC) No.01037/12, WP 196 (Jul. 1, 2012), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf.
[169] AMERICAN BAR ASSOCIATION, MODEL RULES OF PROFESSIONAL CONDUCT 1.1 (2013) (emphasis added)(hereinafter, "Model Rules").
[170] *Id*., Comment 8.

1.1 in 2009 to an attorney who wanted to offer clients a service that would permit them online access to view and retrieve their client files, the Arizona Bar stated, "It is … important that lawyers recognize their own competence limitations regarding computer security measures and take the necessary time and energy to become competent or alternatively consult available experts in the field."[171]

- ABA Model Rule 1.6, which provides that "A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent [or] the disclosure is impliedly authorized in order to carry out the representation."[172] The Rule was amended in 2012 to include the following: "(c) A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."[173] Revised Comment 18 to that Rule reads in part as follows: "Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use)."[174]

- Because cloud computing is a form of outsourcing, ABA Model Rule 5.3 comes into play. That Rule provides, "With respect to a nonlawyer employed or retained by or associated with a lawyer: (a) a partner, and a lawyer who individually or together with other lawyers possesses comparable managerial authority in a law firm shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that the person's conduct is compatible with the professional obligations of the lawyer."[175]

Applying state counterparts to these Rules, 14 state bars or their ethics committees have opined that cloud computing by attorneys is permitted, subject to the general standard of reasonable care and subject to additional requirements or recommendations that vary from state to state.[176] For example, the Pennsylvania Bar opined that "An attorney may ethically allow client confidential material to be stored in 'the cloud' provided the attorney takes reasonable care to assure that (1) all such materials remain confidential, and (2) reasonable safeguards are employed to ensure that the data is protected from breaches, data loss and other risks."[177] The opinion went on to observe that the standard of reasonable care for cloud computing may include the following:

- Backing up data to allow the firm to restore data that has been lost, corrupted, or accidentally deleted;

- Installing a firewall to limit access to the firm's network;

- Limiting information that is provided to others to what is required, needed, or requested;

[171] State Bar of Arizona, Ethics Opinion 09-04 (2009).
[172] Model Rules 1.6.
[173] *Id*.
[174] *Id*., Comment 18.
[175] Model Rules 5.3.
[176] Cloud Ethics Opinions, *supra* note 157.
[177] Pennsylvania Opinion, *supra* note 158, at 1.

- Avoiding inadvertent disclosure of information;
- Verifying the identity of individuals to whom the attorney provides confidential information;
- Refusing to disclose confidential information to unauthorized individuals (including family members and friends) without client permission;
- Protecting electronic records containing confidential data, including backups, by encrypting the confidential data;
- Implementing electronic audit trail procedures to monitor who is accessing the data;
- Creating plans to address security breaches, including the identification of persons to be notified about any known or suspected security breach involving confidential data;
- Ensuring the provider:
    - explicitly agrees that it has no ownership or security interest in the data;
    - has an enforceable obligation to preserve security;
    - will notify the lawyer if requested to produce data to a third party, and provide the lawyer with the ability to respond to the request before the provider produces the requested information;
    - has technology built to withstand a reasonably foreseeable attempt to infiltrate data, including penetration testing;
    - includes in its "Terms of Service" or "Service Level Agreement" an agreement about how confidential client information will be handled;
    - provides the firm with right to audit the provider's security procedures and to obtain copies of any security audits performed;
    - will host the firm's data only within a specified geographic area. If by agreement, the data are hosted outside of the United States, the law firm must determine that the hosting jurisdiction has privacy laws, data security laws, and protections against unlawful search and seizure that are as rigorous as those of the United States and Pennsylvania;
    - provides a method of retrieving data if the lawyer terminates use of the SaaS [or cloud] product, the SaaS vendor goes out of business, or the service otherwise has a break in continuity; and,
    - provides the ability for the law firm to get data "off" of the vendor's or third party data hosting company's servers for the firm's own use or in-house backup offline.

- Investigating the provider's:
    - security measures, policies and recovery methods;
    - system for backing up data
    - security of data centers and whether the storage is in multiple centers;
    - safeguards against disasters, including different server locations;
    - history, including how long the provider has been in business;
    - funding and stability;
    - policies for data retrieval upon termination of the relationship and any related charges; and,
    - process to comply with data that is subject to a litigation hold.
- Determining whether:
    - data is in non-proprietary format;
    - the Service Level Agreement clearly states that the attorney owns the data;
    - there is a 3rd party audit of security; and,
    - there is an uptime guarantee and whether failure results in service credits.
- Employees of the firm who use the SaaS must receive training on and are required to abide by all end-user security measures, including, but not limited to, the creation of strong passwords and the regular replacement of passwords.
- Protecting the ability to represent the client reliably by ensuring that a copy of digital data is stored onsite.
- Having an alternate way to connect to the internet, since cloud service is accessed through the internet.[178]

Other state bar opinions, while not as detailed as the Pennsylvania Opinion, contain their own list of issues and concerns to be dealt with before committing a client's information or communications to the cloud. An attorney doing so in any state should read the applicable state ethical rules, read any guidance opinions, fully understand the risks in dealing with a cloud provider, carefully negotiate with that provider and regularly monitor the provider's performance so long as the provider has any of the attorney's client data.

VII. CONCLUSION: WHAT DOES THE FUTURE HOLD?

Whether they like it or not, franchisors are now in the data privacy and security business. In our increasingly digital world, the personal information obtained from customers and others

[178] Pennsylvania Opinion, *supra* note 158, at 8-10.

has become an asset of ever-growing importance. Thus the collection, maintenance, use and protection of such information have become business imperatives for any franchise company. Moreover, the FTC's recent actions highlight a regulatory aim of trying to hold accountable the deepest pocket and the most valuable brand in any corporate system. Therefore, the argument will be that each franchisor has assumed supervisory responsibility for all of the consumer and employee information gathered in its name. Such an extension of potential liability would impose on franchisors duties never anticipated at the outset of most franchise systems, and therefore not expressly captured in contracts and insurance policies.

The only constant in this area of the law will be change. As data privacy and security challenges are driven by shifts in technology, social norms and expectations, governmental fashions, business processes and unforeseen Black Swan events, we can expect the unexpected. For example, recent disclosures concerning governmental electronic and drone surveillance activity have forced privacy issues onto the front page and ignited indiscriminate calls for sweeping new privacy controls likely to affect corporate interests as well; these same disclosures have also highlighted the uncomfortable mismatch between American and European models of data protection. For franchisors and their counsel, evaluation and mitigation of these risks is not a one-time or one-country endeavor. While this paper has surveyed the current state of play with respect to this type of regulation, the final word has not yet been written.

APPENDIX A:

CHECKLIST OF ISSUES FOR DATA SERVICES PROVIDER CONTRACT[1]

1. Data: what is the nature of the information to be handled by the provider?

2. Statutory obligations

    a. Based on issue 1, what statutory obligations apply to this information?

    b. Are there regulatory or other restrictions on the data owner's ability to transfer specific data sets to the provider?

    c. Do any applicable laws require the execution of specific data protection/security clauses for the provider or any employees, representatives or subcontractors?

3. Service availability

    a. What commitments will the provider make as to service availability, including data replication and relevant service levels?

    b. What commitments are made with respect to disaster recovery and restoration?

4. Access to data

    a. What data protections are in place?

    b. Who at the provider will have access to the owner's data?

    c. Does the provider commit to prevent third party access to data and enable data to be retained for appropriate periods in order to comply with applicable law and applicable disclosure?

    d. Is the provider obliged to notify the owner following receipt of a subpoena or other request from any law enforcement regarding the owner's data?

5. Authentication

    a. What procedures are in place to manage authentication and encryption key management?

    b. What processes address verification of key personnel of the provider and its subcontractors?

6. Audit rights

[1] *Adapted from* Cloud Security Checklist Project Working Group, Cyberspace Law Committee, American Bar Association, *Cloud Security Checklist* (draft of May 6, 2013).

a. Does the owner have the right to audit the technical and organizational security measures of the provider?

b. May the owner obtain copies of the provider's own audit reports?

c. Will the provider allow for penetration testing?

7. Security standards/security certifications

a. Disclose all security standards to which the provider adheres and explain how security is managed on behalf of the provider.

b. Does the provider use encryption to protect stored data?

8. Integrity

a. Determine whether the owner's data is commingled with third party data and, if so, how integrity is managed and how third party access to data is controlled.

b. What other technological measures does the provider use to protect the owner's data integrity?

9. Privacy/regulatory compliance

a. Obtain assurances that the provider is compliant and will remain compliant with applicable privacy laws.

b. Determine how the provider enables the owner to comply with applicable data protection laws.

c. What amendments need to be made to the provider's agreement to make the ensure compliance?

10. Confidentiality: confirm how the provider protects the confidentiality of the owner's information.

11. Data breaches

a. Does the provider's agreement describe the provider's data breach procedures?

b. Does the agreement allow the owner to investigate such breaches separately or require the provider to assist any investigations conducted by government privacy regulators?

11.3 What forensic analysis tools, if any, does the provider have to analyze any data breach?

12. Operational security: does the agreement describe the provider's operational security policies and procedures?

13. Jurisdiction

    a. Does the agreement identify the location of the provider and of the server or servers on which personal information will be hosted?

    b. Will the provider commit to storing the personal data in a specific jurisdiction? Is this stated clearly in the agreement?

    c. If other than the data owner's home jurisdiction, do any laws in the owner's jurisdiction prohibit movement of personal information or outside that home jurisdiction?

    d. What law applies to the agreement and how will it be enforced?

14. Discovery

    14.1 Does the agreement contain provisions to assist in e-discovery?

    14.2 Describe the architecture of the provider's system, how data will be stored and in what format and what tools are provided to enable the owner's data to be accessed in the event of e-discovery or e-disclosure.

15. Business continuity

    a. What is the provider's disaster recovery plan and what will happen to the owner's data in the event of a disaster?

    b. How will the provider's management of data impact the owner's business continuity plan and processes?

16. Contract terms

    a. Does the agreement impose practical and commercial controls on the rights and responsibilities of the provider?

    b. Does the agreement adequately describe the physical, technological and organizational controls put in place by the provider to protect personal information?

    c. How is compliance with any contractual provision audited or auditable by the owner?

17. Insurance

    a. What insurance cover does the owner carry in respect of the specific risks raised by use of the provider's services?

    b. Does the use of the provider's services negate any existing insurance which the owner currently carries?

    c. Does the owner need to purchase more specialized insurance products, including cybersecurity/cyberliability?

d. What insurance do the provider and its subcontractors carry?

e. What cyber risk insurance does the provider have in place for the benefit of the owner?

f. Is the insurance coverage appropriate to the potential risk and related financial liability?

18. Portability

a. What portability rights does the owner have or need in respect of the movements of data both during and at the end of the agreement with the provider?

b. Does the agreement provide for "step-in" rights?

c. Does the agreement with anticipate and provide for portability rights of data subjects that may require removal of their specific data?

19. Rights on termination

a. Regardless of the cause of termination, will the owner's data be available to the owner in a portable and useable format for as long as is reasonably necessary on and after termination?

b. Can the owner's data be held hostage, depending on the nature of the termination?

c. Post-termination, how does the owner manage the return, removal or destruction of personal data from the systems of the provider?

d. Does the agreement describe in adequate detail the way in which the provider will actually delete or return the owner's data?

e. Does the agreement also address the deletion or return of any owner data managed by subcontractors?

f. Does the agreement anticipate the ongoing retention of certain of the owner's data? If so, in what form and for what purpose?

g. Will there be additional costs for data retrieval in a format acceptable to owner? Are these described in the agreement?

20. Subcontracting

a. Does the provider use subcontractors to provide any of its services?

b. If so, how will the owner control or exercise governance over such subcontractors?

c. What rights contractually does the owner have over subcontractors and other third parties that the provider may engage during the term of the agreement?

d. Where necessary, how will the owner establish the suitability of specific staff or subcontractors who will have access to the owner's data, particularly in the case of sensitive personal data?

21. Records Retention

a. What mechanisms are in place to guarantee the integrity of a record maintained by the provider?

b. How does the provider assure protection of any data or records maintained by the provider?

c. How accessible is the data in the event of a compliance audit by an agency or auditor?

d. To whom is the data made available besides members of owner's organization?

e. What procedures are in place to assure disposition of records and data in accordance with owner's records retention schedule?

f. Does the provider allow for original records to be pulled out of their systems for historical preservation or archiving?

SPEAKERS' BIOGRAPHIES

MICHAEL K. LINDSEY

Michael is a partner in the Los Angeles office of Paul Hastings LLP, an international law firm with offices in major business centers across Asia, Europe and the U.S. He is a corporate and transactional lawyer, with a practice concentration in the areas of franchise, distribution and intellectual property law. Michael's practice includes the acquisition, development, protection and licensing of various forms of intellectual property; antitrust preventive counseling; merger analysis and structuring; franchise disclosure, registration and relationship matters; and advice concerning the sale, distribution and marketing of products and services through manufacturing, joint venture, distribution, dealership and agency relationships. He has spoken and written extensively in these fields. He serves as co-editor-in-chief of INTERNATIONAL FRANCHISE SALES LAWS (ABA 2006 and 2009 - 2011 supplements). He is also a co-author of ANTITRUST HANDBOOK FOR FRANCHISE AND DISTRIBUTION PRACTITIONERS (ABA 2008), THE INTELLECTUAL PROPERTY HANDBOOK: A PRACTICAL GUIDE FOR FRANCHISE, BUSINESS AND IP COUNSEL (ABA 2005), ANNUAL FRANCHISE AND DISTRIBUTION LAW DEVELOPMENTS 2003 (ABA 2003) and INTERNATIONAL SALES TRANSACTION CHECKLIST (IBA 2003).

Michael has been active for a number of years in various Bar organizations, including the ABA Forum on Franchising, for which he has served as a member of the Governing Committee, co-chair of the 2011 annual meeting and Director of the International Division. He currently serves as Treasurer and Trustee of the Los Angeles County Bar Association and member of the Executive Committee of the USC Intellectual Property Law Institute. His recent past positions include chair of the Computer Industry & Internet Committee of the ABA Section of Antitrust Law, member of ABA Steering Committees on Continuing Legal Education and Technology and Information Systems, and officer of the International Franchising Committee of the International Bar Association. Michael is listed in THE BEST LAWYERS IN AMERICA, CHAMBERS GLOBAL, CHAMBERS USA, SUPER LAWYERS and in WHO'S WHO LEGAL.

MARK S. MELODIA

Mark leads Reed Smith LLP's Global Data Security, Privacy & Management practice as a partner within the Global Regulatory Enforcement Group. He has recognized experience in litigating putative class actions in the data security/privacy area.

Mark has led defense efforts in more than 70 putative class actions arising from alleged consumer privacy violations. Mark routinely represents clients responding to government privacy investigations, including before the Federal Trade Commission, the Office for Civil Rights, the State Attorneys General, and the United States Department of Justice.

Mark defended the first joint privacy investigation by the FTC and the OCR enforcing HIPAA. He has also served as lead defense counsel for both Macy's and jcp in negotiating and securing approval in nationwide class action settlements over use of HTML and Flash Cookies / Local Shared Objects ("LSOs"). Mark is currently lead counsel for Blizzard Entertainment (the industry-leading online game company which publishes World of War Craft) in a CDCA putative nationwide class action arising from a data theft.

Mark was recognized by Chambers USA 2012 as a notable practitioner in the area of Privacy & Data Security: Nationwide and was recognized again by The Legal 500 United States for regularly advising clients "on the issues that arise from the actual and potential breaches of personal information". Mark also was named in 2011 by Law360 as one of four national MVPs in Privacy & Consumer Protection. Further recognition of Mark's intellectual leadership in this field is found in the recent Big Data cover feature of Mark in Law Technology News, his lecture at NYU School of Law on privacy issues in employment law, his election to the American Law Institute, and his presentations on privacy and litigation risk to the Defense Research Institute.