Ownership, Protection and Use of Customer Data – Yours, Mine or Ours?

Robert L. Ebe
Bingham McCutchen LLP
San Francisco, California

and

Howard E. Bundy
Bundy & Morrill, Inc., P.S.
Seattle, Washington

October 10 – 12, 2007
JW Marriott Desert Ridge
Phoenix, AZ
TABLE OF CONTENTS

I. INTRODUCTION ..............................................................................................................1

II. OWNERSHIP ..................................................................................................................2
   A. Introduction ...........................................................................................................2
   B. Trade Secrets .......................................................................................................5
      1. Background/Overview of Trade Secret Law .............................................6
      2. The “Easy” Case .....................................................................................11
      3. Franchisee Efforts ...................................................................................13
         a. Employment Authority Background .............................................13
         b. Franchise Relationship Authorities .............................................16
            i. What If Customers Share Data With Others? ...................17
            ii. What Is The Significance Of The Franchisee
                Having Participated In Developing, Or Developed
                On Its Own, The Customer Data? ...................................19
      4. What If The Data Remains In the Franchisees’ Memories? ...................22
      5. Franchisees’ Assertions Of Their Own Trade Secret Rights In
         Customer Data........................................................................................23
      6. Joint Ownership Issues ...........................................................................25
      7. Trade Secret Rights May Be Assigned ...................................................26
   C. Contract Restraints On Customer Data Which Is Not A Trade Secret ...............28

III. PRIVACY ...................................................................................................................33
   A. Restrictions On Gathering, Using and Sharing Information..........................33
      1. Privacy Policies Found On Websites: In General, No Federal
         Requirement To Implement A Privacy Policy .....................................34
      2. Gathering Information Online Regarding Minors .................................35
      3. Gathering Information Through Telemarketing .....................................36
      4. Social Security Numbers ........................................................................36
      5. Spyware .................................................................................................37
      6. Do Not Call Lists ..................................................................................38
      7. E-Mail Marketing ...................................................................................38
   B. Sharing Data Between Franchisor and Franchisee ............................................40
TABLE OF CONTENTS

(continued)

C. Protecting Data After It Has Been Legally Gathered ........................................... 41
   1. Security Safeguards ......................................................................................... 41
   2. Notification To Consumers Regarding Disclosures To Third Parties ................ 44
   3. Companies That Issue Credit Card Receipts: FACTA .................................... 45
   4. Destroying Data .............................................................................................. 46
D. Breach of Security .................................................................................................. 46
   2. Franchisor/Franchisee Issues ............................................................................ 48
E. Special Industry Standards ..................................................................................... 50
F. International Laws .................................................................................................. 52
   1. The European Union ......................................................................................... 53
   2. Canada .............................................................................................................. 55
G. What Does It All Mean? ......................................................................................... 57
   1. Class Action Law Suits ..................................................................................... 57
   2. Problems Unique To The Franchisor/Franchisee Relationship ......................... 58

IV. CONCLUSION .......................................................................................................... 59

EXHIBIT A - Status of State Adoption of Uniform Trade Secrets Act

EXHIBIT B – Definitions
I. INTRODUCTION

Businesses have always had access to, and collected, information about their actual or prospective customers. The most obvious type of information is that necessary to complete a transaction. As customers, we routinely give up our names, addresses and credit card numbers for these purposes. Some businesses need more information in order to provide what we want, such as highly personal financial information to prepare our taxes, personal medical information to ease our back pain, or our children’s school records to facilitate their testing. Many businesses request more information in order to serve our personal preferences, and to advertise and market directly to us for future business. They keep track of whatever we reveal. This includes details such as room preferences, companion names, passport numbers, passwords, pet breeds and names, favorite pizza toppings, or whether we want a GPS unit in our rental car. All of this gathering could, and often did, happen before computers or the internet. Technology has now made it easier to collect, store, use and share all of this data.

In addition to data that we provide voluntarily, businesses collect data in largely invisible ways that reveal even more private information about us. Techniques range from video images of us while in the business, to installing cookies on our computers, to collecting data about what parts of a web site we click on, and in what order, and how we behaved in response to the information received on the last click. The types of things that constitute customer data are very broad indeed.1

A lot of people need or want access to customer data in franchise systems. Franchisors and franchisees may share our information between themselves. They may also share it with other businesses, affiliated or not, who might use our information for their own marketing or other purposes. Vendors and suppliers might need or want customer data for some legitimate reasons relating to the value they provide a franchise system, and they would not mind having the data if their relationships with the franchisor sour and they want to sell directly to or target its customers, perhaps through other firms. See, e.g., General Business Servs., Inc. v. Rouse, 495 F. Supp. 526, 531-32 (E.D. Pa. 1980) (list of franchisees was franchisor’s trade secret vis-à-vis vendor); Jan Marini Skin Research, Inc. v. Allure Cosmetic USA, Inc., Nos. A108613, A108631, A108633, 2007 WL 1508686, at *13-18 (Cal. Ct. App. May 24, 2007) (unpublished opinion) (protecting brand seller’s trade secret against manufacturer/supplier’s wrongful use). Competitors and would-be competitors obviously would like to get access to customer data. They may want to get the customers for themselves, or use their data to plan more generally how better to compete. See, e.g., Physicians Interactive v. Lathian Sys., Inc., No. 03-1193-A, 2003 WL 23018270, at *1, 8 (E.D. Va. Dec. 5, 2003) (competitor’s employee misappropriated trade secrets in customer lists and information owned by host of interactive website for medical professionals by hacking into plaintiff’s computer system). Finally, there are the really bad guys, who would like access to personal information for illegitimate reasons. See, e.g., Cellco P’ship v. Data Find Solutions, Inc., No. 06-326 (FLW), 2007 WL 1521075 (D.N.J. May 22, 2007); cf. Four Seasons Hotels and Resorts, B.V. v. Consorcio Barr, S.A., 267 F. Supp. 2d 1268 (S.D. Fla. 2003).

The authors acknowledge with appreciation Heather Kabele, contributor to the Ownership section of this paper; Roxanne Torabian-Bashardoust, contributor to the Privacy section; and Rosanne Mah for her help in finishing the entire paper. Heather is a counsel, and Roxanne an associate, in the Los Angeles office of Bingham McCutchen LLP; Rosanne is an associate in the firm’s San Francisco office.

1 We use the term “customer data” broadly throughout this paper, unless otherwise indicated; however, in the privacy context, certain statutes define specifically what kinds of customer information are protected.
The value of customer data varies from industry to industry and from franchise system to system. To the extent customer data has value and is properly collected within a system, it must be protected in order to preserve and maximize that value. Customer data can be obtained from customers in the first instance by either the franchisor or its franchisees, or both. Who owns it? How is it protected?

Disputes over customer data generally arise when a relationship ends and someone wants to take and use the customer data. Franchisees often believe that customer relationships resulted from their in-the-field efforts giving them “sweat equity” ownership rights to the data. Franchisors argue that the franchisees agreed to pay royalties to license the franchisor’s marks and other intellectual property, as well as the know-how and other aspects of the franchise system, which attracted customers and earned profits. The goodwill generated from this system, manifested in the customers drawn to it, is generally reserved by franchise agreements as the property of the franchisor, and information about those customers is the franchisor’s, so the argument goes.

This paper is divided into essentially two parts. First we address the issue of ownership. This section will focus largely on the law of trade secrets and on contract provisions protecting customer data. Then we address some of the consequences of ownership of customer data. Burdens accompany the benefits, as reflected in the rapidly evolving laws that protect the privacy of the consumers, and require safeguards to ensure the security of the data collected about them. We provide a survey of these evolving laws. At various points, we offer some guarded observations as to what might be best practices in addressing some of these issues.

II. OWNERSHIP

A. Introduction

Customer information is a somewhat unusual asset. Other assets may change over time, as, for example, do recipes or software. But customer data, by its nature, changes constantly. In some systems, customer data already exists before the franchise relationship, and the franchisor can provide it to the new franchisee. In most systems, the franchisee, and often the franchisor, develops much, if not all, of the data as the relationship proceeds. Customer data may be stored purely in a franchisee’s mind, in a ledger book, or in a variety of databases, all conceivably organized in different types of compilations containing different types of information. For example, one might list names of insureds and types of insurance they have, and still another list might identify expiration or renewal dates for their policies. Some data is provided only by the franchisor to the franchisee. Other data is gathered by the franchisee, all or some of which it may share with the franchisor. Identifying a system’s customer data and keeping tabs on it can be more challenging than with other types of assets.

There are two main bodies of law addressing proprietary rights in customer data: trade secret and contract enforcement. When a dispute arises, a franchisor will often attempt to

---

2 Privacy laws generally provide little guidance as to who has ownership and other proprietary rights in customer data. They generally regulate obligations owed to the customers by those who have access to such data regardless of how they obtained access. The requirements of a very few of those laws depend upon ownership, but no cases have yet interpreted what ownership means in those contexts. See Part III below.

3 We do not discuss patent or copyright protection because in most cases those would not be appropriate methods to protect customer data. Patent or copyright protection generally results in detailed disclosure of the protected information, so its trade secret status can be lost. In addition, although trade secret status is potentially indefinite, Continued on following page
enforce contract provisions limiting the franchisee’s use of customer data, and simultaneously claim the franchisee misappropriated its trade secret or otherwise unfairly competed. These two theories are, of course, interrelated. We address trade secrets first for several reasons.

First, there are many different types of franchise systems in a large variety of industries, each of which has different uses for customer data, resulting in a wide range of contract provisions. The variability in contract terms and differences in enforceability stand in contrast to trade secret law, which is relatively consistent across the country, owing first to the Restatement of Torts and, more recently, the Uniform Trade Secrets Act (“UTSA”).

Second, many courts are more likely to enforce restrictive covenants regarding customer data if the data is a trade secret. California is a clear example. Trade secrets are an exception to its statute voiding most contracts that restrain people from engaging in business. Both patent and copyright protection only last for a term of years, at which point the information automatically becomes part of the public domain. Copyrights protect only forms of expression, not necessarily the content; while patent protection does concern inventions or discoveries, customer data compilation is very unlikely to have the elements of novelty, utility, and non-obviousness required. Customer data is an ever-changing compilation of dynamic and specialized information, as opposed to a static formula, process, product or design that would benefit from patent protection. Although there are other considerations which are beyond the scope of this paper, the authors believe that trade secret status and contractual provisions are the most appropriate protection for customer data. For additional information in this regard, see THE TRADE SECRET HANDBOOK: PROTECTING YOUR FRANCHISE SYSTEM’S COMPETITIVE ADVANTAGE 11-13 (Michael J. Lockerby ed., A.B.A. Forum on Franchising 2001); Jeffrey L. Fillerup & Robin M. Spencer, THE ONE WHO KNEW TOO MUCH: LITIGATION OF TRADE SECRET AND ESPIONAGE CLAIMS 10-12 (A.B.A. Forum on Franchising 2003); Ronald T. Coleman & Linda K. Stevens, TRADE SECRETS AND CONFIDENTIAL INFORMATION: RIGHTS AND REMEDIES 9-11 (A.B.A. Forum on Franchising 2000).

---

4 Franchise agreements treat this subject in various ways. Some simply ignore it, and do not even mention customers or customer data. Many such agreements acknowledge or grant general rights (usually to franchisors) that may create trade secret and other proprietary rights in customer data. Some of these use language creating good arguments; other language seems not to have contemplated customer data at all. Some agreements mention customer data, but in ways that are unclear, ambiguous or even contradictory as to the extent of rights and obligations intended or likely to be claimed, and by whom. Still other agreements are very clear and specific, expressly providing, for example, that all customer data is the property of the franchisor, that it must be returned at the relationship’s end and never disclosed, and franchisees cannot solicit business from or do business with their prior, nor any other system’s customers. Most agreements addressing customer data also contain a more general obligation not to compete. Agreements sometimes expressly assign or convey customer data rights to the franchisor.

5 California Business & Professions Code § 16600 provides that “every contract by which anyone is restrained from engaging in a lawful profession, trade, or business of any kind is to that extent void.” Exceptions to the statute permit enforcement of restrictive covenants in connection with the sale of the goodwill of a business and the dissolution of a partnership or limited liability company. CAL. BUS. & PROF. CODE §§ 16601-16602.5 (2007). A judicially-created exception permits covenants restraining competition to be enforced where necessary to protect against misappropriation of trade secrets or unfair competition. See Scott v. Snelling & Snelling, Inc., 732 F. Supp. 1034, 1043 (N.D. Cal. 1990); see also Jan Marini Skin Research, Inc. v. Allure Cosmetic USA, Inc., Nos. A108613, A108631, A108633, 2007 WL 1508686, at *13 (Cal. Ct. App. May 24, 2007) (internal citation omitted) (unpublished opinion).

A line of primarily Ninth Circuit Court of Appeals cases have also recognized a “narrow restraint” exception to Section 16600, under which a restrictive covenant is not void as long as the restriction imposed is limited, i.e., bars one from pursuing only a small or limited part of a business, trade or profession, leaving “a substantial portion of the market available to the employee.” See Edwards II v. Arthur Andersen LLP, 47 Cal. Rptr. 3d 788, 798 (Cal. App. 2006) (not citable by grant of review). The Edwards court rejected this approach as not authorized by statute, holding the noncompetition agreement there at issue to be invalid and a violation of California’s public policy unless on remand it was proven to fall under the trade secret exception to Section 16600. Id. at 803. The California Supreme Court has now granted review and will hear the issue of whether a noncompetition agreement between an employer and employee that prohibits the employee from performing services for former clients is invalid under Section 16600 unless it falls within the statutory or judicially-created trade secret exceptions to the statute. The restraint in Edwards prohibited working for any customer on whose account the former employee had worked during the 18 months before Continued on following page
Third, courts generally give broader enforcement to trade secret rights, often not subjecting them to reasonableness limitations as to scope, time and geography. Contractual provisions are often so limited, either by their own terms or by the courts. Thus franchisees can use the customer data a few miles away or after waiting a few months or years. Consequently, the starting place for enforcement is usually to try to establish that the data is a trade secret.

Fourth, contract provisions are to some extent beside the point of trade secret law. The UTSA expressly provides that it does not affect contractual liability, whether or not based on trade secret misappropriation, or other civil remedies not based upon misappropriation of a trade secret. UNIF. TRADE SECRETS ACT, § 7(b) (1985). See also Roger M. Milgrim, MILGRIM ON TRADE SECRETS § 1.01[3][a] (Mathew Bender & Co. 2007). Though a contract recital as to the existence of a trade secret can be an important factor, it is generally not dispositive. See, e.g., Roll Sys., Inc. v. Shupe, No. 97-12689-GAO, 1998 WL 1785455, at *4 n.3 (D. Mass. Jan. 22, 1998); Morlife, Inc. v. Perry, 56 Cal. App. 4th 1514, 1522 (Ct. App. 1997); Arcor, Inc. v. Haas, 842 N.E.2d 265, 271 (Ill. App. Ct. 2005) (mere presence of confidentiality agreement not determinative that customer information was trade secret). Trade secrets also can be found without such provisions. General Business, 495 F. Supp. at 531 (E.D. Pa. 1980) (franchisor told vendor to keep list confidential); Re/Max of Am., Inc. v. Viehweg, 619 F. Supp. 621, 623 (E.D. Mo. 1985) (customer lists were considered trade secrets where franchisor told employee that the customer lists were confidential and proprietary); Digital Dev. Corp. v. International Memory Sys., 185 U.S.P.Q. 136, 141 (S.D Cal. 1973) (there need be no express agreement to keep information secret; confidential relationship existed “by virtue of the negotiations” for purchase and sale of product). Calling something a trade secret in a contract and reciting that all of the elements have been met does not make it so. The requisite elements of a trade secret must, in fact, be established. The information must still have value, result from time and effort to compile, and adequate safeguards must have been adopted at all levels (including the franchisee level) to maintain its secrecy. See Re/Max, 619 F. Supp. at 625-26.

Finally, most courts address rights in customer data initially, if not principally, in the context of claimed trade secrets.\(^5\)

---

\(^5\) See, e.g., NaturaLawn of Am., Inc. v. West Group, LLC, 484 F. Supp. 2d 392, 398-399, 404 (D. Md. 2007) (enjoining former franchisee from further accessing plaintiff’s customer lists, regardless of contract restrictions, where plaintiff demonstrated that the information was obtained from plaintiff’s uniquely enhanced software, warranting trade secret protection); ReadyLink Healthcare v. Cotton, 126 Cal. App. 4th 1006, 1011 (Ct. App. 2005) (upholding preliminary injunction in favor of employer, regardless of the enforceability of the parties’ noncompete agreement, where there was sufficient evidence establishing former employee misappropriated trade secrets); Roll Sys., Inc. v. Shupe, No. 97-12689-GAO, 1998 WL 1785455, at *4 (D. Mass. Jan. 22, 1998) (in enjoining former employee’s use of former employer’s confidential customer lists, despite the seeming invalidity of the parties’ noncompete agreement, the court reasoned: information constituting a \textit{trade secret} “may not be used by a former employee regardless of whether … there has been a contract restricting its use”); General Business Servs., Inc. v. Rouse, 495 F. Supp. 526, 529 (E.D. Pa. 1980) (in the manufacturing and distribution business, it is not uncommon to form partnerships which involve the sharing of confidential data; however, where a business’s confidential customer lists and information represent a “material investment of … time and money,” such data constitutes a trade secret entitling it to “protection, independent of a non-disclosure contract”).
Thus we first review trade secret law as applied to customer data, sometimes identifying contract clauses that were germane to the courts’ resolution of particular cases. Then we discuss enforcement of contractual restrictive covenants in which customer data was considered apart from trade secret analysis.

B. Trade Secrets

Customer data is merely one among many types of information generated by a franchise system that might be a trade secret. For generally applicable trade secret law, we commend to you the excellent materials previously published by the Forum. Our focus is customer data.

Nor can we summarize here all of the huge body of law relating to trade secret claims in customer data, much of which arises in the context of employment relationships. Those authorities are germane to franchising, in that a franchisor’s own employees might try to take a franchisor’s customer data with them when they leave their jobs. See, e.g., Re/Max, 619 F. Supp. at 626 (E.D. Mo. 1985) (list of potential franchisees was trade secret protected from use by franchisor’s former employee). In addition, the franchise and distribution authorities involving customer data appear to rely to a significant degree on employment cases, as a source of the state’s law and also for guidance in how to apply it to the facts at hand.

Instead, we initially provide an overview of trade secret law and refer you to other sources for its details. We share all of the authorities of which we are aware involving customer data trade secret claims in the franchise and distribution context. We do so by discussing some of the issues that courts have tended to address. And in doing so we refer to some of the authorities from employment or other relationship contexts on which courts have relied.

In sum, arguably the “easiest” case for enforcing trade secrets is when the franchisor develops its own customer data and provides it to the franchisee, but that case is not without challenges. Franchisors must still meet the minimum requirements for a trade secret, including adequate steps to maintain secrecy, and for proving misappropriation, and not be too aggressive (or greedy) in the process of formulating supporting arguments. Decisions in these cases are very fact specific. Differences in result seem to be less from splits among courts on what the law is or how to apply it, than simply differences in facts and circumstances.

The more difficult case for a franchisor to enforce trade secret rights is where the franchisee participates in gathering the customer data. In this area, courts seem to be able to reach different results on similar facts.

We then discuss below some variations on this theme of franchisee efforts. One concerns whether a trade secret can exist in customer data found only in one’s mind. We also identify cases where franchisees have brought claims against franchisors asserting proprietary rights in customer data. We touch briefly on the issue of joint ownership of trade secrets, as to which there is little law, none of which we are aware involving customer data, but it seems

---


8 See, e.g., HANDBOOK, supra note 7, at 2, citing to four decisions illustrating customer lists as a potential type of trade secret for franchise systems, all of which were employment cases.
germane to the relationship between franchisees and franchisor. Finally, we examine whether persons in possession of customer data trade secrets may be held to agreements as to who owns or has the right to use the data.9

1. **Background/Overview of Trade Secret Law**

There are two principal sources for trade secret law: The Restatement of Torts § 75710 published in 1939, and the Uniform Trade Secrets Act, recommended for enactment in 1979 and amended in 1985.11 At least 43 states have adopted the UTSA in one form or another. See MILGRIM ON TRADE SECRETS § 1.01[b]; HANDBOOK, supra note 7, at 4 & n.1. A current list of states adopting the UTSA is attached as Exhibit A. The remaining states generally rely on the Restatement. Courts in UTSA states often still look to the Restatement for guidance. The principal differences between the two seem generally inconsequential to the determination of whether customer data is a trade secret.12

The UTSA defines a trade secret as follows:

“Trade secret” means information, including a formula, pattern, compilation, program, device, method, technique, or process, that:

(i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and

(ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.” UNIF. TRADE SECRETS ACT § 1 (4).

---

9 The UTSA does not prevent parties from contracting to transfer property rights, including in trade secrets. By its express terms, the Act does not preempt the availability of contract remedies, whether or not based on misappropriation of trade secrets. UNIF. TRADE SECRETS ACT § 7(b). The Commissioners’ Comment further states that the Act “does not apply to duties voluntarily assumed through an express or an implied-in-fact contract.” Id. Case law confirms the availability of contract to set forth who owns or has the rights to use trade secrets. See, e.g., American Family Mutual Ins. Co. v. Roth, 485 F.3d 930, 933 (7th Cir. 2007), discussed in further detail later in this paper.

10 The Restatement of Torts has been superseded by the Restatement (Second) of Torts, but the second Restatement does not contain a section corresponding to § 757 of the first Restatement. A more recent counterpart to § 757 of the Restatement of Torts can be found, however, in the Restatement (Third) of Unfair Competition §§ 39-43, which was issued in 1995.

11 In addition, the Economic Espionage Act of 1996 prohibits the theft of trade secrets “related to or included in a product that is produced for or placed in interstate or foreign commerce . . . .” 18 U.S.C. § 1832(a) (2007). Private entities lack standing to assert civil actions under the statute, which provides for severe criminal penalties in the event of violation. We have found no cases applying this statute to the theft of customer data.

12 The Restatement definition of a trade secret does not include “negative know-how” and “blind alleys,” i.e., information about failures or past mistakes. The UTSA also does not require, as does the Restatement, that information be in “continuous use in operation of the business.” See HANDBOOK, supra note 7, at 2-5. Neither of these subjects seems particularly important to customer data.
Some adopting states modified the UTSA. Five states specifically added customer information to the list of items that may be trade secrets.¹³

Actual or threatened misappropriation may be enjoined. Complainants may also recover damages for their actual losses or the defendant’s unjust enrichment, in addition to receiving up to doubled exemplary damages. The UTSA displaces any law of civil liability for misappropriation, but it does not affect contractual or other civil liability or relief not based on misappropriation, or criminal liability.¹⁴ Misappropriation is defined as follows:

---


¹⁴ See supra note 11. The extent to which torts other than trade secret misappropriation are preempted by the UTSA is a complex issue that varies by jurisdiction. The debate and differences in approach regarding this issue center on the purpose behind the UTSA’s preemption provision and whether recognizing alternative tort claims to protect confidential information not rising to the level of trade secrets would render that provision effectively meaningless. For a more extensive discussion regarding preemption, see Coleman & Stevens, supra note 3, at 13-15. See also Tait Graves, Nonpublic Information and California Tort Law: A Proposal for Harmonizing California’s Employee Mobility and Intellectual Property Regimes Under the Uniform Trade Secrets Act, 2006 UCLA J.L. & Tech. 1 (2006).

Some states, perhaps the majority that have considered the issue, deem alternative tort claims preempted by the UTSA to the extent the factual predicate for the claim is the same as that proffered to support a claim for trade secret misappropriation. See, e.g., Digital Envoy, Inc. v. Google, Inc., 370 F. Supp. 2d 1025, 1033-1035 (N.D. Cal. 2005) (California UTSA preempted claims for unfair competition under Bus. & Prof. Code § 17200 and unjust enrichment on ground they arose from the same common nucleus of facts as trade secret allegation); Tax Track Sys. Corp. v. New Investor World, Inc., No. 01C6217, 2005 WL 936638, at *9 (N.D. Ill. Mar. 24, 2005), aff’d, 478 F.3d 783 (7th Cir. 2007) (in denying common law claims for misappropriation and quantum meruit, court notes that the ‘ITSA preempts non-contract claims based on misappropriation of confidential information, as well as trade secrets.’); Bliss Clearing Niagara, Inc. v. Midwest Brake Bond Co., 270 F. Supp. 2d 943, 948-49 (W.D. Mich. 2003) (deeming preempted by MUTSA claims for conversion and common law trade secret misappropriation, and allowing remaining claims to proceed to the extent based on wrongful conduct independent of alleged trade secret misappropriation); but see Cerven Corp. v. Slater, No. 06-CV-2632, 2007 U.S. Dist. LEXIS 9966, at *5-12 (E.D. Pa. Feb. 13, 2007) (criticizing Bliss). Other states, relying on a body of law first articulated in the Restatement of Torts § 759 and now encompassed within the Restatement (Third) of Unfair Competition §§ 39-43, offer tort protection against the improper use of “confidential” information not rising to the level of trade secret. See, e.g., Stone Castle Fin., Inc. v. Friedman, Billings, Ramsey & Co., Inc., 191 F. Supp. 2d 652, 658-59 (E.D. Va. 2002) (claims not preempted by VUTSA at motion to dismiss stage; court concludes that unless it can clearly be discerned that the information in question is a trade secret, alternative theories of recovery cannot be dismissed as being preempted under the

Continued on following page
“(i) acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means; or

(ii) disclosure or use of a trade secret of another without express or implied consent by a person who

(A) used improper means to acquire knowledge of the trade secret; or

(B) at the time of disclosure or use, knew or had reason to know that his knowledge of the trade secret was

(I) derived from or through a person who had utilized improper means to acquire it;

(II) acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use; or

(III) derived from or through a person who owed a duty to the person seeking relief to maintain its secrecy or limit its use; or

(C) before a material change of his [or her] position, knew or had reason to know that it was a trade secret and that knowledge of it had been acquired by accident or mistake.” UNIF. TRADE SECRETS ACT § 1 (2).

Because trade secret cases are very fact specific, a trade secret proponent must be prepared to prove that its list or other compilation of customer data has economic value or gives it some competitive advantage over those who do not have it. The proponent should be prepared to show that it spent considerable time and resources to obtain and compile the data it seeks to protect—whether it is just a list of names or something more detailed about the customers. It must show that the information is not generally known or publicly available, and that the information is not readily ascertainable by others using proper means.

VUTSA); Pestco, Inc. v. Associated Prods., Inc., 880 A.2d 700, 708-09 (Pa. Super. Ct. 2005) (competitor liable under theory articulated in Restatement § 759 for taking bills of lading containing confidential but not trade secret information). It is also worth noting that California, among other states, has recognized a distinct tort for breach of confidence; while typically used in California in connection with fact patterns involving the entertainment industry, it is not so limited by its legal elements and calls for the protection of information of a confidential nature that was communicated in confidence and improperly used by the defendant. See, e.g., Entertainment Research Group, Inc. v. Genesis Creative Group, Inc., 122 F.3d 1211, 1226-27 (9th Cir. 1997) (denying California tort for breach of confidence with respect to alleged disclosure of manufacturing and design processes and prices that purchasers were paying for manufactured costumes; court notes that information must be “confidential and novel” but need not be protectable “as a trade secret” without explaining what the difference would be, if any, between confidentiality and secrecy).

Analysis of the preemption issue is made more difficult by the fact that courts sometimes appear to use the terms “trade secret” and “confidential information” interchangeably, or at least without discussion as to what the difference is between the two standards. See, e.g., id. See also Hickory Specialties, Inc. v. Forest Flavors Int’l., Inc., No. 99-5003, 2000 WL 687681, at *8 (6th Cir. May 19, 2000) (unpublished opinion) (under Tennessee law, “trade secret and confidential information mean substantially the same thing”).

8
Customer list cases depend largely on the particular industry and its economics. If everyone in the trade knows whom an employer targets, or who its actual customers are, or they can easily learn that information, a list of these people would not be a trade secret. If, on the other hand, the nature of the market makes difficult learning who actually buys from whom, then the list might be protected. A list revealing not just names but also key information about customers which cannot be learned easily—such as dates of expiration and renewal of insurance policies, or the likes and dislikes of a hotel's repeat guests—is more likely to be a trade secret. See, e.g., *ABBA Rubber Co. v. Seaquist*, 235 Cal. App. 3d 1, 19-20 (Ct. App. 1991) (contrasting two hypotheticals distinguishing circumstances creating trade secrets).

In addition, the proponent must have used reasonable efforts to maintain its information's secrecy. That includes efforts to ensure that those with whom the proponent shares the information, including franchisees or their employees, will keep it secret, too. See generally, *Milgrim on Trade Secrets* § 1.04; *Handbook*, supra note 7, at 23-35.

One of the leading treatises on trade secrets, *Milgrim on Trade Secrets*, supra, spends over 50 pages summarizing the law from all jurisdictions on claims that customer data qualifies as trade secrets. See § 1.09[7]; see also *Trade Secrets Practice in California* § 1.5 (2d ed., Continuing Educ. of the Bar - Cal. 2006) (customer lists). Milgrim categorizes the cases by separating retail "route" from wholesale customer lists, a distinction that existed in early cases and he concedes is "arbitrary." See § 1.09[7]. He distinguishes further within these categories between the absence or presence of restrictive covenants. *Id.* Milgrim's analysis is premised largely on the equities of restraining employees who are changing jobs, a situation generally different from franchise and distribution relationships. See *id*.

On this basis, Milgrim concludes that retail customer lists without restrictive covenants have received "uncertain treatment" from jurisdiction to jurisdiction, and "have not generated enforcement in a majority of cases," but that "no clear majority rule can be stated." *Id.* at § 1.09[7][a][ii]. By contrast, it is "almost universal that a [retail] customer list which has some basis for a claim of secrecy can be protected by a restrictive covenant," with reasonable limitations. *Id.* Wholesale customer lists not protected by restrictive covenants "are seldom accorded protection" according to Milgrim, *id.* at § 1.09[7][b][i], while the majority rule upholds protection by reasonable restrictive covenants. *Id.* at § 1.09[7][b][ii]. One lesson from this admittedly arbitrary and somewhat confusing analysis is, of course, that franchise agreements should be drafted to include as many protections as are desired of customer data, even though those provisions alone may not ensure protection.

Most cases in this area arise in the context of a preliminary or final injunction of some type, as well as damages for misappropriation. Principles of equity are therefore generally at issue. An insightful illustration of how these concepts are applied (though not in a distribution relationship) is *Surgidev Corp. v. Eye Tech., Inc.*, 648 F. Supp. 661, 680 (D. Minn. 1986) (applying both California and Minnesota law under the UTSA), which involved a variety of different kinds of customer information in the technical field of ophthalmology. The *Surgidev* plaintiff's claims against its former employee included trade secret misappropriation and breach of contract. *Id.* at 668. The employment agreement prohibited him from competitive planning during his employment, from disclosing plaintiff's trade secrets for ten years after his job ended, and from soliciting plaintiff's customers for five years after that. *Id.* at 675-677. The court relied upon the Ninth Circuit's decision in *Hollingsworth Solderless Terminal Co. v. Turley*, 622 F.2d 1324 (9th Cir. 1980), itself reliant on a California Court of Appeal decision, *California Intelligence*
Bureau v. Cunningham, 83 Cal. App. 2d 197 (Ct. App. 1948), all of which were focused on the requisites for trade secret status of customer information.15

Surgidev held that an injunction prohibiting customer solicitation by a former employee is appropriate where:

“(1) the former employee is in possession of trade or business secrets or confidential information, or the like, not readily accessible to others; (2) the former employee solicits the customers of his former employer in a competing business with intent to injure his former employer's business; (3) the former employee solicits the customers of his former employer, who comprise a list of preferred customers whose trade is profitable to a supplier of a service, knowledge of whom is a trade secret and confidential; (4) one concern is usually patronized by a customer and the lists and names and addresses of the customers are considered secret and have the character of property; (5) there is an established business relationship between the customer and the former employer which, unless interfered with, normally continues.” Id. at 681.

The following additional principles obtain in applying these factors:

“(1) although in most instances where customer information will be protectible as a trade secret all five of the circumstances described above will be present, California law is best viewed as not requiring a plaintiff to prove all five in order to prevail;

(2) it is not essential for the employer to demonstrate that its efforts, as opposed to the employee's independent efforts, were principally responsible for development of the customer information, although this is one factor to be considered;

(3) a list of plaintiff's customers may be a trade secret even where the general class of potential customers is obvious and readily accessible.” Id. at 681-82.

15 California is in the minority of states that do not enforce post-term non-competition clauses, but an exception to that rule exists for trade secrets. Milgrim has opined that California is “a leading state in the protection of the customer relationship as a form of trade secret” and has a “generally protective position.” MILGRIM ON TRADE SECRETS § 1.09[7][a][i]. Thus we submit that California law is worth considering generally in this area.

In addition, the California Intelligence decision contrasted factors from a second group of cases in which former employees generally will not be enjoined from using customer data:

“(1) the customers solicited (a) do not constitute a trade secret, or confidential information, or a confidential list in which a proprietary interest might be claimed, or (b) are commonly known to the trade and are called upon by salesmen for various companies, or are wholesale buyers whose names appear in directories and are so few in number that anyone might readily discover them, and the list of them is not secret or confidential; (2) the former employer is in open competition with others engaged in similar business, selling in an open, competitive market; (3) the former employee was a salesman of his former employer in a commercial field where there was no assurance of an order unless he could satisfy his customer that his product was better, cheaper, or more salable than that of his competitor, where the customer usually desired to examine, inspect and compare the product and prices offered to him and each sale was a distinct transaction, not necessarily implying that another will follow; (4) no secret or trust reposed in the former employee in the course of his employment is violated and no trade or business secret or confidential information is used by the former employee.” California Intelligence, 83 Cal. App. 2d at 202-03 (Ct. App. 1948).

An ex-employee has a right “to use anything that is not the property of his employer. Trade and business secrets and confidential information are the property of the employer and cannot be used by the employee for his own benefit. A list of [customers] built up by ingenuity, time, labor and expense of the owner over a period of many years is property of the employer, a part of the good will of his business and, in some instances, his entire business.” Id. at 203.

With this background in mind, we turn to franchise and distribution cases involving customer data. There are not nearly as many such cases as those involving employment relationships that analyze to any significant extent a claim that customer data is a trade secret. They exist, however, and we present them in this paper.

2. The “Easy” Case

Arguably the “easiest” case is where the franchisor develops its own customer data and provides it to franchisees at the relationship’s inception, or afterwards. It is relatively easy to segregate this data, designate it as confidential, monitor its usage, and protect its secrecy; documenting efforts to generate it also should not be hard. Such a case is Great Expectations Franchise Corp. v. V.L.P. Enterprises, Inc., Bus. Franchise Guide (CCH) ¶ 11,434 (S.D. Cal 1998). A franchisor of a social introduction service center terminated a franchisee. Id. at 30,778. When the franchisee did not de-identify, the franchisor sought a preliminary injunction against continued trademark infringement and misappropriation of trade secrets in the form of “membership data,” including customer names, profiles, videos, photographs, and lists of

---

16 We consider together cases involving both franchise and distribution relationships including those not regulated by the Federal Trade Commission’s Franchise Rule, or other franchise laws. They share the same types of business issues, are distinguishable from employment relationships and, we submit, are meaningfully analogous. We refer only to “franchises” from now on, but have in mind all such relationships.
former, present and prospective members. *Id.* at 30,778, 30,780. The franchisor established that it spent considerable effort gathering this data, and that it was a valuable asset of the franchise system. *Id.* at 30,781. The franchisor took “reasonable steps to maintain” the data's secrecy by, among other things, “directing its franchisees to establish procedures to safeguard” the data. *Id.* The court found that the information was a trade secret and ordered the franchisee not to compete unfairly, not to infringe on the franchisor’s copyrights or to misappropriate its trade secrets, and to turn over all of the protected materials. *Id.* at 30,778.

Another recent example is *NaturaLawn of America, Inc. v. West Group, LLC*, 484 F. Supp. 2d 392, 395-98 (D. Md. 2007), an action by the franchisor of an organic-based landscape and lawn care system against a former franchisee who repudiated its contract on “inexcusable,” “blatant” and “unjustified” terms. The contract prohibited the franchisee for 24 months after termination from using the marks, system, confidential information or trade secrets, and required return of all customer lists, which were expressly designated as the property of the franchisor. *Id.* at 396-97. The contract also prohibited the franchisee from competing within a 20-mile radius of the licensed territory. *Id.* at 397. The court held that the customer lists were trade secrets that identified the customers of the franchisor, who had developed them over time through expense and effort. *Id.* at 399. The court enjoined the franchisee from competing against the franchisor, using the franchisor’s trade secrets and advertising or otherwise using the franchisor’s trade name, stating that the franchisor was “certain to win its claims under the MUTSA, the Lanham Act, and for breach of contract.” *Id.* at 404.18

Franchisors do not always win these cases, however, particularly if they are overly aggressive in what they lay claim to and/or do not take care to present detailed evidence adequate to satisfy their burden of proof under the applicable factors.19

---

17 There is no other discussion of the terms of the parties' agreement, and even this language leaves unclear whether the "direction" was a term in an agreement, an operating manual, a letter or even an oral "direction."

18 See also *General Business Servs., Inc. v. Rouse*, 495 F. Supp. 526, 529 (E.D. Pa. 1980), where a franchisor sought trade secret protection against a terminated system vendor of a list of the system’s franchisee's customers to whom the vendor was trying to sell directly. The franchisor had given the list to the vendor for use in their business, told the vendor that the information was confidential, and required the vendor to destroy any replaced versions. *Id.* at 531. The court held that there did not have to be an express agreement to keep the information confidential; circumstances can establish that obligation, including the franchisor's statement. *Id.* at 529-32. The vendor claimed that the list was available through public sources. See *id.* at 531. It tried to prove this by replicating the system in the library, but its efforts were both time consuming and produced something significantly less than the list the franchisor was attempting to protect, thus further establishing the franchisor's claim. See *id.*

Similarly, in *Re/Max of Am., Inc. v. Viehweg*, 619 F. Supp. 621, 626 (E.D. Mo. 1985), a franchisor's list of potential customers, i.e., potential franchisees, was a trade secret misappropriated by its ex-employee who took the list to a competitor. The list was developed over time at a substantial investment. *Id.* The franchisor would suffer competitive injury if its competitors obtained it. *Id.* The employee was told the information was confidential and intended only for his use in his employment, not for any other purpose. *Id.* at 623. See also *Mutiut Corp. v. Draiman*, 834 N.E.2d 43, 45, 50 (Ill. App. Ct. 2005) (energy consulting service company entitled to trade secret protection for customer data vis-à-vis independent "associates," where the information was safeguarded by limiting access and requiring employees to sign confidentiality agreements); *MCL Fin. Group v. Bak*, No. G035192, 2006 WL 1320543, at *1-2 (Cal. Ct. App. May 12, 2006) (unpublished opinion) (tax strategy planning business entitled to injunction against licensed independent contractors for trade secrets in company-originated customer leads, including unique information about each person, which contract provided were property of owner, who spent time, money and effort to compile and used reasonable efforts to protect including computer passwords).19 E.g., *Winston Franchise Corp. v. Williams*, No. 91 Civ. 7963 (CSH), 1992 WL 7843, at *8 (S.D.N.Y. Jan. 10, 1992) (discussed in text below in greater detail; finding past and prospective customers not to be confidential because names and detailed information were readily ascertainable from outside sources); *P.A.L. Investment Group, Inc. v. Staff-Builders, Inc.*, 118 F. Supp. 2d 781, 786 (E.D. Mich. 2000) (franchisor did not rebut franchisee’s proof that it had Continued on following page
3. Franchisee Efforts

The courts seem to have had greater difficulty with resolving situations where the franchisor claims rights in more than what it created and gave its franchisee. These are situations where the franchisee has worked to develop customer relationships and/or generated the data for which the franchisor seeks trade secret protection. This is where the battle lines are often drawn in franchise litigation. The issue is sweat equity versus brand value. There seems to be less uniformity in the judicial decisions in this regard. Our sample review of franchise agreements shows little attention to this issue which, we submit, could often be resolved by careful drafting. Many agreements either ignore the issue, confuse it with ambiguous or inconsistent language, or give away the store altogether (sometimes, it seems, unintentionally).

The first franchise decision to address this issue was apparently Scott v. Snelling & Snelling, Inc., 732 F. Supp. 1034 (N.D. Cal. 1990). Scott, like many other franchise cases in this area, relied upon employment authority. It is therefore instructive to begin by reviewing the evolution of this debate in that area, which began well before the Uniform Trade Secrets Act was adopted.

a. Employment Authority Background

An early case, Avocado Sales Co. v. Wyse, 122 Cal. App. 627 (Ct. App. 1932), which illustrates the Milgrim categorization discussed earlier, involved a list of wholesale grocers and fresh produce stands who might buy avocados from the plaintiff. The court would not treat this list as a trade secret, by contrast with lists of retailers, because the names and addresses of wholesale buyers could be easily ascertained, they were solicited by other produce sellers, and they never bought exclusively from the plaintiff, but instead generally bought based on price and market conditions. Id. at 629, 634. Thus there was nothing secret about their identities. The court also observed that, in these circumstances, it was not equitable to enjoin a former employee who made personal friends and acquired personal knowledge of his customers to stop dealing with them. Id. at 634. “Equity,” the court stated in a phrase oft-repeated, “has no power to compel a man who changes employers to wipe clean the slate of his memory.” Id.

Fifty years later, in Moss, Adams & Co. v. Shilling, 179 Cal. App. 3d 124, 130 (Ct. App. 1986), another California court refused to give trade secret status to a rolodex of names and addresses (nothing more) of local people whose names a former employee of the plaintiff

boxed, stored and never used alleged trade secret customer/patient lists and records, so no likelihood of success on contract breach and trade secret claims; breaching franchisor could not enforce non-competition clause against rescinding franchise).

20 Avocado relied on a New York decision, Peerless Pattern Co. v. Pictorial Review Co., 132 N.Y.S. 37, 39 (1911), which may be the actual source of the quoted phrase “wipe clean the slate of [the employee’s] memory” in this context. Avocado Sales Co. v. Wyse, 122 Cal. App. 627, 632 (Ct. App. 1932). For the past 100-odd years since Peerless, this phrase or a paraphrase of it has shown up in numerous jurisdictions, including federal and state courts in New York, Indiana, Oregon, Kentucky, Pennsylvania, North Carolina, Illinois, Virginia, Ohio, Maryland, Wisconsin, Connecticut, Massachusetts, Oklahoma and New Mexico. See, e.g., PrimeCare Home Health v. Angels of Mercy Home Health Care, L.L.C., 824 N.E.2d 376, 382 (Ind. Ct. App. 2005) (“properly-acquired knowledge of the employer’s business is [not] automatically made a trade secret . . . simply because it [could] be compiled into . . . a list.”; employee not required to “wipe clean the slate of his memory”); IKON Office Solutions, Inc. v. American Office Prods., Inc., 178 F. Supp. 2d 1154, 1169 (D. Or. 2001) (noting that “[a] court cannot compel a man who changes employers to wipe clean the slate of his memory”); North Atlantic Instruments, Inc. v. Haber, 188 F.3d 38, 50 (2d Cir. 1999) (same, citing Peerless); and BJM & Associates, Inc. v. Norell Servs., Inc., 855 F. Supp. 1481, 1497 (E.D. Ky. 1994) (relying on California authority which held “[e]quity has no power to compel a man who changes employers to wipe clean the slate from [sic] his memory.”).
accounting firm knew from servicing them. This case, like *Avocado*, was not decided under California’s UTSA. In *Moss*, defendants, plaintiff’s former managerial employees, signed employment agreements stating that the names and addresses of plaintiff’s clients were trade secrets that could neither be revealed to others, nor used to solicit clients within one year of their termination. *Id.* at 126. When the defendants departed, they simply mailed the ex-clients a notice of change of employment, which is generally regarded not to be solicitation. *Id.* at 127. The plaintiff argued that, even so, using a trade secret (rolodex) to facilitate such a mailing was wrongful. *Id.* The court concurred that solicitation is not the only possible misuse of a customer list, but held that the defendants had not breached their employment agreements and that the names were not trade secrets because they became known, and a business relationship was developed, through personal contact and provision of accounting services. *Id.* at 128-29. The former employees would not be compelled to “wipe clean the slate of their memories” of those names. *Id.* at 129. As for the addresses, they were not trade secrets because they could be obtained easily from public phone directories. *Id.*\(^{21}\)

Thus was generated in California the controversial notion, particularly relevant to franchising, that customer data which might otherwise be a trade secret is denied that status if the purported purloiner had something to do with generating the information. More than one employment case has rejected this idea, in and outside of California, some quite forcefully, thus creating a split of authority. See *Liberty Mutual Ins. Co. v. Gallagher & Co.*, No. C94-3384 MHP, 1994 WL 715613, at *4 (N.D. Cal. Dec. 19, 1994) (acknowledging split of authority); *Roll Sys., Inc. v. Shupe*, No. 97-12689-GAO, 1998 WL 1785455, at *4 (D. Mass. Jan. 22, 1998) (accord).

Most of these cases have rejected an argument that, even if the information is a trade secret, former employees did not misappropriate contrary to an express non-solicitation agreement because they had personal relationships with the customers. See, e.g., *American Credit Indemnity Co. v. Sacks*, 213 Cal. App. 3d 622, 636 (Ct. App. 1989) (applying the UTSA to protect employer’s valuable trade secret in insurance customer information, and stating that “[p]roviding personal service to a customer whose identity is a trade secret does not thereafter render that customer fair game for solicitation.”).

An even more forceful rejection of the notion came in 1997 in *Morlife, Inc. v. Perry*, 56 Cal. App. 4th 1514, 1524-26 (Ct. App. 1997). In *Morlife*, plaintiff, a roof-repair firm catering to commercial clients, successfully sued its former employees, one of whom had signed an agreement stating that he would not use, duplicate or disclose customer data after the

---

\(^{21}\) This type of analysis and holding is not limited to California. See also, e.g., *Fish v. Adams*, 401 So. 2d 843, 845 (Fla. Ct. App. 1981) (in considering whether beauticians had breached their duty of loyalty to former employer in setting up a competing business, court considers whether beauticians had used confidential information acquired during the course of their employment to solicit customers prior to the end of their employment; court notes that an employee may take with him a customer list that he himself developed upon termination of the employment relationship); *Mittenzwei v. Indus. Waste Serv., Inc.*, 618 So. 2d 328, 329-30 (Fla. Ct. App. 1993) (former employee free to solicit customers where necessary showing that customer list entitled to trade secret protection not made and no noncompete agreement in existence; court notes that former employee cannot be precluded from using customer lists she developed or contacts and expertise gained during former employment); *United Aircraft Corp. v. Boreen*, 284 F. Supp. 428, 446-47 (E.D. Pa. 1968) (no unlawful misappropriation where customer lists were the product of employees’ own efforts, and the bulk of additions to the lists came from information contained in trade journals and listings in the telephone directory); *Leo Silfen, Inc. v. Cream*, 29 N.Y.2d 387, 395 (1972) (requiring customer list to be written, not just in memory, where no express confidentiality contract with employee protecting those lists). See generally *Corpus Juris Secundum, Employer-Employee Relationships* § 126 (2006) (former employee may take with him a customer list that he himself has developed, citing *Fish* decision).
termination of his employment, for misappropriation of trade secrets and violation of the UTSA. Id. at 1517-18. When the employees left, they took a collection of business cards, accumulated over years of employment, to a competitor. Id. at 1518. Morlife began by characterizing as “fundamental to the preservation of our free market economic system” the “right to have the ingenuity and industry one invests in the success of the business or occupation protected from the gratuitous use of that ‘sweat-of-the-brow’ by others.” Id. at 1520. Morlife then proceeded to attack as “artificial,” having “no legitimate reason” and “rest[ing] on an unsound premise” Moss’s distinction between employees who personally dealt with customers and those who did not. Id. at 1526. The “rubric of commercial impracticality in not being able to ‘wipe clean’ one former employee’s memory constitutes unjustified abandonment of legitimate regulation of competitive activity, and ignores the paramount interest in protecting … trade secret[s].” Id. Moss, the court held, “did not appropriately recognize that information developed by an employee about the employer’s customers “represents an investment of time and money on the part of the employer.” Id. (emphasis in original). Indeed, it is the former employee’s “personal acquaintance and additional influence of the friendship developed during his employment … which makes solicitation of former customers by [the employee] so unfair to his former employer.” Id. (emphasis in original); accord, Gable-Leigh, Inc. v. North American Miss, No. 01-01019 MMM (SHX), 2001 WL 521695, at *18 n.93 (C.D. Cal. April 13, 2001); Liberty Mutual, 1994 WL 715613, at *4, 6 (N.D. Cal. Dec. 19, 1994) (acknowledging split of authority in California and ordering former employee to return any list of customer prospects developed while at his employer); see also Surgidev Corp. v. Eye Tech., Inc., 648 F. Supp. 661, 681-82 (D. Minn. 1986) (principle #2, supra).\(^{22}\)

Lawyers on both sides of the franchisee/franchisor continuum often consider analogies to employment relationships in arguing their causes, particularly franchisee lawyers arguing that contract terms are unconscionable.\(^{23}\) Are the duties of loyalty in, and other aspects of,

\(^{22}\) Cases from other jurisdictions are in accord. See, e.g., North Atlantic Instruments, 188 F.3d at 49 (2d Cir. 1999) (granting injunction against use by former executive of trade secret customer data which he developed over many years; agreements required non-disclosure or use of confidential and trade secret matters including customer data); Fireworks Spectacular, Inc. v. Premier Pyrotechnics, Inc., 147 F. Supp. 2d 1057, 1066 (D. Kan. 2001) (granting injunction because former employee’s personal logbook and other customer lists were employer’s property even if only related to sales the defendant made; oral non-competition agreement); Deutsche Inv. Mgmt. Americas, Inc. v. Riverpoint Capital Mgmt., Inc., No. C-1-02-577, 2002 U.S. Dist. Lexis 16147, at *7,15-16 (S.D. Ohio 2002) (former investment manager required to return and not use rolodex of names and account numbers of customers including those who were defendants’ friends; status of client and friend is inextricably intertwined, and business must prevail over friendship). Cf. American Family Mutual Ins. Co. v. Roth, 485 F.3d 930, 933 (7th Cir. 2007) (enforcing non-solicitation clauses to protect trade secrets in customer data collected by franchisee, but in which contract granted proprietary rights to franchisor). See generally, 54A AM. JUR. 2d. MONOPOLIES, RESTRANTS OF TRADE, AND UNFAIR TRADE PRACTICES § 1122 (immaterial, in suit against former employee, whether employee herself compiled or added to the list in the course of employment, citing Rhode Island, Pennsylvania and Kansas law, and compare with CJS cited in note 21 above.

\(^{23}\) This argument has arisen in cases challenging as unconscionable certain arbitration provisions in franchise agreements and requesting fee-shifting for the costs of arbitrating statutory claims. In Independent Association of Mailbox Center Owners, Inc. v. Superior Court., 133 Cal. App. 4th 396, 410, 417 (Ct. App. 2005), the court stated that “franchise agreements . . . resemble employment agreements to the extent that the franchisees’ livelihoods are involved and subject to contractual arbitration for dispute resolution . . . ” and likened the franchise factual context to mandatory employer/employee arbitration in determining that certain of the arbitration provisions were unconscionable and that fee-shifting of some of the arbitration costs might be appropriate; accord, Nagrampa v. MailCoup, Inc., 469 F.3d 1257, 1282 (9th Cir. 2006) (noting that the relationship between franchisor and franchisee often involves unequal bargaining power and the use of contracts of adhesion presented on a take-it-or-leave-it basis – arguments commonly asserted by employees challenging as unconscionable arbitration provisions contained in employment agreements). Cf. Postal Instant Press, Inc. v. Sealy, 43 Cal. App. 4th 1704, 1715-16 (Ct. App. 1996) (analogyizing franchise and consumer agreements for purposes of unconscionability analysis); Jan Marini Skin Research, Inc. v. Allure Cosmetic USA, Inc., Nos. A108613, A108631, A108633, 2007 WL 1508686, *11 n.16 (Cal. Continued on following page)
employment relationships also present by analogy in franchise relationships sufficient to make the employment authorities apposite to franchisor's rights? What if the franchise agreement creates express obligations of confidentiality and non-disclosure comparable to those in the employment cases? With those questions in mind, we move to the franchise decisions that have evolved in this area.

b. Franchise Relationship Authorities

Scott v. Snelling & Snelling, Inc., 732 F. Supp. 1034, 1036 (N.D. Cal. 1990), involved a temporary employment agency franchisee who broke away to compete with the system. The court granted a preliminary injunction requiring the franchisee to provide customer lists to the franchisor; the franchisees had complied. Id. at 1037. The franchisee then sought summary judgment against enforcement of the post-term non-competition clause under the California statute voiding contracts restraining someone from engaging in a lawful profession, trade or business. Id. at 1037-45; CAL. BUS. & PROF. CODE § 16600 (2007). As stated earlier (note 5), a judicial exception to that rule of public policy exists, however, where enforcement is necessary to protect trade secrets or other confidential or proprietary information. Thus the court reached the issue of whether the customer lists were trade secrets, and held as a matter of law that they were not. Id. at 1045.

Snelling apparently did not rebut the franchisees' evidence that typical employer customers are companies of all sizes and sorts “easily discoverable through public sources.” Id.

24 Courts routinely say that nonsolicitation provisions are permissible to the extent necessary to protect trade secrets “or confidential proprietary information.” See, e.g., Thompson v. Impaxx, Inc., 113 Cal. App. 4th 1425, 1431 (Ct. App. 2003). The exception has also been described as permitting a restrictive covenant to be enforced "when the subsequent competition constitutes unfair competition, such as the unauthorized use of trade secrets or confidential information." Liberty Mutual Ins. Co. v. Gallagher & Co., No. C94-3384 MHP, 1994 WL 715613, at *2 (N.D. Cal. Dec. 19, 1994). Courts outside of California have likewise recognized that legitimate business interests protectable by restrictive covenants include, among other things, the protection of trade secrets and the prevention of unfair competition. See, e.g., Winston Franchise Corp. v. Williams, No. 91 Civ. 7963 (CSH), 1992 WL 7843, at *8 (S.D.N.Y. Jan. 10, 1992). See generally Coleman & Stevens, supra note 3, at 11-15 (discussing the enforceability of covenants in franchise agreements that restrict the disclosure and use of trade secrets and confidential information). In the context of customer data, we have found no cases applying the judicially-created exception in California to something beyond trade secrets. Perhaps that explains the court's restatement of the rule in a recent California decision, as follows: “Put another way, contracts that restrain trade are unenforceable where the information sought to be protected is not a trade secret under the UTSA.” Jan Marini, 2007 WL 1508686, at *13 (Cal. Ct. App. May 24, 2007). See also Surgidev Corp. v. Eye Tech., Inc., 648 F. Supp. 661, 697 n.19 (D. Minn. 1986) (applying California law chosen in agreement; to the extent customer information constitutes a trade secret, it may be protected under California law by a valid contractual covenant, and conversely, to the extent the information is not a trade secret, a contractual covenant which purports to restrict its use is to that extent invalid). For discussion regarding the availability of tort protection for “confidential” information not rising to the level of trade secret, see infra note 14.
Moreover, the franchisees established that they developed the lists through their own efforts, personal knowledge and business contacts. \textit{Id.} at 1045. Relying on Moss and \textit{Avocado}, the court stated that California courts have “repeatedly” held that a customer list is not a trade secret because “[e]quity has no power to compel a man who changes employers to wipe clean the slate of his memory.”\textsuperscript{22}

Employment agency cases generally involve two types of customer lists: (a) potential employers who may hire the agency and (b) potential employees. \textit{Scott} went on to hold that a second list of customers, \textit{i.e.}, temporary employees, was not a trade secret either. \textit{Id.} at 1045. The court acknowledged that this list may have “independent economic value by containing special information such as the employees’ skills and preferences which cannot be developed through resort to public sources.” \textit{Id.} Two factors kept the lists from protection, however. First, the lists are “non-exclusive” in that the temporary employees typically list themselves with a number of agencies, \textit{i.e.}, competitors. \textit{Id.} Second, the franchisees established that they developed these lists through their own efforts. \textit{Id.}\textsuperscript{28}

i. \textbf{What If Customers Share Data With Others?}

The first of these reasons is worth remembering in all cases such as these, not just where a franchisee’s efforts are involved. The idea seems to be that the information was about the customer, who was free to share it with others, and had in fact done so, thus rendering the franchisor’s list containing such information unprotectable. This is a superficially logical argument. Indeed, one court, in what we submit illustrates both somewhat more obvious circumstances and also an overly aggressive attempt to claim trade secret protection, held that the supposed trade secret information was the customer’s secret, if anyone’s, not that of the

\textsuperscript{22} To the extent this was the basis for the court’s holding that the lists were not trade secrets, it seems to have ignored that California did not adopt the portion of the UTSA requiring that the information not be “readily accessible to a reasonably diligent competitor or salesman,” which some courts regard as the “most important” factor. See \textit{Hollingsworth Soldierless Terminal Co. v. Turley}, 622 F.2d 1324, 1332 (9th Cir. 1980). California’s trade secret act only requires in this regard that the information not be “generally known to” the public or others who can gain economic value from knowing or using it. See \textit{CAL. CIV. CODE} § 3426.1(d)(1) (2007). See \textit{ABBA Rubber Co. v. Seaquist}, 235 Cal. App. 3d 1, 18-19 (Ct. App. 1991) criticizing \textit{American Paper & Packaging Prods., Inc. v. Kirgan}, 183 Cal. App. 3d 1318 (Ct. App. 1986), “to the extent that it suggests that information is not protectable as a trade secret if it is “known or readily ascertainable.”” \textit{ABBA}, 235 Cal. App. at 21 (emphasis in original). \textit{ABBA} did acknowledge, however, that this omitted definitional factor can be relied upon to disprove misappropriation. \textit{Id.} at 21 n.9. See \textit{Celeritas Technologies, Ltd. v. Rockwell Int’l Corp.}, 150 F.3d 1354, 1358 (Fed. Cir. 1998) (California law unsettled on this point); \textit{Jan Marini}, 2007 WL 1508686, at *12 (Cal. Ct. App. May 24, 2007) (acknowledging disagreement). Even if wrong under California law, \textit{Scott} is still instructive in states that have adopted the full UTSA.

\textsuperscript{28} \textit{Scott v. Snelling & Snelling, Inc.}, 732 F. Supp. 1034, 1044-45 (N.D. Cal. 1990). The court gave “see also” cites to two other California decisions that did not support this proposition. The former employee in \textit{American Paper}, 183 Cal. App. 3d at 1325-26 (Ct. App. 1986), argued that he developed the lists himself, but that was not the basis for the court’s holding. In \textit{Aetna Bldg. Maintenance Co., Inc. v. West}, 39 Cal. 2d 198, 205 (1952), a decision on which \textit{American Paper} itself said reliance is “misplaced” because it preceded adoption of the UTSA, \textit{American Paper}, 183 Cal. App. at 1324, the court suggested that trade secret status was less likely to be found when “patronage depends upon efficiency of service rather than personal relationship[s],” which were absent in the case.

\textsuperscript{28} A California statute provides that, with respect to employment agencies, customer lists of certain employer customers and all applicant customers are trade secrets belonging to the employment agency for a one year period. \textit{CAL. BUS. & PROF. CODE} § 16607 (2007). The court held that this statute was not applicable because it became effective only after the period at issue in the case and also because the court construed it to apply only to relations between an agency owner and his former employees who might want to take customer lists with them. Applicable or not, this statute clearly suggests a public policy of California that employment agency customer lists are trade secrets. The \textit{Scott} court might have felt the policy showed more solicitude toward proprietary rights of the agency operator/owner, vis-à-vis his employees, than toward the system’s franchisor.
plaintiff suing to enjoin its use. See, e.g., Metro Traffic Control, Inc. v. Shadow Traffic Network, 22 Cal. App. 4th 853, 860-63 (Ct. App. 1994). See also Electro Optical Indus., Inc. v. White, 90 Cal. Rptr. 2d 680, 685 (Ct. App. 2000) (depublished) (list of customers not trade secret because easy to learn their identities in small market, and all were solicited regularly by competing firms; nor was information about the customers’ requirements, preferences and specifics secret, because the customers could disclose it to any of plaintiff’s competitors; if a trade secret, it belongs to the customer); cf. Trailer Leasing Co. v. Assocs. Commercial Corp., No. 96 C 2305, 1996 WL 450801, at *1 (N.D. Ill. Aug. 8, 1996) (general rates of a leasing company not trade secret, certainly not for long, since customers will shop to get better prices).

Generally speaking, however, this logic may prove too much depending on the circumstances. The fact that consumers are free to share information about themselves does not mean that, when a company compiles such data in a certain way for a certain use, the compilation does not have value to it and potentially to its competitors. Nor does the fact that consumers share some information about themselves with the company’s competitors mean that the same data was shared with all of the competitors, or even most of them, or that the plaintiff’s compilation is as good as the others’, if they have one, or that all of the people on the plaintiff’s lists are on all of the lists of all of the competitors who have some such information. Scott did not address any of these issues.

Consider, by contrast, Four Seasons Hotels and Resorts, B.V. v. Consorcio Barr, S.A., 267 F. Supp. 2d 1268, 1325 (S.D. Fla. 2003), holding that a luxury resort property owner misappropriated trade secrets by hacking into the resort operator’s computer and taking the “profiles” of guests at this hotel and other hotels within the system. The parties had agreed that Four Seasons would license its trademark to the hotel and provide advisory, operations, and management services in exchange for the owner’s promise to construct the hotel. The owner used its licensee status inappropriately to access customer data, which included not just the guests’ occupancy history, but names, addresses, passport numbers, spouse names, pet types and names, past complaints, personal preferences, etc. Presumably these guests could have given the same information to other hotel chains, as the information was about them, not the hotel operator. It was the time and expense taken to compile and protect the data that made it valuable, however, not the theoretical fact that others might have been able to do the same but did not necessarily do so.

Notwithstanding Four Seasons, the possibility exists that a trier of fact might have the reaction in Scott and the other cited cases. This cautions carefully evaluating how one characterizes what is supposedly secret, both in drafting agreements on the subject and in shaping evidence and arguments for or against granting the customer data trade secret status.

---

29 In Metro Traffic Control, a company that contracted with radio stations to gather and broadcast local traffic information sought an injunction preventing a competitor and contract successor from soliciting the plaintiff’s employee talent. Metro Traffic Control, Inc. v. Shadow Traffic Network, 22 Cal. App. 4th 853, 855-56 (Ct. App. 1994). Metro’s employment agreement required employees to treat all traffic gathering and reporting procedures as confidential, and forbade competing with Metro in the traffic reporting business during the employment relationship and for one year post-termination. Id. at 855. The theory was that the customer radio station shared with the plaintiff what profile of anchor talent the station desired, and this was a trade secret. The court said this was more of a job description which the customer would fully describe to any provider. Id. at 862-63. If anyone’s trade secret, said the court, it belonged to the customer station. Id. at 863.

30 In an unpublished opinion, the Eleventh Circuit Court of Appeals affirmed the district court holding with respect to trade secret misappropriation, but reversed the damages award on that claim as based on flawed data and unduly speculative methodology. Four Seasons Hotels and Resorts, B.V. v. Consorcio Barr, S.A., No. 03-16189 (11th Cir. Mar. 31, 2005) (unpublished opinion).
It is not just the data itself, but the time spent, the manner in which the information is compiled, and the value from its secrecy, which create the trade secret. See, e.g., Bacon v. Volvo Serv. Ctr., Inc., 597 S.E.2d 440, 443-44 (Ga. Ct. App. 2004) (customers are not trade secrets; list on computer not trade secret where not password-protected, employees were not told it was confidential or required to sign nondisclosure agreement, and was available on other documents). See also Coleman & Stevens, supra note 3, at 24 (suggesting one way to avoid problem is to focus on specific type of customer-related information that is not known to the customer, at least not fully). 31

**ii. What Is The Significance Of The Franchisee Having Participated In Developing, Or Developed On Its Own, The Customer Data?**

Courts in other franchise cases have both agreed with, and rejected, the second basis for the *Scott* holding, namely, the extent of the franchisee’s involvement in developing the customer data. In *BJM & Associates, Inc. v. Norrell Servs., Inc.*, 855 F. Supp. 1481, 1483 (E.D. Ky. 1994), another employment agency case, decided under Georgia law, BJM promised to operate its agency under the Norrell system in exchange for a fifty-percent split of the franchisee’s profits and losses. *Id.* at 1482. The parties’ agreement included a noncompete clause, a termination clause and a buy-out provision. The court relied on *Scott* to deny trade secret status to customer data, in part because the franchisee proved that it developed its own lists without assistance from the franchisor. *Id.* at 1496-97. There was no proof that the franchisor ever provided the franchisee with a business lead or contact with any clients. *Id.* at 1497. 32

Similarly, in *Great Expectations*, Bus. Franchise Guide (CCH) ¶ 11,434 (S.D. Cal. 1998), discussed earlier, the court would only provide trade secret protection to membership profiles and other data “developed through [the franchisor’s] own independent efforts” that had been

---

31 A somewhat similar issue of entitlement to claim trade secret status arose in *Moss v. O.E. Clark Paper Box Co.*, No. B152258, 2002 WL 849940 (Cal. Ct. App. May 3, 2002) (unpublished opinion). A plaintiff employee’s former employer went bankrupt, after which the employee took customer data with her to a new job that she obtained by representing she would use the data to help the new employer’s business, a competitor of the failed firm. *Id.* at *1. The new employer eventually fired her. *Id.* at *2. The court granted summary judgment dismissing her claim against it, for allegedly misappropriating for its own use the customer data trade secrets she had brought with her. *Id.* at *5-6. She never intended to keep them secret from that second employer, so they were not misappropriated even if otherwise secret. *Id.* at *5. The customer data was not secret either, because of the highly competitive nature of the packaging industry. *Id.* Finally, the court added, the employee had not created the list, and it was not the result of substantial efforts by her. “The only rightful claimant to an interest in this information is [the bankrupt former employer] itself.” *Id.* at *6. Also noteworthy is the case *Prime Tech Staffing, Inc. v. Mickelsen*, No. G034128, 2005 WL 775688, at *1 (Cal. Ct. App. April 6, 2005) (unpublished opinion), in which an employer unsuccessfully sought to enjoin its former employee and her new company from soliciting the employer’s customers. The employee had signed an employee handbook acknowledging that she would gain access to “trade secrets and confidential information of a proprietary nature” to the employer, including “customer lists,” and requiring her not to disclose, disseminate or use such information outside of her employment. *Id.* at *6. Nonetheless, the employee successfully argued that the customer information was not a trade secret; it was known or readily ascertainable to other persons in the healthcare staffing industry, and had in any event been compiled through the employee’s sole efforts, in large part before she was hired by her former employer. *Id.* at *5.

32 Franchisors might try to distinguish *BJM* because of the unusual way in which the court reached the trade secret issues. The franchisor had breached the agreement, and the court granted the franchisee’s request for rescission. *BJM & Associates, Inc. v. Norrell Servs., Inc.*, 855 F. Supp. 1481, 1495-98 (E.D. Ky. 1994). The franchisor tried to defend against that remedy on the theory that the franchisee could not return to the franchisor the “know-how” of the system and other value received, including customer data. *Id.* at 1496. The franchisor’s theory was interesting, but it resulted in findings rejecting all of the alleged trade secrets in its system. *Id.* at 1496-97.
provided to the franchisees. \textit{Id.} at 30,781. The court would not protect such data that the franchisees “developed through their independent efforts.” \textit{Id.} at 30,778. There is no discussion in the case of what the parties’ agreement provided. \textit{Cf. Maharis v. Omaha Vaccine Co.}, No. 90-56356, 1992 WL 133117, at **3 (9th Cir. 1992) (unpublished opinion) (discussed further below; applying California law, and observing in \textit{dicta} that a defendant could not be prevented from utilizing knowledge it gained in expanding a customer list owned, and provided to it under contract, by someone else).\textsuperscript{33}

On the other side of the issue is the relatively recent decision in \textit{American Express Fin. Advisors, Inc. v. Yantis}, 358 F. Supp. 2d 818 (N.D. Iowa 2005) ("Yantis"). In that case, the franchisee left its investment advice business system to go with a competitor. \textit{Id.} at 821, 824. The franchise agreement contained many express provisions that are instructive here. \textit{Id.} at 821-24. It recited that, because the franchisee was entrusted with access to the franchisor’s valuable trade secrets and confidential information, and to protect client confidentiality (a rare acknowledgment of that potential priority, discussed below in Part III), the franchisee agreed never to divulge or use outside the system confidential information or trade secrets including customer data which may be communicated to the franchisee “or of which [the franchisee] may be apprised by virtue of [his] operation under the terms of [the franchise agreement].” \textit{Id.} at 821-22. The agreement also forbade revealing information about potential clients to whom presentations had been made, and who thus might reasonably be expected to do business with the franchisor. \textit{Id.} at 822. The franchisee agreed to divulge this information only to such of his employees as “must have access.” \textit{Id.} The franchisee agreed again elsewhere that client data in client records was confidential, including compilations and lists of such client information, even if of otherwise public information, if such compilations or lists were the result of substantial effort, time and/or money expended pursuant to the system. \textit{Id.} The franchisee agreed on conclusion of the agreement to immediately deliver to the franchisor all such information, which the franchisee acknowledged was the property of the franchisor, including originals of all client records and any other records containing customer data belonging to the franchisor. \textit{Id.} The franchisee agreed not to solicit clients for one year after termination. \textit{Id.} at 823. Finally, the franchisee also agreed, in order to protect the confidentiality of the franchisor’s customer data, that he would not induce any client to stop doing business with the franchisor or solicit any client that the franchisee contacted, serviced or learned about while operating as a franchisee. \textit{Id.}

The franchisor sued to enforce trade secret rights, and for breach of contract and conversion of the franchisor’s property. \textit{Id.} at 824. The court granted an injunction broadly enforcing the franchise agreement after considering the other factors in connection with such an equitable remedy. \textit{Id.} at 826-34. The customer data included suitability information, investments and investment history, financial plans, and client financial goals, and prospective client names. \textit{Id.} at 830-31. The client files were, as the court found under the conversion claim, “the property of [the franchisor].” \textit{Id.} at 834. The information was not generally known to and not readily ascertainable by proper means by someone able to obtain economic value from its disclosure or use, and competitors would require cost, time and effort to duplicate it. \textit{Id.} at 832. The franchisor made significant efforts to guard the secrecy of its information by, in addition to the above contract, requiring every financial advisor to sign a contract designed to

\textsuperscript{33} It is interesting that neither \textit{Scott} nor \textit{Maharis}, both federal decisions applying California law, cited to American Credit Indemnity Co. v. Sacks, 213 Cal. App. 3d 622 (1989) (see page 14, above), which had been decided by the time of those two federal decisions, or acknowledged the split of authority in California between \textit{Moss} and \textit{American Credit} on this issue involving franchisee efforts. As mentioned earlier, the court in \textit{Liberty Mutual Ins. Co. v. Gallagher & Co.}, No. C94-3384 MHP, 1994 WL 715613, at *4 (N.D. Cal. Dec. 19, 1994) (Judge Patel), by contrast, did acknowledge that split a couple of years after \textit{Maharis}. 

20
protect the information and requiring any members of the franchisee’s staff having access to sign a confidentiality agreement. *Id.*

The court ordered the franchisee to immediately return all client records, and to cease using the franchisor’s confidential information, as set forth in the franchise agreement, and also enjoined him from soliciting, revealing any information about, or inducing to stop doing business with the franchisor “any [franchisor] client[s] whom [the franchisee] served or whose name became known to [him] while [he] represented [the franchisor].” *Id.* at 836-37.34

*Winston Franchise Corp.*, No. 91 Civ. 7963 (CSH), 1992 WL 7843, at *8-11, (S.D.N.Y. Jan. 10, 1992) is another case illustrating the tension over whether customers are garnered, and their data rightfully possessed, through a franchisee’s sweat or a franchisor’s brand. *Winston* concerned another employment agency franchise system, one which specialized in the food retailing, drug and food manufacturing industries. *Id.* at *1. By contrast with the situations described in *Scott* and *BJM*, Winston administered interchange of information among a nationwide group of franchisees. *Id.* For example, if a California client needed an executive and the local franchisee had no one suitable, the franchisor would notify other franchisees who might suggest candidates. *Id.* Franchisees could also make the availability and qualifications of their applicants known throughout the system, hoping to obtain placements with corporate clients elsewhere. *Id.* Finding fees were split in such circumstances. *Id.*

The lengthy provisions of the franchise agreement that the court quoted never use the phrase “trade secret.” They do recite, however, that the franchisor created substantial good will in its name; the licensee wanted to use it; and the licensor would furnish a list of applicants and clients, if any, in the licensee’s territory, as well as its information interchange system. *Id.* at *2. On termination, the licensee would discontinue using all trade names and associations with the franchisor’s name; for three years it would not engage in a similar business anywhere in the U.S., or divulge or use any customer data acquired as a result of the parties’ agreement; and the licensee would promptly deliver to the franchisor all of its records containing customer data. *Id.* at *2-3.*

The court analyzed the enforceability of the restrictive covenants under a rule of reason applicable to commercial contracts, first considering whether legitimate business interests required enforcement. *Id.* at *8. Franchisors commonly suggest a number of such interests. *See generally*, authorities contained within note 7, *supra.* *See also* Douglas L. Carden & Peter J. Klarfeld, “WE HAVE TO LIVE WITH IT” -- TIPS FROM THE LITIGATORS’ PERSPECTIVE ON ADVANCED DRAFTING (A.B.A. Forum on Franchising 2005); William Killion & Eric Yaffe, PROTECTING THE FRANCHISE SYSTEM WITH RESTRICTIVE COVENANTS AGAINST COMPETITION (IFA Annual Legal Symposium 2007). This included, according to the court, protection of trade secrets and unfair competition. *Winston*, 1992 WL 7843, at *8 (S.D.N.Y. 1992). The court held that much of what the licensor sought to protect was not protectable, despite the contract provision, including names of past or prospective beverage industry customers, whose names and contract information were all readily ascertainable from sources outside the franchisor. *Id.*

---

34 The *Yantis* decision did not address directly the notion in *Avocado*, *Moss* and *Scott* that franchisee efforts may avoid trade secret protection. But clearly the court ruled for the franchisor cognizant in that regard. The court protected, as the agreement required, not just information “communicated [to the franchisee],” but also information “of which [the franchisee] may be apprised by virtue of [its] operation . . . .” *American Express Fin. Advisors, Inc. v. Yantis*, 358 F. Supp. 2d 818, 832 (N.D. Iowa 2005) ("Yantis"). That included potential clients to whom business development presentations had been made. *Id.* at 822. And the non-solicitation order included franchisor clients whom the franchisee served or whose name became known to him while he represented the franchisor. *Id.* at 837.
Winston did hold, however, that the names, addresses and other particulars of applicants seeking employment “stand on a different footing.” Id. at *9. The court never expressly found that the customer data was a trade secret, but it analyzed the data under trade secret authorities. Id. at *9-10.\(^\text{35}\) The franchisee generated files containing data while he was part of the system, but he did not completely fit the mold of an employee who takes from an employer customer or applicant lists created by the employer’s own efforts.” Id. at *9. Instead, the “great majority” of the files resulted from ads in trade publications which the franchisee itself ran and paid for. Id. The franchisee also used his own contacts and reputation developed over many years. Id. If that was all, the court observed, the franchisor likely would not prevail. Id. However, the franchisee published its ads under the franchisor’s name before being terminated. Id. The court acknowledged that it was “probably impossible to ascertain why each of the applicants who responded to [the ads] using the [franchisor’s] name did so. It is fair to assume, however, that a motivating factor in at least some cases was the use by [the franchisee of the franchisor’s] name…” Id. The court concluded that the data generated through the franchisee’s own efforts and expense during the term of the agreement were likely entitled to protection under the franchisor’s restrictive covenant. Id. at *10.

The court characterized the applicant customer data as “confidential information owned and protectible by” the franchisor. Id. at *10. The franchisee had to return to the franchisor, in addition to all documents received from the franchisor, all applicant files generated by the franchisee until 30 days after publishing the last ad with the system’s name, and the franchisee was preliminarily enjoined from affirmatively soliciting anyone in those files. Id. The franchisee was permitted, however, to advertise and deal with individuals responding to its post-termination ads even if an individual had responded to an earlier ad under the franchisor’s name. Id. at *11.\(^\text{36}\) See also Jan Marini Skin Research, Inc. v. Allure Cosmetic USA, Inc., Nos. A108613, A108631, A108633, 2007 WL 1508686, at *30 (Cal. Ct. App. May 24, 2007) (unpublished opinion) (refusing to extend scope of injunction against solicitation of list of trade secret customers by former supplier to customers who seek out the defendant on their own, instead of just those who defendants would affirmatively solicit).

4. **What If The Data Remains In the Franchisees’ Memories?**

Another issue that comes up is whether a franchisor can have trade secrets in customer data that a franchisee takes away in her mind only, not in tangible form in her briefcase.

Recall the quotation earlier from **Avocado** about equity not wiping clean the slate of memory. The **Avocado** court, however, clarified that it did not mean to suggest that customer

---

\(^{35}\) It is noteworthy that **Winston** is a New York decision and that New York has not adopted the Uniform Trade Secrets Act.

\(^{36}\) It is interesting to read in this context an article by Robert W. Emerson, **Franchising Covenants Against Competition**, 80 Iowa L. Rev. 1049, 1050 (1995), in which he reviews the “comparatively meager” law on covenants not to compete as applied in the franchise context, and further discusses the approaches adopted by courts in other, more prevalent and, he argues, distinguishable contexts, namely, covenants found in employment agreements and covenants concomitant to the sale of a business. In discussing protection of customer lists as a rationale for enforcing a post-term noncompete provision, he suggests that the mandatory contributions franchisees are obligated to make to franchisor advertising funds undercuts the franchisor’s argument that the goodwill associated with its name entitles it to proprietary rights in customer data. For reasons not disclosed, Emerson cites **Winston** for its holding that names of potential employer customers were not trade secrets. He does not mention anywhere that **Winston** went on to hold that the franchisor had ownership rights in other customer data generated by franchisee advertising -- indeed, advertising placed and paid for by the franchisee itself, not just placed by the franchisor from franchisee contributions -- which advertising gave the franchisor ownership rights if associated with its name.
data must be in writing to be protected, specifically acknowledging that California cases had
granted injunctions in the appropriate case to protect customer lists “whether in writing or in the

Cases have not been uniform on this issue, however. According to Milgrim, the majority
rule nationally is that “appropriation by memory will be restrained under the same circumstances
as will appropriation by written list.” MILGRIM ON TRADE SECRETS app. at 15A-3 (citing a variety
of authorities). Georgia’s UTSA statute, GA. CODE ANN. § 10-1-761(4) (2007), which specifically
mentions “a list of actual or potential customers,” has been interpreted to continue the Georgia
common law rule distinguishing between protectable tangible lists that were an employer’s
property, on the one hand, and an employee’s mental knowledge that he could take with him, on
intangible list of customers not trade secret; non-competition and non-disclosure clauses
unenforceable); Avnet, Inc. v. Wyle Laboratories, Inc., 437 S.E.2d 302, 304-06 (Ga. 1993); 1st
court limited protection of customer lists to written lists because an employer does not possess
a property right in the employee’s mental processes; holding that in light of the employment
contract’s express non-disclosure clause, taken together, expiration and renewal dates,
personal customer data and customer names and addresses in insurance agency’s customer
file “comprise a trade secret even though separately each item may not rise to that level.”).
North American Miss., No. 01-01019 MMM (SHX), 2001 WL 521695, at *61 n.92 (C.D. Cal. April
13, 2001); North Atlantic Instruments, Inc. v. Haber, 188 F.3d 38, 47 (2d Cir. 1999); American
trend discards written-memorized distinction); Sweetzel, Inc. v. Hawk Hill Cookies, Inc., 39
U.S.P.Q. 2d 1258, 1269 (E.D. Pa. 1995) (whether a list is committed to former employee’s
memory or embodied in written lists is of no significance under Pennsylvania law).

5. Franchisees’ Assertions Of Their Own Trade Secret Rights In
Customer Data

Thus far we have discussed claims by a franchisor, usually vis-à-vis franchisees, that it
has trade secret rights in connection with its system’s customer data. Decisions denying such
claims do not necessarily mean that the franchisee has trade secret rights, though the cases
discussed above based on the franchisees’ efforts lend themselves to that possible conclusion.
There are also a number of decisions in which franchisees themselves have sought to assert
rights in their customer data, often vis-à-vis the franchisor.

These authorities seem to teach a few rather obvious lessons. First, it can be difficult for
franchisees to lay claim to proprietary rights of their own in customer data because franchisors
so often have the right and need to see that information in performing under the parties' 
agreement. Second, if a franchisee transmits customer data to its franchisor and wants to retain
proprietary rights for itself, it should do so under circumstances adequately confirming and
protecting those rights. Third, franchisees should be careful to safeguard the secrecy of the
information themselves, not just from franchisors but from other persons as well. And finally,
franchisors should take care not to misuse information received from franchisees and, at least,
clarify adequately by agreement who has what rights in information generated in the system.

A number of cases illustrate the first points. In Adcom Express, Inc. v. EPK, Inc., No.
Minnesota federal court applied California law to deny a terminated air freight forwarding system
The franchisor already knew the customers' names, because it handled their billing; and nothing in the parties' agreement required the franchisor to keep that information confidential. *Id.* Indeed, the contract expressly allowed the franchisor to contact customers after termination. *Id.* at *7.

The law did not require the information to be generally known to the public to lose its status as a trade secret vis-à-vis the franchisor. *Id.* at *6*. Were that not enough, the franchisee itself had given the list to a competitor of the franchisor. *Id.* Interestingly, though, the court rejected as unsupported by authority the franchisor's big picture argument that it was "axiomatic" that a franchisee could not keep a franchisor from dealing directly with a franchisee's customers. *Id.* at *7*. That assumed too much.

In *Sitco, Inc. v. Agco Corp.*, No. CV-05-073-EBLW, 2006 WL 908065, at *1 (D. Idaho April 7, 2006), a terminated dealer alleged that its manufacturer misappropriated the dealer's trade secrets by sharing the dealer's customer list with another dealer. The list was not secret, however. *Id.* It was part of a delivery report that was sent to the manufacturer on a regular basis without restriction. *Id.* In addition, there could be no restriction on the manufacturer knowing the names of its dealer's customers, since the manufacturer had warranty obligations to them and therefore a need to know their identities. *Id.* The manufacturer also received the list from a former employee of the dealer who went to work for the manufacturer; the dealer had not imposed any confidentiality obligations on the ex-employee. *Id.* at *2*. See also *Home Paramount Pest Control Companies, Inc. v. FMC Corp./Agric. Prods. Group*, 107 F. Supp. 2d 684, 693 (D. Md. 2000) (list of distributor's customers given by manufacturer to distributor's competitor was not trade secret, where it did not cull and contain key information, the information was publicly available, the distributor did not adequately safeguard its disclosure, and the manufacturer did not disclose the most important part of what it had received); *Watkins Inc. v. Lewis*, No. 02-3708 (RHK/AJB), 2002 WL 31319491, at *14 (D. Minn. Oct. 11, 2002), aff'd, 346 F.3d 841 (8th Cir. 2003) (rejecting sales representative's claim of trade secrecy in information about customer identities, preferences and motivations because manufacturer had access to information in the ordinary course of business from orders placed with it by representative).  

Not all franchisees have failed in their efforts against franchisors, however. Two cases are noteworthy. In *Camp Creek Hospitality Inns, Inc. v. Sheraton Franchise Corp.*, 139 F.3d 1396, 1400, 1410-11 (11th Cir. 1998), a franchisee routinely sent in to the franchisor hotel system information about its individual operations of a type which was closely guarded in the industry, e.g., occupancy levels, average daily rates, discounting policies, rate levels, long-term contracts, marketing plans, etc. Competitors could not easily derive this information; they could use it to their advantage. *Id.* at 1411. The franchisee gave this information for use on the franchisor's database with the "apparently mutual understanding that it would be kept confidential" and disclosed only "as part of aggregate industry statistics" not traceable to individual operators. *Id.* The franchisor could have violated the franchisee's rights when it

---

Note: The text continues on the following page.
disclosed the individual hotel’s information to a subsidiary that operated a hotel in direct competition with the franchisee. *Id.* at 1412. This case illustrates the need not just for franchisees to document adequately their expectations of privacy, but also for franchisors to ensure that private information properly received is not improperly used.

Finally, in *Richmond Pharmacy & Surgical, Inc. v. Therasense, Inc.*, No. C-04-2070 SC, 2004 WL 2414974, at *1-2 (N.D. Cal. Oct. 28, 2004), the court denied a manufacturer’s motion to dismiss a claim by its distributor that the manufacturer wrongfully gave to the distributor’s competitors detailed customer sales data, including customer lists, and conducted wrongful audits to obtain more such customer data. The distributor avoided dismissal by arguing that its list was of companies actually buying and reselling the products—*i.e.*, actual customers instead of just potential—so their identities could not easily be derived from public sources. Compare *John Keenan Co., Inc. v. Norrell Corp.*, No. 99-1924, 2001 WL 815600, at *16 (E.D. La. July 18, 2001) (franchisee’s claim against franchisor for misappropriation of its trade secrets denied because franchisor never improperly disclosed any proprietary information of the franchisee).

6. Joint Ownership Issues

Efforts by franchisors and franchisees each to claim or defeat proprietary trade secret interests in customer data for the same system naturally lead to the question of whether this data can be jointly owned. There is little law on the subject of joint ownership of trade secrets, but it has been recognized in some decisions, none of which involve customer data so far as we are aware. The challenge of joint ownership is grounded largely in the fact that secrecy, more than content, results in the proprietary rights, and joint ownership presents even greater challenges for preserving that essential secrecy adequately and in defining the respective rights and obligations of the “owners.”

Ideally the fact of joint ownership and the many issues it creates should all be covered by express agreement, *e.g.*, rights to use, obligations to account, rights to license or disclose to others, with or without consent, and, of particular importance, duties to protect the secret from disclosure, both to preserve its proprietary existence and to avoid privacy and security issues discussed later in this paper.

It has been suggested generally that, absent agreement to the contrary, joint owners should each be entitled to use a joint trade secret, equity ought to require accounting for this use, and co-owners owe a duty to the other to protect against disclosure. See Gary Moore, *Joint Ownership of Intellectual Property: Issues and Approaches in Strategic Alliances*, 1260 PLI/Corp. 313, 347-49 (2001); see also *Baldwin v. Von Micheroux*, 25 N.Y.S. 857, 859 (Supreme Court, Special Term, NY County, 1893) (after partnership dissolved, former partners were co-owners of secret process and each had the right to use it); *B.F. Gladding & Co., Inc. v. Scientific Anglers, Inc.*, 245 F.2d 722, 729-30 (6th Cir. 1957) (finding that even though the contractual provisions did not specifically address jointly-owned trade secrets, the trade secrets were still entitled to protection against improper disclosure by either owner); *DTM Research, L.L.C. v. AT&T Corp.*, 245 F.3d 327, 333 (4th Cir. 2001) (although co-ownership was not involved, case suggests that a trade secret can lose its value when a co-owner discloses the information or fails to protect it).

keep the information secret were reasonable under the circumstances, as required to garner trade secret protection under Georgia’s UTSA. *Camp Creek Hospitality Inns, Inc. v. Sheraton Franchise Corp.*, 139 F.3d 1396, 1411 (11th Cir. 1998).
7. **Trade Secret Rights May Be Assigned**

The final issue we raise with respect to trade secrets is the extent to which trade secret rights may be transferred or contracted away.

As mentioned earlier, (see note 9), the UTSA expressly states that it does not affect contractual liability or relief that is not based upon misappropriation of a trade secret. The Commissioners’ Comment clarifies that the Act “does not apply to a duty voluntarily assumed through an express or an implied-in-fact contract.” UNIF. TRADE SECRETS ACT § 7. The enforceability of non-disclosure and non-competition covenants intended to protect trade secrets is governed by other law. Thus courts can enjoin use of trade secret customer data in addition to and apart from enforcing a contractual non-solicitation clause. See, e.g., *Liberty Mutual Ins. Co. v. Gallagher & Co.*, No. C94-3384 MHP, 1994 WL 715613, at *6 (N.D. Cal. Dec. 19, 1994).

Parties can contract as to who owns or has the right to use a trade secret. That is the essence of a license. Thus, for example, a court should enforce a franchise agreement provision intended to grant ownership or proprietary rights in customer data to a franchisor, if the data meets the applicable test for establishing a trade secret, which the contract may address but cannot control.

Two cases illustrate this nicely, both of which are instructive for franchise systems.

In *Maharis v. Omaha Vaccine Co.*, No. 90-56356, 1992 WL 133117, at **1 (9th Cir. 1992) (unpublished opinion), the plaintiff built a business of distributing equestrian videos. She licensed the entire business for three years to the defendant, at the end of which it had to buy the business or return all of the assets which the plaintiff had turned over when the license began. *Id.* The assets included her customer list. *Id.* Before the term had expired, the defendant sold the business to a third party, who obtained the customer list as part of the transaction. *Id.* at **2. Thus the defendant could not perform its obligation to return the licensed assets when the agreement expired. *Id.* The plaintiff sued for contract breach and misappropriation of the customer list trade secrets. *Id.*

Applying California law, the Ninth Circuit held that the customer list was a trade secret, distinguishing California cases such as *Scott and Moss*. *Id.* at **3-4. Here, unlike there, the list showed “actual” customers, and plaintiff employed substantial efforts to develop it. *Id.* Moreover, the court observed, in those other cases the defendant had personal knowledge of the information; here the defendant did not develop its own list, but rather, simply bought the list. *Id.* at **3. The licensee had orally agreed to keep the list secret, and it forced its own employees to sign confidentiality agreements as to the list while it operated the business. *Id.* at **4.

The defendant had “enhanced” the list during its operations, spending over $25,000 on a promotion for that purpose, and buying other lists of potential customers, thus creating a more valuable list than originally licensed. *Id.* The court required this enhanced list to be returned, not just the one originally transferred. *Id.* Under the license agreement, the licensee had a duty to make reasonable efforts to expand the original customer list and to return the enhanced version at termination. *Id.* at **6 n.1. (The decision is not clear as to whether this was an express or implied term.) The defendant “acted on [the licensor’s] behalf in developing and expanding the list.” *Id.* What is particularly interesting is the court’s observation in *dicta*, citing to the California *Moss* decision, that “while [the licensee] could not be prevented from utilizing
the knowledge it gained in expanding the list, see Moss, Adams, & Co., [179 Cal. App. 3d 124 (Ct. App. 1986)], it could not sell the list to a third party.” Id.

A similar case is Judge Posner’s decision earlier this year in American Family Mutual Ins. Co. v. Roth, 485 F.3d 930 (7th Cir. 2007) (applying Wisconsin law). An insurer sued former agents for misappropriating alleged trade secret customer names in a database which were “filtered for their suitability to buy insurance.” Id. at 933. After being terminated, the agents began soliciting customers. Id. at 931. Agents were required by contract to submit all new business and changes through the system as directed by the company. Id. The “system” referred to the “digitized database of customer information.” Id. The agreement acknowledged that the database contained confidential, proprietary and trade secret information, and the agent and its employees promised not to use or disclose it unless in the ordinary course of their business with the company. Id. at 931-32. The agent had access only to information about customers whom he served, either customers he originated on his own or names the company furnished to him. Id. at 932. The contract “forbade the defendants to use any name in the database, whatever the source.” Id. The defendants were using a list maintained separately from the database. Id. It contained 1,847 names, the vast majority of which were in the plaintiff's database. Id. Most were likely names of customers in a group of 2,000 which the plaintiff had furnished to defendants. Id.

Once the insurance agents entered customer information into the database, the information became the exclusive property of the plaintiff, or at least exclusive as against the agent. Id. The information developed by the agent would be his trade secret initially. Id. But once he uploaded it into the database, it became the plaintiff’s trade secret. Id. The court referred to this provision of the contract as a “grantback” clause, common in patent and other IP settings. Id. Once the data was thus sold, it could no longer be used by the seller. Id. The court said there was “nothing unconscionable or even one-sided” about this arrangement. Id. The agents benefited from being able to use the plaintiff’s database, as well as from receiving customers; in exchange they gave the plaintiff the right, after termination, to keep any customer information they had acquired in the course of their agency relationship. Id.

The omission of a time limit on duration of the contract restraint was not fatal, since the information was a trade secret under Wisconsin’s trade secret act. Id. at 933.39 The filtering of names resulted in a “defined, manageable and economically viable universe of uniquely receptive potential customers.” Id. The court remanded with instructions to modify the injunction that had been entered so that defendants would be forbidden from using only those of the names in their separately-maintained list that also appeared in plaintiff’s database. Id. at 934.40

Maharis and American Family both illustrate that, for trade secret protection, it is not enough for a contract to state that the customer data is a trade secret. The data must pass the applicable test in all events, though the contract language may assist. Taken together, and mindful of this practical reality, the two decisions suggest some interesting drafting possibilities to consider in the context of customer information.

39 But see 1st American Sys., Inc. v. Rezatto, 311 N.W.2d 51, 58-59 (S.D. 1981) (clause prohibiting disclosure of trade secret for ten years must meet test of reasonableness).

40 It is interesting to note that the plaintiff, an insurance company, sued also under the Gramm-Leach Billey privacy act, discussed below, trying to allege a private right of action on behalf of its customers. The district court dismissed this claim because the plaintiff had no standing to bring it. American Family Mut. Ins., Co. v. Roth, No. 05 C 3839, 2005 U.S. Dist. Lexis 39567, at *17-37 (N.D. Ill. Aug. 5, 2005). The issue was not raised on appeal.
Franchisors should consider reciting the existence, if true, of each of the elements of a trade secret definition for particular customer data for which a franchisor desires such protection, ideally taking care to define relatively specifically the kind(s) of secret customer data; conclude with a recital and agreement that it is in fact a trade secret; and obligate franchisees contractually to take specified steps to safeguard this data to protect its secrecy, including limitation of access only as needed, failing which they are liable for material breach. Franchisees could also be required to agree that they collected all customer data of this type while engaged in business under the franchisor’s marks and system, that it was for the benefit of the entire system, and that it is also a trade secret owned by the franchisor. In order to reduce doubt and argument, franchisees could contractually convey and grant ownership of any of its work product in this regard to the franchisor, including any customer data that the franchisee might believe it brought into the system with her. This grant could also include any value that the franchisee added to customer data which the franchisor provided to the franchisee. In addition to customary post-term non-competition provisions and others entitling the franchisor to audit franchisee records and unrestricted access to the franchisee computer systems, the provisions regarding customer data could also include non-solicitation, non-disclosure and mandatory return provisions.41

C. Contract Restraints On Customer Data Which Is Not A Trade Secret

We have seen that courts will generally enforce contract provisions to protect trade secret rights in order to prevent misappropriation. We now turn to a review of cases where the customer data was not a trade secret for some reason. We seek to understand the extent to which in this circumstance courts will enforce contracts designating ownership of, or restricting post-termination use of, such customer data. We will not try to cover the broader topic of general contractual restrictions on competition of various types.42 Instead, our focus is covenants protecting interests in customer data, and cases in which customer data was a significant factor. We have found few cases going beyond a mere mention of customer data, generally in the course of enforcing a broader general covenant against competition.

Our sense, based on the modest number of reported decisions, is that courts may be more willing to enforce such provisions when they are clear and relatively narrow in scope, that data is in tangible form, and the data is more substantive than just names and addresses. Some courts have been willing to enforce relatively broad clauses specifying that one party

---

41 See also Coleman and Stevens, supra note, 3 at 11-15, discussing the fact that, in states such as Wisconsin (whose law American Family applied) and Georgia, contract restrictions on using confidential customer data which a court found did not rise to the level of a trade secret may be unenforceable without reasonable contract limitations of time and/or geography. Those authors therefore suggest that counsel consider drafting confidentiality agreements in two parts, one for trade secrets without such limits and another for confidential information (presumably anything not found to be a trade secret) which would be limited. Those authors query in support of this suggestion whether limits on trade secrets render their protection illusory. That may be true in many, if not most, situations, but we suggest that this is not necessarily always the case, since customer data may in fact have a limited shelf life or geographic significance depending on the system or industry. In that situation, we posit, the likelihood of a court protecting trade secrets might well increase from the existence of thoughtful, voluntarily imposed, contractual limitations designed to preserve only the extent of protection which the data realistically and reasonably needs.

owns the data and that, upon termination or expiration, all customer data is to be returned to its owner (a “grant-back” clause)\(^{43}\).

Courts that have enforced contract restraints generally view customer data (and similar items of information) as personal property—and those courts have enforced contracts permitting a franchisee to use the property and obligating the franchisee to later return it.

One of the most thoughtful and complete analyses of customer data as property is contained in *Brenco Enterprises, Inc. v. Takeout Taxi Franchising Sys., Inc.*, No. 177164, 2003 WL 21659422 (Va. Cir. Ct. May 2, 2003). Takeout Taxi was a service that delivered meals to homes and businesses from restaurants that otherwise normally did not provide take-out service. *Id.* at *1*. The franchisees marketed almost exclusively under the Takeout Taxi marks and used Takeout Taxi’s proprietary software to compile a database of names and addresses of customers and a record of the food and restaurants they preferred. *Id.* at *1-2*. The franchise agreements required, upon termination or expiration, a one year period of non-competition, assignment of telephone numbers, return of the software and customer database, and return of certain advertising materials. *Id.* at *1, 4-7, *7 n.77.

The *Brenco* plaintiffs’ franchise agreements had expired. *Id.* at *3*. The franchisees argued that that they, not the franchisor, owned the telephone numbers, directory listings and customer databases they had used in their businesses. *Id.* at *8*. The court concluded that the contract clearly vested ownership of those items in the franchisor. *Id.* The court specifically referred to the “cessation of use” provision and the “return of franchise materials” provision as evidencing “the parties’ intent to shift control over the telephone numbers, directory listings, and software back to Takeout Taxi in the event of either expiration or termination….” *Id.* Further, the court reasoned that, under the Lanham Act (the federal trademark act), any “goodwill” benefits from a trademark licensee’s use of the franchisor’s trademarks inured exclusively to the benefit of the franchisor/licensor. *Id.* The court expressly refers to these residual post-termination rights as the franchisor’s “property rights”. *Id.*

The franchisees argued that the contract provisions were impermissible restraints on trade and unenforceable as a matter of law. *Id.* at *9*. They asked the court to apply a higher level of scrutiny applicable to covenants not to compete in the employment context. *Id.* Takeout Taxi argued, on the other hand, for a lesser standard because the contract terms at issue sought only to obtain the return of its property (telephone numbers and customer databases). *Id.* The court, concluding that a higher level of scrutiny was not applicable, engaged in the following “property” analysis:

“Franchise agreements generally result in a transfer of good will.

***

In the franchise agreements here, the first transfer of good will occurred when Takeout Taxi granted to each Plaintiff ‘the nonexclusive right and license … to operate a Takeout Taxi business’ and to use Takeout Taxi’s proprietary marks in

---

\(^{43}\) In addition to being limited by the small number of reported cases, this analysis of contract enforcement where the customer data was not a trade secret is necessarily limited because most of the reported cases are in the procedural posture of deciding whether to grant a preliminary injunction.
conjunction with that business. The second transfer of good will occurs when the franchisees return to the franchisor ... customer databases, associated customer lists, and all telephone numbers and directory listings upon conclusion of the parties’ relationship.

Under the express terms of the franchise agreements, the parties plainly did not intend for the franchisees to own any good will, service marks, or any other assets associated with the franchise system after they left it.

* * *

Fundamental principles of a franchise relationship would be destroyed if the franchisees are permitted to use telephone numbers and customer databases associated with Takeout Taxi’s proprietary mark after the expiration of the agreements. Neither [of the contract provisions] qualifies as, or has the effect of, a restraint on trade. Instead, these provisions merely require a return of Takeout Taxi’s assets and property. In sum, the post-term obligations here are enforceable contractual provisions for which no showing of ‘legitimate protectable interest’ is required. If the franchisees elect not to renew their franchise agreements, thereby removing themselves from the franchise system, then they must do so without a concomitant right to use Takeout Taxi’s marks or related franchise assets.” *Id.* at *9-10 (citations omitted).

The court stated that no “court has held that such franchise agreement obligations amount to disfavored restraints on trade,” and distinguished the franchisees’ authorities because none involved an obligation “for the return of certain proprietary information to the owner upon expiration of the agreement.” *Id.* at *9, 9 n.105.

In sum, the *Brenco* court held that a franchise agreement is a conveyance of the franchisor’s goodwill for the duration of the contract—to be returned upon termination or expiration. *Id.* at *19. 44 In choosing to become Takeout Taxi franchisees, the franchisees had “placed significant value on the strength of Takeout Taxi’s marks and brand identity.” *Id.* The franchisees “traded off the [brand] by attracting customers through promotional efforts predicated exclusively on the brand awareness of such marks.” *Id.* The franchisees “understood the value . . . of the . . . software system, the customer databases (products of the software system), the Takeout Taxi’s trademarks, advertising and other promotional materials.” *Id.*45

44 We observe that the *Scott* decision may not be inconsistent with this grant-back notion. *Scott* rejected a proposed analogy to the sale of a business in that franchising does not really effect a transfer of ownership of goodwill. *Scott v. Snelling & Snelling, Inc.*, 732 F. Supp. 1034, 1041 (N.D. Cal. 1990). The court opined that a franchise was more like a “lease” of goodwill because the goodwill is to be returned at the end of the relationship. *Id.* If customer data is the embodiment of goodwill, even though the *Scott* court might not find that it constituted a trade secret, it appeared to be prepared to and did order return of the physical manifestations of the asset on the basis that it was the franchisor’s property. *Id.* at 1045 n.15.

45 See also, e.g., *NaturalLawn of Am., Inc. v. West Group, LLC*, 484 F. Supp. 2d 392, 397, 399-402 (D. Md. 2007) (enforcing general covenant while mentioning that the agreement contained a grant-back clause and a provision that Continued on following page
It is also interesting to compare *Scott v. Snelling & Snelling, Inc.*, 732 F. Supp. 1034 (N.D. Cal. 1990), discussed earlier, with a subsequent decision from the same federal district and the same franchise system in *Snelling & Snelling, Inc. v. Martin*, No. C 97-4479 FMS, 1998 WL 56995 (N.D. Cal. Jan. 28, 1998) ("Martin"). In *Scott*, the contract required the franchisee to provide the franchisor upon leaving the system with a “typewritten list” of customers who purchased services during the two years before termination or placed an order during the 90 prior days. *Scott*, 732 F. Supp. at 1037 n.3. As mentioned previously, the court had granted a preliminary injunction requiring, among other things, customer lists to be provided to the franchisor, and the franchisees had complied. Thus, though *Scott* is often cited for California’s unwillingness to find that the customer data was a trade secret, the court had previously enforced the franchisor’s property right to receive delivery of the physical list. The decision does not state whether the franchisee was entitled to continue to use the contents of, or another copy of, the “typewritten list”.

In *Martin*, the court ordered Snelling to advise a former franchisee of what action the franchisee should take, and what files the franchisee should transfer, to comply with an ambiguous contract obligation to “wrap up or transfer” their relationships with clients as directed by a written notice the franchisor itself had not yet sent. *Martin*, 1998 WL 56995, at *3. The court did not order the files to be turned over, but left the issue open depending on what Snelling asked for under the contract. *Id.* at *3-4. Thus the *Martin* court, although not explicitly stating so, appeared to view customer data as property which can be transferred and re-transferred by enforceable contract provisions.

*American Express Fin. Advisors, Inc. v. Yantis*, 358 F. Supp. 2d 818 (N.D. Iowa 2005), discussed earlier, seems consistent with *Brenco* and *Martin*. In addition to finding that customer data was a trade secret, the court stated in *dicta* that a franchisor established a claim for conversion of customer data where the contract specified that the data was the franchisor’s property upon cessation of the franchise agreement. *Id.* at 833-34.

---

31

46 The *Martin* court also ordered the franchisee to comply with its contract obligation to assign its lease to the franchisor, rejecting the franchisee’s argument that the required assignment would be “punitive” and “serve no useful purpose” because there were other comparable premises available in the same building. *Snelling & Snelling, Inc. v. Martin*, No. C 97-4479 FMS, 1998 WL 56995, at *4 (N.D. Cal. Jan. 28, 1998) ("Martin"). The court noted that the contract was intended to allow Snelling to retain clients familiar with the business’s precise location, without which Snelling would lose the intangible benefit of the location. *Id.* The court also held that a provision requiring sale of the entire franchise to Snelling was neither unconscionable nor an illegal restraint of trade under California law because, if the franchisor elected that right, the former franchisee was free to compete and attract its former clients. *Id.* at *3. The court did not, however, order compliance with that clause, leaving the franchisor to its damages remedy, because two other Snelling franchise agreements did not contain this provision, thus suggesting that provisions requiring transfer of client relationships, leases and files were sufficient to protect the franchisor’s legitimate interest in goodwill by providing uninterrupted service. *Id.*

Another interesting case where a federal court enforced under California law an agreement limiting use of non-trade secret information is *Universal Gym Equip., Inc. v. ERWA Exercise Equip. Ltd.*, 827 F.2d 1542 (Fed. Cir. 1987). In *Universal Gym*, a patent owner sought to enforce a contract prohibition on the licensee’s post-term manufacture, use, sale or distribution of any products that “include any of the features, designs, technical information or said know-how. . . .” *Id.* at 1545. The court acknowledged that, absent the contract, the licensee could have purchased one of Universal’s products and reverse-engineered it with impunity. *Id.* at 1550. The court also rejected plaintiff’s patent infringement claim. *Id.* at 1548. However, because the licensee had voluntarily entered into the contract and accepted the benefits of it, the licensee was bound by its agreement not to use certain otherwise unprotected information and know-how. *Id.* at 1550-51. The court concluded: “Parties to a contract may limit their right to take action they previously had been free to take.” *Id.* at 1550.
Similarly, Judge Posner, in his 2007 decision in *American Family*, 485 F.3d 930 (7th Cir.), as discussed earlier, held that the customer data was a trade secret, but suggested in *dicta* that, absent this finding, the court would enforce the contract forbidding use or disclosure of customer data after termination or expiration “if the contractual prohibition is reasonable in time and scope and, specifically, only if its duration is limited.” *Id.* at 933-34.

The importance of addressing customer data in the contract is also illustrated by a Pennsylvania employment case involving customer data that was not a trade secret. *Si Handling Sys., Inc. v. Heisley*, 753 F.2d 1244, 1258 (3d. Cir. 1985), acknowledged that the information was part of the employer’s goodwill and extremely valuable to the employer. The court pointed out that the employer could have protected the information with a reasonable restrictive covenant, but the employer had not done so and could not now bootstrap such protection by characterizing the data as a trade secret. *Id.* at 1258-59.

*McCart v. H&R Block, Inc.*, 470 N.E.2d 756 (Ind. Ct. App. 1984), is another interesting case involving customer data that was not a trade secret. The franchisor sought to enforce a general covenant against competition against a former franchisee and her husband. *Id.* at 758. The franchisee said she did not receive any “trade secrets, confidential information or customer lists” from the franchisor. *Id.* at 762-63. She had a list of the customers who used her service while with the system, which she continued using after leaving to take advantage of the customer affiliations. *Id.* at 765. In enforcing the covenant, the court discussed Block’s “valuable property right in its service mark.” *Id.* at 763. The court rejected the franchisee’s argument that the customers belonged to her, concluding that she paid good money for the franchise because she saw the value of the brand name in attracting customers and that the name had, in fact, attracted the customers. *Id.* at 763-64. The court concluded:

“[A]t the time [the franchisee] entered the contract with Block, both parties understood that the bargain for use of the Block service mark was a bargain for customers who would be attracted to the Block name. She cannot now be heard to claim Block has no protectible interest in those customers she gained while offering services under that name.” *Id.* at 764.

A “grant-back” clause defeated one franchisee’s claim that it owned customer data in *Geib v. Amoco Oil Co.*, 29 F.3d 1050 (6th Cir. 1994) (applying Michigan law). The franchisee sought to control the customer data, arguing that a representative of the franchisor had verbally promised the company would hold the customer data in confidence. *Id.* at 1061. The court found that there was little credible evidence of such an agreement and that it was contrary to the franchisor’s express right to use the data for promotional and other purposes. *Id.* Most significantly, the court held that the agreement of the parties provided that “all rights herein granted the Dealer shall . . . revert to Amoco” upon termination or expiration of the agreement. *Id.* In effect, because of that simple “grant-back” clause, the franchisor was able to retain access to the data. However, the court did not determine whether the franchisor’s access was exclusive—whether the franchisee would be barred from using the data that had reverted back to the franchisor.47

---

47 See also *Economou v. Physicians Weight Loss Centers of Am.*, 756 F. Supp. 1024, 1032 (N.D. Ohio 1991), where, despite little evidence that a terminated franchisee was using confidential information or trade secrets, the court enforced a post-term noncompetition clause because the former franchisee’s existing business posed danger to the franchisor’s prospective business, including potential harm to the franchisor’s goodwill if the franchisee were allowed

Continued on following page
We have described all of the cases we are aware of where courts have enforced contracts involving customer data that is not a trade secret. To the extent we can draw lessons from such a small universe of cases, it is that: (a) it is important that franchise agreements clearly address the issue of who owns and has what rights and duties regarding customer data (whether or not it is a trade secret); (b) some courts will enforce relatively broad “grant-back” clauses; (c) it may be wise to limit the scope of the contractual restrictions in recognition of the fact that most customer data has a limited useful life; and (d) enforcement may be more likely if the customer data consists of quite a lot more detail about the customers than just names and addresses. The law has not yet developed to where we can provide clear guidance in this area.

III. PRIVACY

We now consider what responsibilities and liabilities follow from a franchisor’s decision to assert ownership or control over or require access to customer data collected by franchisees.\(^{48}\) Collecting, maintaining or having access to customer data implicates a wide variety of federal, state, local and international legal issues and concerns. We offer the following as merely a survey of this rapidly developing body of law. It is now necessary for franchisors and franchisees to consider carefully what information they collect, what they need, why, and what they are going to do with it while it is in their possession. Some privacy issues have become a hot topic because they have recently been a source of class action litigation.

There are several federal statutes which govern privacy in the United States. While some of these statutes are unique to the federal government accessing information, the vast majority cover private entities, including franchisors and franchisees. The federal statutes govern how a company may collect or gather information regarding customers or employees, how the company must then protect such data, what the company should do in case of a breach of security, and whether the company may share the data with third parties (i.e., whether a franchisee may share the information with the franchisor and vice versa). In addition, there are several federal statutes unique to certain industries (i.e., financial institutions, the medical industry, cable companies, videotape/DVD rental companies, etc.). In addition, there are also several state laws which govern residents’ privacy rights.

A. \textbf{Restrictions On Gathering, Using and Sharing Information}

We begin with an overview of federal and state statutes governing gathering, using and sharing customer data.\(^{49}\)


\(^{49}\) In addition to the statutes referenced in this section, it is important to note that there are also many statutes which govern how an employer may gather information regarding an employee. See, e.g., the Employee Polygraph Protection Act of 1988 and the Electronic Communications Privacy Act.
1. Privacy Policies Found On Websites: In General, No Federal Requirement To Implement A Privacy Policy

Many companies adopt privacy policies, motivated by an evolving array of laws and by a public that increasingly demands assurance that their personal information will not be misused and will be protected from identity theft. In addition, there are several state laws, as well as industry specific laws which require online privacy policies. A company should seriously consider whether or not to adopt such a policy, as well as what to include in such a policy. There is no one set definition of a privacy policy. In general, privacy policies explain to users what type of information a business will collect, how the information will be used, how the user can access this data and/or how the user can have the data removed. Often, a privacy statement will also include information regarding how the collecting company will protect the data. Although this section of the paper discusses privacy policies found on websites, privacy policies also exist for more traditional ways of collecting information other than websites. For example, the notices required by both the Gramm-Leach-Bliley Act (“GLBA”) and the Health Insurance Portability and Accountability Act (“HIPAA”) must also contain a privacy policy.

In general, there is no federal requirement that companies must have privacy policies, let alone that they must post such policies on their websites; however, there are several state laws that require privacy policies. California was the first state to require commercial websites and online services operators to post a privacy policy when it adopted the California Online Privacy Protection Act in 2003 (“OPPA”). Like many of California’s privacy statutes, OPPA extends beyond California’s borders and requires any person or company operating a website that collects personally identifiable information from California consumers to post a conspicuous privacy policy on the homepage or the first significant page after entering the website. As written, the statute is not limited to businesses located within California. Rather, conceivably, regardless of where the business is located or headquartered, if it collects personally identifiable information online about an individual consumer who is located in California, the company would be covered by OPPA. In order to comply, the privacy policy must identify what types of personally identifiable information is collected about consumers who use or visit the website, identify the third parties with which the information may be shared, describe how consumers may review and request changes to their personally identifiable information (if there is such a

---


52 Although there is no federal requirement in general, there are federal requirements which address privacy issues in certain industries, such as the financial industry and the medical industry. For a discussion of some of these industry-specific statutes, see infra Part III.E.


55 Personally identifiable information includes the collection or maintenance of the following information: first and last name; home or physical address; email address; telephone number; social security number; or any other identifying information that permits the physical or online contacting of a specific individual. Id. at §§ 22575(a), 22577(b).

56 Id. at § 22577(c).
process), describe how users will be notified regarding changes to the privacy policy, and identify the effective date of the policy.\textsuperscript{57}

In franchise settings where OPPA might apply, there may be risks if all of the privacy policies in a system are not consistent. At a minimum, they should clearly state that information will be shared between franchisor and franchisee. In some cases, the party receiving the data from the collecting party may be required to comply with the privacy policy of the collecting party. Franchisors also must be aware of and comply with OPPA with regard to the franchise opportunity page of their website—at least to the extent they are collecting information from California residents. In addition, franchisors need to consider whether their franchise brokers (by whatever name they are called) comply with OPPA and in a way that permits the franchisor to lawfully receive the data. The franchisor may have to comply with the broker’s privacy policy.\textsuperscript{58} Franchisors should certainly consider obligating their brokers to comply with the franchisor’s privacy policies.

Regardless of whether a statute requires a privacy policy, once a company adopts a privacy policy, the Federal Trade Commission (FTC) may pursue a company’s failure to abide by its own adopted policy. The FTC’s mission in this context is to protect consumers from “unfair and deceptive trade practices.” Under 15 U.S.C. § 45, more commonly known as Section 5 of the FTCA, “unfair or deceptive acts or practices in or affecting commerce...[are] unlawful.” The FTC uses Section 5 as a means of pursuing companies that violate their own privacy policies. Other laws whose violation the FTC may pursue through authority conferred by the FTCA include the Children’s Online Privacy Protection Act, the Gramm-Leach-Bliley Act (“GLBA”), the Telemarketing and Consumer Fraud Abuse and Prevention Act, and the Fair Credit Reporting Act (“FCRA”) (discussed \textit{infra} Part III.E.). Some states by statute specifically provide that knowingly making false or misleading statements in a privacy policy is a violation of the state’s Unfair Business Practices Act.\textsuperscript{59}

\subsection*{2. Gathering Information Online Regarding Minors}

If a franchisor or franchisee is gathering personal information regarding children under the age of 13 on the internet, it must comply with the Children’s Online Privacy Protection Act (“COPPA”).\textsuperscript{60} COPPA requires that websites must post privacy policies and obtain “parental consent for the collection, use, or disclosure of personal information from children.”\textsuperscript{61} COPPA

\textsuperscript{57} Id. at § 22575(b).
\textsuperscript{58} For example, see Days Inn privacy policy, http://www.daysinn.com/DaysInn/control/privacy_policy (last visited July 26, 2007); Dunkin Donuts, https://www.dunkindonuts.com/help/Privacy.aspx (last visited July 26, 2007) (the privacy policy specifies “The Franchise Opportunity Web site collects personal information from candidates. Please note that the privacy policy of the Franchise Opportunity Web site, not the DunkinDonuts.com privacy policy, applies to the Franchise Opportunity Web site.”). Since OPPA covers both collection of data and maintenance of data, it could cover both franchisor and franchisee.
\textsuperscript{61} “Personal information” includes: a first and last name; a home or other physical address including street name and city or town; an e-mail address; a telephone number; social security number; any other identifiable information that permits the physical or online contacting of a specific individual; or, any information concerning the child or the parents of that child that the website collects online from the child and combines with an identifier described above. Id. at § 6501(8).
applies only to websites “directed to children” or where the operator of the website “has actual knowledge that it is collecting personal information from a child.”

3. **Gathering Information Through Telemarketing**

Under the Telemarketing and Consumer Fraud Abuse and Prevention Act, telemarketers must clearly disclose at the outset of the call the seller’s identity, the purpose of the call, and what goods or services the seller is offering to the consumer. Telemarketers are prohibited from using false pretenses to induce consumers to pay for goods or services. Franchise systems that use telemarketing must comply with this statute. Depending on the franchise agreement, both parties may be responsible for compliance. This is another situation where careful drafting is needed.

4. **Social Security Numbers**

There are several state laws that require either truncation of social security numbers or prohibit their use to identify consumers. In addition, there are also proposed federal bills regarding the use of social security numbers.

---

62 Id. at § 6502(a). For examples of websites with privacy policies that seem to be trying to cover the COPPA requirements, see Gymboree, http://www.gymboree.com/our_company/help_template.jsp?FOLDER%3C%3Efolder_id=2534374302778339&bmUID=1185487284483 (last visited July 26, 2007) (“How We Protect Children’s Privacy. Gymboree is concerned about the safety and security of children when they use the Internet. Our web sites are general audience sites. We will not knowingly accept personally identifiable information from anyone under the age of 13. Children under the age of 13 must ask a parent or guardian for permission before providing any personal information online.”) and Blockbuster, http://www.blockbuster.com/corporate/privacyPolicy (last visited July 26, 2007) (“How Does Blockbuster Handle Information from Children? Please note that Blockbuster has no intention of collecting personal information from individuals under the age of 13 (‘children’). We are committed to protecting children’s privacy on the Internet and we comply fully with the Children’s Online Privacy Protection Act (COPPA). Where appropriate, we will instruct children not to provide such information to us. If a parent becomes aware that a child has provided us with personal information, we ask that the parent or legal guardian of the child contact us by sending an e-mail to blockbuster@custhelp.com or in writing to 1201 Elm Street, ATTN: Online Customer Loyalty, Dallas, TX 75270 to request that this information be deleted from our records.”).


64 See id. at § 6102.

65 For example, if the franchisor requires the franchisee to use a specific script in its telemarketing activities that results in a violation. Another example would be where the franchisor requires the use of a franchisor-provided “on-hold” message that contains the violation.


5. Spyware

Spyware is software that can track or collect the online activities and personal information of internet users, change settings on computers and cause advertising messages to pop up. Internet users are often unaware that Spyware has been downloaded into their computers, and Spyware is often extremely difficult to remove. Spyware has become more prevalent and can "become buried among code for other programs...[making it] difficult to detect and remove."\(^{68}\)

In addition to some pending federal bills,\(^{69}\) several states have passed anti-spyware statutes. The California Consumer Protection Against Computer Spyware Act\(^{70}\) bans unauthorized users from willfully loading software onto a resident's computer and using the software to do certain activities. The Act prohibits misleading residents to install a software component by intentionally misrepresenting that it is necessary for security or privacy or misleading residents to open, view, or play a particular type of content.\(^{71}\) The Act may be privately enforceable under California’s Unfair Competition Law.\(^{72}\)

Arizona, Arkansas, Georgia, Indiana, Iowa, Louisiana, New Hampshire, Texas, and Washington have similar anti-spyware statutes.\(^{73}\) In addition, Alaska and Utah have enacted statutes that only ban Spyware that causes pop-up advertisements.\(^{74}\)

---

\(^{68}\) Hines, supra note 67.

\(^{69}\) The House Energy and Commerce Committee unanimously approved the Securely Protect Yourself from Cyber-Trespass, or Spy Act, in early May 2007. Hines, supra note 67. The Spy Act would prohibit gaining control of an end user's computer through keystroke-logging programs, changing a user's home page, modifying other internet settings, or installing "information collection programs," without prior approval from the consumer via an end user licensing agreement ("EULA"). H.R. 964, 110th Cong. § 2 (2007). The Spy Act would preempt similar state laws, except for laws that cover trespass, contract, torts, or fraud. Id. at § 6. The Spy Act also would require that distributors of legitimate "information collection programs" both obtain the consumer's consent through a "clear and conspicuous notice" and build the program so that it is easily identifiable and easily removable. Many advertisers are opposed to the Spy Act because of their fear that it would cover cookies. Cookies are files stored on a user's hard drive by the user's web browser such as Internet Explorer or Netscape, which are created at the request of a website, unless the user has disabled that function in his or her browser. Cookies allow websites to "remember" facts about a visitor, such as a login ID and password, as a visitor browses through a site. Without cookies, users have to login anew at every page visited at a secure website. In addition, advertisers use cookies to target advertisements to particular users based on their browsing history. While the Spy Act exempts cookies from "information collection programs," online advertisers and marketing groups oppose the notice requirement, arguing that "new, non-cookie technologies down the pipe could be threatened by the bill." Anne Broache, House Committee Endorses SSN Limits, Antispyware Effort, CNET News.com, May 11, 2007, http://news.com.com/2100-7348_3-6182973.html (last visited July 26, 2007). Another recent bill passed by House committees, the Internet Spyware Prevention Act of 2007, has the support of advertisers and marketing groups because it provides up to five years imprisonment for malicious spyware activities, without regulating the technology involved and focusing instead on the intent of the activities. See H.R. 1525, 110th Cong. § 2 (2007). Thus, the intent behind using the technology rather than the mere use of the technology would be punishable.


\(^{71}\) Id. at § 22947.2.-3.

\(^{72}\) CAL. BUS. & PROF. CODE § 17200 et seq. (2007).

\(^{73}\) ARIZ. REV. STAT. ANN. § 44-7304 (2007) (The State Attorney General may seek injunctive relief and recover the greater of actual damages or $100,000 for each violation. In addition, suit may be brought by computer software providers and website and trademark owners affected by a violation of the state law.). GA. CODE ANN. § 16-9-150, et

Continued on following page
6. **Do Not Call Lists**

In the process of gathering information regarding consumers, it is important that companies heed the various federal statutes that would fall under the rubric of “do not call” lists. The Telephone Consumer Protection Act (“TCPA”) allows consumers to request that telemarketers not call them again.\(^75\) If, after such a request, the telemarketer continues to call, consumers may sue for actual damages or $500 for each such subsequent call, whichever is greater.\(^76\) In addition, the TCPA prohibits the transmission of unsolicited fax advertisements and of faxes that do not provide proper identification of the sender.

Additionally, people may voluntarily register their phone number on the National Do Not Call Registry.\(^77\) Once a consumer’s phone number is on the National Do Not Call Registry, telemarketers are prohibited from calling that number.

7. **E-Mail Marketing**

Congress has considered adopting a federal do not e-mail list, much like the do not call list, but the FTC has argued any such list would more likely aid abusers than reduce spam.\(^78\) Congress, however, has adopted the Controlling the Assault of Non-Solicited Pornography and Marketing Act (“CAN-SPAM”)\(^79\) to try to control spam. It prohibits knowingly sending commercial messages that deceive or mislead recipients (note that while the word “pornography” is in the title of CAN-SPAM, it is not limited to pornographic messages, but rather encompasses all commercial emails). CAN-SPAM requires commercial e-mail to include: “(1) clear and conspicuous identification that the message is an advertisement or solicitation, (2) clear and conspicuous notice of the opportunity to decline to receive further commercial email..."
from the sender and (3) a valid physical postal address of the sender. The act provides both civil and criminal penalties. The government (i.e., the FTC and attorneys general) has broad enforcement rights and providers of “internet access service” may bring suit—but not consumers or businesses receiving spam. The definition of an internet access service provider has been interpreted very broadly to include any entity that provides e-mail accounts and e-mail access, such as a university, or that allows users to send messages to one another, such as myspace.com. The FCC has held that CAN-SPAM covers wireless providers, thus banning wireless providers from sending Mobile Service Commercial Messages (“MSCMs”) without express prior authorization by the consumer.

Several states have enacted legislation regarding marketing to minors. Michigan and Utah have passed statutes aimed primarily at preventing children from receiving electronic communications containing material that a child should not be receiving (i.e., advertisements for guns, alcohol, pornography, etc.). Both states have set up “do not e-mail” registries for minors, defined as children under 18 years of age.

Georgia, Connecticut, Iowa, Illinois, Wisconsin and Hawaii have also considered and rejected legislation that would create similar registries for minors. The states’ rejections appear to be influenced by an FTC report to Congress presenting the policy arguments for and against creating a national “do not e-mail registry.” In particular, the registry laws are intended to prevent children from receiving or viewing materials that are unsuitable for their age. The FTC report argues that these laws have been relatively ineffective at preventing children from receiving inappropriate materials, that they impose considerable costs on legitimate businesses, and that owing to current limitations on information security the list of validated children’s e-mail addresses could be obtained more easily by pedophiles or other criminals than before creation of a registry. In other words, the registries will most likely be misused rather than deter any type of inappropriate activity.

The CAN-SPAM Act pre-empts state laws that expressly regulate commercial electronic mail, with exceptions for state laws relating to fraud, falsity or other deceptive practices. In addition, state laws that are not related to electronic mail (i.e., criminal laws, contracts, torts, trespass) are also not pre-empted. A Utah federal court held that the Act does not pre-empt Utah’s statute which provides for a do not e-mail registry for minors. Free Speech Coalition, Inc. v. Shurtleff, No. 2:05CV949DAK, 2007 U.S. Dist. LEXIS 21556, at *20-5 (D. Utah Mar. 23, 2007).

---

82 White Buffalo Ventures, LLC v. Univ. of Tex., 420 F.3d 366, 372-73 (5th Cir. 2005).
87 Snell & Itatani, supra note 80.
88 Id.
B. Sharing Data Between Franchisor and Franchisee

The franchise relationship may make compliance with the maze of privacy statutes and rules challenging—for both franchisors and franchisees. Many existing franchise agreements did not anticipate this body of law. Depending upon the nature of the parties' business, where each of them does business, where any of their customers live, and what information they may want to collect, maintain or use, the parties may have to sort out many layers of overlapping and inconsistent laws and regulations—in an environment where federal and state governments are rapidly legislating in response to newly perceived threats.

The parties may have to decide who has the right or obligation to publish a privacy policy and whether it is prudent to publish a privacy policy or to require or permit the other party to do so. If the franchisee publishes a privacy policy (or fails to publish one if required) and it is different than the franchisor’s policy, it may be unclear which policy governs and who has liability and other responsibilities arising out of a possible breach of conflicting policies.

Franchisors and franchisees often want or need to transfer or share customer data among franchisees (such as in a marketing cooperative), between the franchisor and franchisees (this may occur in the ordinary course of business, pursuant to a “grant-back” clause or even in the course of an audit), and between franchisors (or franchisees) and their affiliates—or third parties, including vendors. The duties may differ based on whether the transferor and transferee of the customer data are “affiliates.” Unfortunately, in making even that determination, we face multiple definitions of “affiliate.” For example, the FTC has its definition, the GLBA has its definition, and California’s FIPA has its own definition.

We have found no judicial or legislative guidance on the specific question of whether or to what extent a claim of ownership in a franchise agreement will impact the rights and responsibilities of the parties with respect to customer data under the applicable privacy laws. Likewise, we have found no authority on the question of whether or to what extent the assumption of duties or control under the privacy laws will impact the question of who owns or has post-termination rights to customer data. We cannot foresee how the courts will resolve such questions, but do anticipate that, in responding to this rapidly changing area of law, the courts will have to revisit—and perhaps revise—many of the policies we describe in this paper. To all of the balancing of factors in both the trade secrets analysis and the contract analysis, the courts may now need to add the interests of the customers whose data is in question, which interests the courts will probably view through the prism of statutory and regulatory schemes that are currently in a dynamic stage of development. We do not know how the courts will the answer such questions. However, we think courts will probably begin to take into consideration privacy issues in determining ownership and ownership issues in determining privacy rights and responsibilities.

Currently, the potential questions far outnumber the known answers. For example, if a franchisee, without the franchisor’s knowledge or consent, makes representations to customers contrary to the franchisor’s policies regarding what will or will not be done with customer data, does the franchisor have a remedy? Does that potentially place the data out of the franchisor’s reach? If such a “rogue” franchisee leaves the system for any reason, can the franchisor transfer the customer data to a new franchisee? If the applicable privacy policy is silent on the specific issue, can the franchisor make such a transfer in any event? What governs? Who decides? If a franchisor has not anticipated the privacy law developments, can the franchisor
get all this under control without signing new contracts with all franchisees? Is it possible to make a sufficient change in the operations manual?\textsuperscript{89}

Taking the franchisor/franchisee dynamics to the next plane, let us assume a franchisee is contractually required to share data with the franchisor, and then later, the franchisee adopts a privacy policy that is unauthorized (but not prohibited) by the franchisor. Can the franchisor terminate the franchisee under a breach of contract theory for refusing to turn over customer data when to do so would be in violation of the franchisee’s privacy policy? Would that be a wrongful termination under applicable franchise laws? What if the franchisee’s privacy policy is so strong that the franchisee refuses to permit a meaningful audit on that basis? If the franchisee acquiesces, does that create a breach, reportable or not, and is the franchisor then liable to the customers; is the franchisor liable for statutory penalties, if any?

The other side of this hypothetical is the franchisee who adopts a very broad privacy policy giving little protection to customer data. If the franchisor has not retained the right to require certain minimum privacy protections, such a situation could affect the franchisor’s ability to share with that franchisee data it has received under its own privacy policy which provides for greater protection of customer data. It certainly might impact the ability of the franchisor to share with that franchisee information it received from customers in the European Union and other countries with stringent privacy laws. In that situation, the franchisor would also need to concern itself with the extent to which its other franchisees (who did have compliant policies) shared information they received from the franchisor or other franchisees with the franchisee whose published policy provides little or no protection. Depending upon the circumstances, the franchisee providing information to another franchisee who has committed to a lower level of protection may also have reasons for concern.

Because franchising always involves multiple parties (franchisor, franchisee, other franchisees, parents, affiliates, vendors and others) who have some common and some conflicting economic interests and potentially conflicting interests in customer data and privacy issues, these will not be easy questions to answer. The risk of being held responsible for a violation by someone you had no contractual control over is real—especially where the parties cannot agree to necessary amendments to a legacy contract.

C. Protecting Data After It Has Been Legally Gathered

1. Security Safeguards

In the past few years, the FTC and state attorneys general have been cracking down on companies which lack adequate security safeguards to protect consumers’ personal information. The FTC has defined “adequate” security safeguards in its report to Congress entitled “Privacy Online: Fair Information Practices in the Electronic Marketplace.”\textsuperscript{90} Interestingly, even if the company does not have a privacy policy in place or any type of policy under which the company promises consumers to safeguard their information, the FTC has nonetheless pursued some companies under Section 5. Penalties include civil penalties of

\textsuperscript{89} Catharine Boschee, Thomas Epstein & Karin Simonson, IMPLEMENTING A FRANCHISE-WIDE DATA PROTECTION PROGRAM (Int’l Franchise Ass’n 40th Annual Legal Symposium 2007).

$11,000 for each violation, where each day a violation occurs is considered a separate violation.\textsuperscript{91}

A well known example of such FTC enforcement is BJ’s Wholesale Club, Inc. BJ’s did not have a privacy policy, but it did collect consumers’ personal information. The FTC determined that BJ’s had failed to take “appropriate measures” to protect the security of sensitive information about thousands of customers, including names, credit or debit card numbers and expiration dates.\textsuperscript{92} Two banks have also sued BJ’s on these privacy issues.\textsuperscript{93}

Other recent examples of FTC action include:

- **Guess.com.** Guess.com was vulnerable to commonly known attacks by hackers, and consumer information was not always stored in an encrypted format.\textsuperscript{94}

- **Tower MTS, Inc. (“Tower”).** When Tower redesigned its website, the site contained a security flaw that allowed any person who entered a valid order number to view the order history and personal information of the customer who placed the order.\textsuperscript{95}

- **Petco.** Petco failed to implement reasonable and appropriate security measures to protect sensitive consumer data and did not encrypt the information. A hacker was able to access consumer records, including credit card numbers.\textsuperscript{96}

\textsuperscript{91} Pursuant to Section 5, the Commission may file complaints, hold hearings, issue orders and penalize “persons, partnerships or corporations” for trade practices which “cause or likely cause substantial injury to consumers.” See 15 U.S.C. § 45(a)(2), (n) (2006).


\textsuperscript{93} See Sovereign Bank v. BJ’s Wholesale Club, Inc., No. 1:CV-05-1150, 2006 WL 1722398 (M.D. Pa. June 16, 2006); Banknorth, N.A. v. BJ’s Wholesale Club, Inc., 442 F. Supp. 2d 206 (M.D. Pa. 2006). In Sovereign Bank, the plaintiff, an “Issuing Bank” in the Visa system, sought damages from BJ’s and another defendant (the “Acquiring Bank”), for losses incurred to cover unauthorized charges to customers’ accounts and the costs of reissuing new debit cards as a result of the theft of its customers’ account information from BJ’s computer files. Sovereign accused both BJ’s and the Acquiring Bank of breach of contract, negligence, equitable indemnification, and promissory estoppel. Sovereign also accused BJ’s of breach of fiduciary duty. With the exception of Sovereign’s claim of breach of contract against the Acquiring Bank (which was later dismissed on a motion for summary judgment), the district court dismissed each of Sovereign’s claims. See 427 F. Supp. 2d 526 (M.D. Pa. 2006); 395 F. Supp. 2d 183 (M.D. Pa. 2005). Sovereign appealed the court’s decision regarding each of its claims and the Third Circuit heard oral argument on June 19, 2007. Similarly, in Banknorth, the plaintiff, an “Issuing Bank” in the Visa system, sought damages from BJ’s and the Acquiring Bank for losses incurred to cover unauthorized charges to customers’ accounts and the costs of reissuing new debit cards as a result of the theft of its customers’ account information from BJ’s computer files. Banknorth accused both BJ’s and the Acquiring Bank of breach of contract, negligence, and equitable subrogation. On BJ’s motion for summary judgment, the court denied each of Banknorth’s claims against BJ’s. See 442 F. Supp. 2d 206. Banknorth’s claims against the Acquiring Bank remain, but the case has been stayed pending the Third Circuit’s decision on the Sovereign appeal.


DSW, Inc. ("DSW"). DSW stored consumer credit card, debit card and check information on its in-store computer network. The FTC alleged that several of DSW's practices, when combined, made sensitive consumer information unsecure. The FTC gave examples of practices such as retaining data in multiple files after there was no longer a legitimate business need to keep it, failing to use common security measures to limit wireless access to computer networks, storing information in unencrypted files that could easily be accessed with a commonly known user identification name and password, failing to adequately limit the ability of computers on one in-store network to connect to computers in other in-store networks, and failing to use sufficient measures to detect unauthorized access. About 1.4 million credit and debit cards and 96,000 checking accounts were compromised as a result of DSW's practices and fraudulent charges remained on some of those accounts. 

In addition, commentators have noted that the federal Sarbanes-Oxley Act ("SOX Act") requires some protection of financial information. For example, Section 404 of the SOX Act and its implementing regulations require public companies' CEOs and CFOs to certify to the SEC that their financial information is accurate and that they have maintained adequate "internal controls" to ensure adequate financial information reporting. Such internal controls would necessitate adequate data protection mechanisms for financial information.

Also, some states require adequate security for information that has been gathered regarding their residents. For example, California law requires a business that "owns or licenses" personal information regarding California residents to "provide reasonable security" for that information. Furthermore, this California law also requires that a business that "discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party shall require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information..." 

Several state statutes require internet service providers ("ISPs") to protect the confidentiality of their website customers’ and/or users’ personal information. Minnesota requires ISPs to maintain the confidentiality of their customers’ information that identifies: (1) the customer's physical or electronic address or telephone number; (2) whether the customer

---

100 Christopher Wolf et al., PROSKAUER ON PRIVACY: A GUIDE TO PRIVACY AND DATA SECURITY IN THE INFORMATION AGE § 2.8 (2006).
102 CAL. CIV. CODE § 1798.81.5 (2007) (stating that "owns or licenses" includes, but is not limited to "personal information that a business retains as part of that business' internal customer account or for the purpose of using that information in transactions with the person to whom the information relates.").
has requested or obtained specific materials or services from an ISP; (3) the internet or online sites that the customer visited; or (4) the contents of a customer’s data storage devices. Customers may bring private actions under this statute and may recover the greater of $500 or actual damages as well as costs and attorneys’ fees. Nevada also requires that ISPs keep confidential “all information” concerning their subscribers, imposing fines up to $500 for each violation.

2. Notification To Consumers Regarding Disclosures To Third Parties

Privacy policies, in order to be in compliance with the FTC’s Fair Information Practices and to comply with California’s OPPA, must provide for notification to consumers regarding disclosures to third parties. Many of the statutes governing the financial and telecommunications industries require similar notifications. While the Federal Right to Financial Privacy Act (“RFPA”) provides that government officials and certain financial institutions must use a warrant or subpoena to obtain certain consumer financial information, a number of states have incorporated provisions similar to the RFPA extending the requirements to private parties. Thus, before such information may be shared with a private party, the company that is sharing the information must make sure it is complying with the appropriate laws. The definition of a financial institution is also much broader under the state statutes.

In addition, online businesses that collect information about California or Utah customers must notify consumers whenever they intend to disclose personal information to a third party for direct marketing purposes or for compensation.

103 MINN. STAT. ANN. §§ 325M.01(5), 325M.02 (2007).
104 Id. at § 325M.07.
107 See, e.g., GLBA, 15 U.S.C. § 6802 (setting forth notice requirements for financial institutions before disclosure of nonpublic personal information to third parties); infra Part III.E (discussing industry-specific notice requirements).
111 In California, this type of “personal information” is defined as any information that is maintained by an agency that identifies or describes an individual, including, but not limited to, his or her name, social security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history. CAL. CIV. CODE § 1798.3(a) (2007). It includes statements made by, or attributed to, the individual. Id. In Utah, “personal information” includes non-public information that distinguishes a person from others such as a person’s social security number, proof of credit worthiness, income, employment history, purchasing patterns or personal preferences, when either alone, or joined with public information. UTAH CODE ANN. § 13-37-102(5) (2007).
112 CAL. CIV. CODE § 1798.3(a) (2007); UTAH CODE ANN. § 13-37-201 (2007). The Utah statute provides that a business may not disclose nonpublic, personal information about a consumer to a third party for compensation, Continued on following page
California’s “shine the light” law provides that, if a company discloses a California resident’s personal information to a third party for that party’s direct marketing purposes, the company must at least once a year, upon the consumer’s request, provide the consumer with the names and addresses of the third-party recipients of that information, as well as specific details regarding the information disclosed. In addition, companies must include online privacy policies on the websites that notify California residents regarding their rights under the statute. “Personal information” includes data such as social security numbers, bank account numbers and credit or debit card numbers.

3. Companies That Issue Credit Card Receipts: FACTA

The Fair and Accurate Credit Transactions Act of 2003 (“FACTA”) is a federal law that gave companies who accept credit or debit cards three years to comply. On December 4, 2006, FACTA became fully effective. FACTA prohibits companies from giving consumers electronic receipts that are not truncated (i.e., that display more than the last five digits of the credit or debit card or the expiration date). Unless the receipt is handwritten or an imprint of the credit card, if more than the last five digits or expiration date is shown on the receipt, and even if the company was merely negligent in failing to comply with FACTA, the consumer may be awarded actual damages, including compensation for out-of-pocket losses, embarrassment and humiliation, mental distress, pain and suffering, and attorneys’ fees and costs. If the company’s failure to comply was willful or in reckless disregard of the Act’s provisions, FACTA provides for actual damages of not less than $100 or more than $1,000 per violation, plus punitive damages, in addition to attorneys’ fees and costs. FACTA imposes liability on the entity that generates the receipt. In the franchise context, FACTA could create a problem for both parties if a franchisor requires a franchisee to use an older model terminal that issues non-compliant receipts. There is a risk that a franchisee’s independent use of an older model terminal and possible resultant litigation and publicity could cause serious harm to the system’s goodwill and name.

unless it provides a notice to the consumer that reads substantially as follows: “We may choose to disclose nonpublic personal information about you, the consumer, to a third party for compensation.” Utah Code Ann. § 13-37-201(3)(a) (2007). Violations can cost up to $500 for each occurrence and court costs. Id. at § 13-37-203. Similarly, the California statute requires covered businesses to disclose to California customers, upon request, the categories of personal information disclosed to third parties for direct marketing purposes, as well as the names and addresses of the third parties. Cal. Civil Code § 1798.83. Alternatively, the company can comply by implementing a privacy policy that allows consumers to opt in or opt out of information sharing. Id. at § 1798.83(c)(2). Consumers who are “harmed” may sue to recover damages; civil penalties are between $500 and $3,000 per occurrence, and attorney’s fees. Id. at § 1798.84.

113 Cal. Civil Code § 1798.83(b).

114 Alternatively, companies may comply with the law by providing an opt-in or opt-out policy for sharing information with third parties for direct marketing purposes. In addition, companies doing business in California (i.e., selling products and services to California residents), that cannot argue preemption by federal law, will need to comply with California’s Financial Information Privacy Act (“FIPA”). Cal. Fin. Code §§ 4050-4060 (2007).


4. **Destroying Data**

Some states require customer data to be destroyed or shredded once it is no longer needed. For example, Arkansas requires businesses to “take all reasonable steps to destroy or arrange for the destruction of a customer’s records within its custody or control containing personal information which is no longer to be retained by the person or business by shredding, erasing, or otherwise modifying the personal information in the records to make it unreadable or undecipherable through any means.”\(^{118}\)

Texas requires businesses to develop retention and disposal procedures for their clients' personal information.\(^{119}\) The law provides for civil penalties of up to $500 for each abandoned record. Recently, the Attorney General of Texas has pursued legal action against Radio Shack for dumping bulk customer records in garbage containers behind a store. According to the Attorney General, the records “contained sensitive consumer information, including Social Security numbers, credit and debit card information, names, addresses, and telephone numbers.”\(^{120}\)

California also requires businesses to “take all reasonable steps to destroy, or arrange for the destruction of a customer’s records within its custody or control containing personal information which is no longer to be retained by the business by (1) shredding, (2) erasing, or (3) otherwise modifying the personal information in those records to make it unreadable or undecipherable through any means.”\(^{121}\)

Given these state laws, and special industry standards which require the destruction of data, as well as the potential negative effect on consumers who believe their data is not being disposed of properly, companies should seriously consider whether or not they should adopt a data destruction policy and the specifics of such a policy.

**D. Breach of Security**

Once a franchisor or franchisee has legally gathered a consumer's information and taken the required steps to protect it, the franchisor and/or franchisee may need to comply with laws requiring notification of any potential breach of the security system.

Most states now have statutes that require companies to notify consumers in the event of a security breach (or a potential security breach). In addition, as discussed below, when a security breach occurs and the company does not notify the consumers, this may produce negative media attention and damage a company’s reputation. A franchisee’s failure or inability to give the required notice could have an obvious adverse impact on a franchisor’s name and reputation—even if the failure was out of ignorance. Arguably, the FTC could pursue a company’s lack of notification under Section 5 as an “inadequate” security standard. Thus, a


\(^{119}\) Chapter 35 of the Business and Commerce Code, § 35.48 (2007).


\(^{121}\) CAL. CIVIL CODE § 1798.80 et. seq. (2007). There is currently pending in California a bill which would require retailers to dispose of records containing personal information within 90 days of the transaction or within the period of time during which goods may be returned for a refund or exchange, whichever is shorter. A.B. 779, 2007 Sess. (Cal.).
company should seriously consider whether or not to notify consumers when a breach has, or may have occurred.122


Most statutory activity regarding breach notification has been by states.123 California protects its citizens against security breaches, statutorily requiring notice to consumers when security breaches occur. The law is called the Security Breach Information Act (“SBIA”).124 Under the SBIA, any government agency, company or non-profit, regardless of its location, must “expeditiously” notify California customers if they suspect anyone has gained unauthorized access to California customers’ personal information125 that is held in computerized form, if it is not encrypted. The statute does not cover data which is not in computerized form; however, it is not clear what would happen if the data is a printout of computerized data. Although the California statute does not define what type of encryption is necessary, data encryption is generally defined as “[t]he translation of data into a secret code. . . .To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it.”126 It is interesting to note that the SBIA requires notice if the network is breached even if the customer’s private information was not taken. When the law was first enacted, it was not clear whether a company should notify only California consumers if there was a breach or all consumers regardless of residency.127 Many concluded that from a public relations and legal perspective, it would behoove a company to notify all consumers rather than limiting it to California residents.128

A few years after the SBIA was enacted, this hypothetical situation became a real world event. ChoicePoint, a Georgia-based consumer data company, maintained “personal profiles of nearly every U.S. consumer, which it sells to employers, landlords, marketing companies and about 35 U.S. government agencies.”129 ChoicePoint sold personal data on over 162,000 people to fraudulent companies established by a ring of identity thieves.130 ChoicePoint sent


123 Note that disclosure of security breaches may also be required under the FTC’s general enforcement powers under Section 5. See, e.g., the discussion of the FTC’s treatment of BJ’s Wholesale Club, Inc., supra Part III.C.1. In addition, security breach notifications may be required under the federal statutes which govern specific industries. Proposed federal legislation on a more general level has not been passed into law.

124 CAL. CIVIL CODE § 1798.82 (2007).

125 Personal information is defined as either a first initial (or name) and last name, and one of the following: Social Security Number; driver’s license number; California Identification Card number; or, bank account, credit card, or debit card along with a password or security code that would give access to the account.

126 See http://www.webopedia.com/TERM/E/encryption.html (last visited July 26, 2007), defining encryption. Also, note that other state statutes do define encryption. For example, Maine, Nevada, North Carolina, Ohio, and Pennsylvania’s statutes contain definitions of encryption.


128 Id.


notice of the breach to California residents only. Attorneys general in 38 states “join[ed] in an open letter…demanding” that ChoicePoint notify residents in other states as well.\textsuperscript{131} Soon after, over 30 states and New York City enacted statutes similar to SBIA.\textsuperscript{132} The ChoicePoint case is also noteworthy for representing the largest civil penalty the FTC has ever assessed for disclosing consumers’ personal financial information—$10 million in addition to $5 million in consumer redress. The FTC settlement also required ChoicePoint to implement procedures and security programs to protect consumers’ data, along with an audit every two years for the next twenty years by a qualified, independent, third-party professional.

Although the majority of state statutes regarding security breaches are limited to computerized data, a few state statutes are not so limited.\textsuperscript{133} California and several other states also provide for “security freeze” laws, which allow consumers to restrict access to their credit reports upon notification of a suspected identity theft or fraud.\textsuperscript{134}

2. Franchisor/Franchisee Issues

Even if franchisors and franchisees successfully navigate the shoals of lawfully collecting information, the question of protecting it may prove difficult.


\textsuperscript{132} See, e.g., ARK. CODE ANN. § 4-110-101 et seq. (2007); CONN. GEN. STAT. § 36a-701b (2007); FLA. STAT. § 817.5681 (2007); GA. CODE ANN. § 10-1-911 (2007); 815 ILL. COMP. STAT. 530/5, 530/10 (2007); IND. CODE ANN. § 4-1-11 (2007); MONT. CODE ANN. § 30-14-1704 (2005); NEV. REV. STAT. § 603A.030 et seq. (2007); N.D. CENT. CODE § 51-30-01 et seq. (2005); TEX. BUS. & COM. CODE ANN. § 48.001 et seq. (2007); WASH. REV. CODE § 19.255.010 (2007). See GA. CODE ANN. § 10-1-911 (apply only to “information brokers”), ME. REV. STAT. § 1347(3) (2007) (same). Maine LD 2017, effective January 31, 2007, applies to all other entities. See Arkansas Personal Information Protection Act of 2005, ARK. CODE ANN. §§ 4-110-101 through 4-110-108 (stating that individuals and businesses must “take all reasonable steps to destroy or arrange for the destruction of the customer’s records within its custody or control containing personal information which is no longer to be retained by the person or business by shredding, erasing, or otherwise modifying the personal information in the records to make it unreadable or indecipherable through any means.”). See N.Y. GEN. BUS. LAW § 899-aa(1)(B) (McKinney 2007); IND. CODE ANN. § 4-1-11(2); N.C. GEN. STAT. § 75-61(14) (2007) (notice may be required even if data that is encrypted has been compromised). See IND. CODE ANN. § 24-4.9-2(2007) (requiring notice where there has been a breach of computerized data that “had been transferred to another medium, including paper, microfilm, or similar medium, even if the transferred data are no longer in a computerized format”); N.C. GEN. STAT. ANN. § 75-61(12) (requiring notification when breach of any record occurs, not just breaches of computerized data). See CONN. GEN. STAT. § 36a-701b(a) (”breach of the security system” is defined as “the unauthorized acquisition of computerized data that contains personal information from any person that maintains such personal information.”). See N.D. CENT. CODE § 51-30-01(1) (”breach of the security system” is defined as “the unauthorized acquisition of computerized data when access to personal information has not been secured by encryption or by any other method that renders electronic files, media, or databases unreadable or unusable.”). See e.g., COLO. REV. STAT. § 6-1-716(1)(c)(IV)(A),(2)(a) (2007); FLA. STAT. § 817.5681(4); IDAHO CODE ANN. §§ 28-51-104(2), 28-51-105(1) (2007); MONT. CODE ANN. § 30-14-1704(4)(A); NEV. REV. STAT. § 603A.020 (2007); N.C. GEN. STAT. § 75-61(14); OHIO REV. CODE ANN. § 1349.19(A)(1)(a) (2007); TENN. CODE ANN. § 47-21-2107(a)(1)(2007); WIS. STAT. § 895.507(2)(cm) (2007); WASH. REV. CODE § 19.255.010(10)(d) (these statutes either require notification if the breach “materially” compromised security and confidentiality and exempt notice requirements if an investigator determines misuse of data has not occurred and is not reasonably likely to occur).


\textsuperscript{134} See CAL. CIV. CODE § 1798.92(a) (2007) (permits victim of identity theft to bring an action against a “claimant” defined as one who “has or purports to have a claim for money or an interest in property in connection with a transaction procured through identity theft”); see also COLO. REV. STAT. § 12-14.3-102 (2007); 815 ILL. COMP. STAT. ANN. 505/2MM (2007); TEX. BUS. AND COM. CODE § 20.01 (2007). These state statutes compliment consumers’ rights under the FCRA.
The parties may need to determine, presumably consistent with their agreement, and perhaps pursuant to the operations manual, what information to collect, how it will be kept, how long, and how to dispose of it. Some privacy laws do not limit their application to only the party that “owns” the customer data. Likewise, some do not limit their application to only the party that has “access” to the data. It may be that the franchisor and franchisee are in this together—sharing responsibility and risk.

It is axiomatic that any security system is only as strong as its weakest link. If the franchisee (or the franchisor or a vendor) does not have the resources or inclination to provide “adequate security,” that may expose the other party or parties to risk. If a breach occurs and one party does not have the resources to give the required notices, responsibility for paying that cost may transfer to the other parties who might have been in a position to provide or require adequate security. If a franchisee in California experienced or caused a breach and neither that franchisee nor the franchisor has the resources to give the notices, might a franchisee in Kansas who had access to the entire centralized database be required to bear the cost?

What about vicarious liability? If the franchisor requires the franchisee to use only proprietary hardware and software in conducting the business and the franchisee experiences a breach because of a security flaw in the software, it seems that both franchisor and franchisee might be liable for the violation but the franchisee might have a claim against the franchisor for indemnification or damages.

Many existing franchise agreements are silent as to privacy compliance issues but contain a simple obligation on the part of the franchisee to “comply with all applicable laws.” Query whether privacy law compliance was within the contemplation of either party at the time of the contract. It may not be clear whether a franchisor could properly impose upon an existing franchisee a substantial additional cost of privacy law compliance by making a change in an operations manual.

Can the franchisor, in light of its duties to its entire system, perhaps involving hundreds of franchisees in many states and several countries, afford the risk of leaving privacy law compliance in the hands of individual franchisees with various levels of ability and resources? What about the risk that one franchisee might publish a very restrictive (or the opposite) policy that ultimately affected the entire franchise system? We cannot yet ascertain how the traditional notions of vicarious liability will play out in this new area. If the franchisor imposes the burden of privacy law compliance on the franchisees, that presumably creates a disclosure issue—at least for new franchisees. The bottom line on Item 7 just got a lot bigger. In the right circumstances, the franchisor may have to also disclose the compliance requirements in Item 1.

Consider also the concerns a franchisee might have about a failing franchisor (e.g., _Brenco, supra_ pp. 29-31; see Ellen R. Lokker & Mark J. Loranger, _How Not to Run a Railroad_, Franchise Law Journal, Vol. 25, No. 1 (Summer 2005), at 11-17). In that situation, the

---

135 Boschee, et al., _supra_ note 89.

136 To further explore possible vicarious liability issues would be beyond the scope of this paper. The ABA Forum on Franchising has previously extensively covered the issues generally. See Claudia K. Levitas & Mercedes Gonzales Hale, _Vicarious Liability at Franchised Locations_, Franchise Law Journal, Vol. 26, No. 2 (Fall 2006); Rose Marie Fiore, _Vicarious Liability Cases: Duty to Defend and Conflicts of Interest_, 25-SPG Franchise L.J. 199 (2006).

137 Boschee, et al., _supra_ note 89.
franchisee would be concerned about liability flowing to him because the franchisor did not have the resources to comply.

One commentator expressed concern about increasing franchisor liability risk if they dictate franchisee privacy policies and suggested that franchisors require franchisees to adopt their own privacy policies that at least met minimum standards published by the franchisor—which would be modeled after the general privacy laws in the European Union and Canada, Catharine Boschee, Thomas Epstein & Karin Simonson, Implementing a Franchise-Wide Data Protection Program, International Franchise Association 40th Annual Legal Symposium, at 25-27 (2007).

As with the earlier question of how to lawfully collect customer data, this question of how to protect it after it is properly collected presents franchise lawyers with many challenges. We submit that a one-size-fits-all solution likely will not work and that franchisors and their franchisees will have to closely analyze their data collection needs and the applicable laws in their jurisdictions. One thing is certain: doing nothing invites trouble.

E. Special Industry Standards

There are several federal statutes regarding privacy that are unique to special industries. While a detailed analysis of these laws is beyond the scope of this paper, it is important to take note of them:

- The Bank Secrecy Act requires banks to retain records and create reports to help law enforcement investigations.

- The Fair Credit Reporting Act ("FCRA"), as amended by the Fair and Accurate Credit Transactions Act of 2003 ("FACTA"), covers consumer reporting agencies ("CRA") that prepare and distribute consumer reports, as well as individuals and companies that use or procure consumer reports from CRAs. The FCRA affects any company that obtains credit reports regarding applicants or employees; such credit reports should be "reasonably safeguarded." Willful noncompliance can result in liability for actual and punitive damages, costs, and attorneys’ fees under the FCRA. See 15 U.S.C. § 1681n. Negligent noncompliance can result in liability for actual damages, costs, and attorneys’ fees. See Id. § 1681o. Any officer or employee of a credit reporting agency who knowingly and willfully provides information concerning an individual from the agency’s files to a person not authorized to receive that information faces fines and/or imprisonment of up to two years, in addition to the penalties for willful non-compliance described above. Id. § 1681r.


• The Cable Communications Policy Act ("CCPA")\(^{141}\) requires these companies to notify subscribers about any collection and use of personal information. Cable companies cannot disclose subscriber viewing habits. A private right of action exists.

• Video Privacy Protection Act of 1988 ("VPPA")\(^{142}\) provides that video tape service providers cannot disclose customer video rental or purchase information.

• The Health Insurance Portability and Accountability Act ("HIPAA")\(^{143}\) protects the privacy of medical records. Regulations require, \textit{inter alia}, that consumers authorize all uses and disclosures of their health information that are not for treatment, payment, or healthcare operation (i.e., that are for marketing purposes). HIPAA covers physicians, hospitals, pharmacists, health insurers, as well as "business associates"—companies that provide services to physicians, hospitals, pharmacists, and health insurers. HIPAA also covers employers providing health care benefits to employees.

• The Gramm-Leach-Bliley Act ("GLBA")\(^{144}\) covers "financial institutions," defined to include "any institution the business of which is engaging in financial activities as described in Section 4(k) of the Bank Holding Company Act."\(^{145}\) Regulations interpreting GLBA provide exemplars of entities that would not qualify as financial institutions and entities that would so qualify, such as: real estate appraisers, car dealerships that lease cars, preparers of tax returns, and investment advisory companies.\(^{146}\) Under GLBA, if a financial institution wishes to share, or even sell, "non-public personal information" about its consumers with different branches or affiliates of the institution that are engaged in different services, the institution may do so only if it notifies consumers that it will be sharing this information. Several respected commentators have opined that a franchisor and its franchisees are not considered affiliates of each other.\(^{147}\) Furthermore, after notification, the consumer has no right to prevent the company from sharing information with the affiliates. However, should financial institutions desire to share or sell customer data with third parties that are non-affiliates of the company, consumers must be given a right to opt-out.\(^{148}\)

\(^{145}\) \textit{Id.} at § 6809.
\(^{146}\) See 16 C.F.R. § 313.3(k) (2007). Other examples of financial institutions include: mortgage companies (lenders or brokers), insurance companies, tax preparers, debt collectors, credit counseling services, financial advisors, tax planners, and auto dealers that either lease/finance automobiles.
\(^{148}\) See 15 U.S.C. § 6802(a), (b) (2007). The opt-out provisions of the GLBA were strongly criticized. \textit{See, e.g.}, Edward J. Janger & Paul M. Schwartz, \textit{The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules}, 86 Minn. L. Rev. 1219, 1230-32 (June 2002) – very few customers have opted out because privacy policies are hard to understand, and may be misleading; and opt-out rights are difficult and burdensome to exercise.
Telecommunication services are subject to the FCC’s recently issued Customer Proprietary Network Information (“CPNI”) Order, which is directed to increasing the security of consumer information in telecommunications services (i.e., cellular phones). The FCC has defined CPNI to include “information such as the phone numbers called by a consumer; the frequency, duration, and timing of such calls; and any services purchased by the consumer, such as call waiting.”\footnote{47 U.S.C. § 222(c)(1)(B). Implementation of the Telecommunications Act of 1996: Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information and Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, as amended, CC Docket Nos. 96-115 and 96-149, Second Report and Order and Further Notice of Proposed Rulemaking, 13 FCC Rcd 8061, 8120, ¶ 75 (1998) (CPNI Order).} It is possible that one of the larger carriers will try to appeal the new regulations. Comments were due on or before July 9, 2007, and replies are due on or before August 7, 2007.\footnote{72 Fed. Reg. 31948.} If the new regulations are approved in their entirety, carriers will have six months to come into compliance; smaller carriers may be given an additional six months to come into compliance.\footnote{In 2006, CPNI became a hot topic because of various websites on which cell phone bills were offered for sale by databrokers, not consumers (see attached Exhibit B - Definitions). In addition to media coverage of these websites, the Electronic Privacy Information Center petitioned the FCC to look again at the CPNI regulations. As a result, the FCC issued the April 2 Order which keeps certain current regulations (i.e., yearly compliance certificate), but adds new ones. Some of the new regulations are uncontroversial. For example, carriers would need to notify their consumers immediately regarding any password changes, online account or mailing address changes, and changes to the customer’s pre-selected answers to pre-selected identifying questions. The more controversial aspects include the following: First, the new regulations require a consumer’s opt-in consent before a carrier discloses CPNI to independent contractors or joint venture partners. This may not be enforceable given a 10th Circuit case, U.S. West, Inc. v. Fed. Communications Comm’n, 182 F.3d 1224, 1238-39 (1999), which found opt-in provisions under the original regulations unconstitutional; it was as a result of this case that the old regulations have an opt-out requirement rather than an opt-in requirement. Second, the new regulations have strict breach notification rules requiring that within seven days after “a reasonable determination of a breach,” a carrier must notify the U.S. Secret Service and the FBI regarding the breach. Generally, within seven days after that notification, the carrier may notify its consumers (there are some exceptions to this requirement). There is no definition for a “reasonable determination of a breach;” this term is left uncertain in its meaning. Furthermore, all breaches must be reported, regardless of whether information is taken. Third, a carrier can only release CPNI to a consumer if she provides the carrier with a pre-established password, the consumer asks that her CPNI be sent to her address of record, or the carrier calls the consumer’s telephone number of record to release her CPNI. Specifically, the April 2 Order prohibits carriers from using “readily available biographical information” (defined as the consumer’s Social Security Number or the last four digits thereof, mother’s maiden name, home address, birth date, etc.) or “account information” (i.e., account number, amount of last bill, telephone number of record) in order to verify the consumer’s identity and release CPNI. Thus, for quick or routine questions, it will be difficult for consumers to get a response unless they have a pre-established password that they remember. Report and Order and Further Notice of Proposed Rulemaking, 22 F.C.C.R 6927 (2007).} If the

F. International Laws

As U.S. franchisors do business in foreign countries, they must be aware of and abide by these countries’ laws regarding privacy.\footnote{See generally, Charles B. Cannon, What Franchisors Need to Know About Privacy Rights, a Safe Harbor, and Standard Contractual Clauses Before Exchanging Personal Information with Europeans, 22-WTR Franchise L.J. 176 (2003); Meredith Fuchs, Ronald L. Plesser & Michael Power, PRIVACY: U.S. AND INTERNATIONAL (A.B.A. Forum on Franchising 2002).} Although this paper will focus on Canada and the European Union (“EU”), there are many countries in Latin America (i.e., Argentina and Chile) and Asia (i.e., Japan and India), as well as Australia, that have privacy regulations in place or
are considering implementing such laws. These laws will affect any franchise system with franchisee(s) or company owned units in the subject countries—at least to the extent that the franchisor or franchisees need or want to move customer data across international borders. Any system that has or develops a centralized database for customer data may need to determine the extent to which it needs to comply with applicable international privacy laws. Just collecting certain information from individual customers and moving it across international boundaries may be subject to such laws—even without a franchised or other physical presence in that country.

1. The European Union

The EU Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (“Directive”) required EU member states to enact legislation to protect European consumers’ personal information as set forth in the Directive.153 Each EU member state now has its own data protection law. Although different, each country’s laws follow the Directive’s main principles:

- Personal data must be processed “fairly and lawfully”;

- Personal data must be processed only “for specified, explicit, and legitimate purposes and not further processed in a way incompatible with those purposes” unless the consumer consents to additional purposes;

- Personal data collected must be “adequate and relevant, and not excessive in relation to” the stated purposes;

- Personal data should be “accurate” and, if necessary for the stated purposes, “kept up-to-date”;

- Personal data should not be kept for longer than necessary;

- Personal data should be kept secure;

- Personal data should be processed in accordance with the individual’s rights under the applicable country’s laws; and,

- Personal data should not be transferred to countries that the EU has not recognized as having “adequate” protection laws unless specific steps are taken to ensure that the data will be “adequately protected.”

In addition, most EU member states require entities that process personal data to register processing activities with the country’s Data Protection Authority (“DPA”), and in some instances, to obtain the DPA’s express approval before undertaking certain types of processing activities (i.e., transferring data to a country without “adequate” protection laws). Most countries require or incentivize companies to designate a privacy officer.

Violating privacy laws may lead to civil penalties. In addition, some countries impose mandatory prison sentences. Personal data that has been collected, used and/or transferred in

violation of the privacy laws may be impounded or destroyed. Because of adverse publicity, violations may hurt a company’s branding or name value.

The EU member states, Iceland, Lichtenstein and Norway comprise the European Economic Area (“EEA”). Personal data may be transferred to any of these countries, as well as any other county which has privacy laws that the European Commission has deemed “adequate.” If a country has privacy laws which have not been deemed adequate, it is referred to as a third country. (The United States is a third country.) Personal data may be transferred to a third country outside the EEA only if the transfer falls under an “exception” under Chapter IV, art. 26(1) of the Directive—even if the transfers of data are within the same company. (Thus, a hotel corporation with databases in Europe and the US cannot transfer personal data from the European database to the U.S. unless such transfer falls under an exception.)

One option for a company that is transferring data between the EU and the U.S., is to follow the U.S. Safe Harbor Program (“Safe Harbor”). Under the Safe Harbor, a data processor in the U.S. may receive personal data from the EU if the data processor agrees to submit to restrictions insuring that the personal data is treated as if it is still subject to the Directive’s regulations (in other words, as if it had never left the EU). For a company to be eligible to receive personal data from the EU under the Safe Harbor, it must certify to the U.S. Department of Commerce that the company is in full compliance with the seven Safe Harbor Principles. A company must first establish and make public (i.e., post on its website) a privacy statement which expressly states that it follows the Safe Harbor Principles. It must also appoint a “data protection” contact person, establish a training program for its employees regarding the Safe Harbor Principles, implement a procedure whereby the company audits its compliance with the Safe Harbor Principles, and adopt an independent dispute resolution system. Once the privacy policy is made public, the FTC has the authority to ensure the company complies with its own policy.

Similar to agreeing to be part of the Safe Harbor, a company could enter into a “transborder data flow agreement” with the EU company. In this agreement, the US company would agree to protect the personal data by following the privacy principles under the Directive.

If a U.S. company does not wish to follow the Safe Harbor or Directive principles, it can still access, process and/or use personal data from the EU if: the European consumer has knowingly consented to the transfer; the transfer is of information which is available publicly (i.e., on a public register); or, the transfer is necessary (as opposed to convenient) for entering

154 The following are the Member States of the EU: Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, and United Kingdom.
156 The seven Safe Harbor Principles are: (1) notice must be given to European consumers regarding why a U.S. data processor will have access to their personal data; (2) European consumers must be allowed to opt-out; (3) agreeing to certain restrictions regarding further transferring the personal data to another “third country”; (4) agreeing to keep the personal data secure; (5) using the data only for the purposes disclosed, and keeping the data updated, if necessary for such use; (6) European consumers must be given the opportunity to access their personal data and to correct it, if need be; and, (7) European consumers must be given “affordable” procedures, such as dispute resolution, to enforce their rights under the safe harbor. Id. at Annex I.
or performing certain contracts, for reasons of public interest, to protect the “vital interests” of the consumer, or in connection with legal claims. 157

If none of the above exceptions apply, and if the company does not want to follow the Safe Harbor or Directive principles, the company has only one option left to comply with the EEA laws: binding corporate rules (“BCR”). 158

2. Canada

Canada has adopted the Personal Information Protection and Electronic Documents Act (“PIPEDA”) to protect personal information gathered by private businesses. PIPEDA applies to all provinces that do not have “substantially similar” statutes—only three Canadian provinces (Alberta, British Columbia and Quebec) have their own provincial statutes. PIPEDA consists of two parts; only Part I is relevant to the issues addressed in this paper. Canada is the first country outside of Europe that was considered “substantially similar” for purposes of the Directive, in other words, PIPEDA has been found to offer the same level of protection for consumers as the EU’s Data Protection Principles and the OECD Guidelines. 159 Although Canada and the EU offer an equal amount of protection, it may be easier for American companies to comply with the PIPEDA than the EU regulations, which require filings and governmental approvals that PIPEDA does not require.

PIPEDA has ten basic principles with which companies must comply in order to gather, use and/or disclose consumers’ personal information:

- **Identifying Purposes** The company must identify the purposes for which it is collecting personal information and so notify Canadians at or before the time of collection.

- **Consent** Before collection occurs, the individual must have given his or her informed consent. The consent is considered informed if the individual knows which entity is collecting the information, the type of information that is being collected, how the information will be used and to which entities the information will be disclosed. Individuals must be given the option to withdraw their consent at any time, as well as an opt out provision for non-essential uses of their personal information.

---

157 Id. at Annex IV.

158 Although BCRs sound good in theory, they have been lacking in practice according to several commentators. A BCR is an option for a multi-national company whereby the company adopts corporate rules that would govern the company’s entire enterprise and ensure that personal data would be safeguarded as it is moved within the company, from country to country. There are several problems with BCRs: (1) they are costly as it would require getting each EU country’s approval of the corporate rules; (2) unlike the transborder data flow agreements, there are no model BCRs that the European Commission has drafted and published as acceptable; (3) a company’s subsidiaries, affiliates, partners, subcontractors, etc. would all need to comply with the BCR; and, (4) owing to the lack of existing BCRs which have been approved by all member states, there are no test cases which would show what language should be used in a BCR. Although BCRs have been recognized as ideal for franchisors and franchisees who wish to operate on an international level, until they are more prevalent, they remain out of reach for most companies mainly because of their cost. Boschee, Epstein & Simonson, supra note 89, at 14-15 (2007).

159 Commission of the European Communities, Commission Decision 2002/2/EC, 2002 O.J. (L. 002) 13 (April 1, 2002). Other countries which have been found to offer “adequate” protection include Canada, Argentina, Switzerland, the Isle of Man and Guernsey.
• **Limiting Collection**  Information may not be collected by deception and a company may only collect information that is necessary for the pre-identified purposes.

• **Limiting Use, Disclosure and Retention**  The company must implement guidelines for both retention and destruction of information. The company may not collect information for purposes other than those which have been identified to the individual. The information should not be kept for longer than necessary for the pre-identified purposes.

• **Accuracy**  The company must ensure through “reasonable efforts” that the personal information is accurate and complete, and update the information if necessary for the pre-identified purpose.

• **Safeguards**  The company must safeguard the personal information through “security safeguards” that are appropriate given the nature of the information. Physical, organizational and technological measures are the types of safeguards the company should consider implementing.

• **Openness**  The company’s data policies and practices must be readily available for individuals (i.e., by posting on the company’s website) and must be comprehensible. The company must designate a person to act as a privacy liaison to whom individuals may go to with complaints or questions, and this person’s name or title and contact information must be included with the company’s data policies and practices.

• **Individual Access**  The company must allow the individual access to the type of personal information the company has about that individual, how that information has been used and for what purpose, to which entities the information has been given, and to challenge the accuracy and/or completeness of that information (and amend it, if necessary).

• **Challenging Compliance**  The company must implement a complaint process for individuals to submit complaints regarding the data practices and policies. The complaint process should also contain a method of resolving such complaints.

• **Accountability**  The company must choose a representative who will be accountable for the company’s compliance with PIPEDA. The company must implement policies and practices to give effect to the ten principles of PIPEDA.

Violations of the PIPEDA may include publication of the company’s violation (or requiring the company to post such a notice), awarding civil penalties, and, the potential of fines imposed on individuals within the company (i.e., directors, officers and/or employees).\(^\text{160}\)

A company may transfer personal information to other entities beyond Canada’s borders if the individual has given consent to do so, only for the purpose(s) to which the individual has consented, and only if a contract exists between the company and the non-Canadian entity which ensures a level of protection commensurate with that required under Canadian law. The company remains responsible for abiding by the PIPEDA principles when data is transferred to

another third party; this can be achieved by entering into a contract with the third party which covers the ten principles.

There is an inherent problem in the transfer of personal information from Canada to the U.S. Because PIPEDA allows the transfer of personal information if and only if the receiving entity ensures a level of protection comparable to that of the PIPEDA, this means that the U.S. receiving entity must contractually agree to the ten principles outlined above. However, the U.S. Patriot Act allows government agencies to obtain any individual's personal information that is in the custody of U.S. entities, without obtaining the individual's consent. Thus, several commentators have noted that because of the Patriot Act, U.S. companies may be forced to disclose Canadians' personal information in violation of the PIPEDA.161

G. What Does It All Mean?

1. Class Action Law Suits

Given that many of the privacy statutes provide for actual damages or a statutory award as a remedy, and given that the types of activities which would violate the statutes would be done across large groups of people, the privacy statutes provide a fertile ground for class actions.

For example, the TCPA provides for damages of $500 (or actual damages) for each violation. If a company is sending multiple unsolicited faxes (and the chances are high that if one unsolicited fax is being sent, there are hundreds or thousands of unsolicited faxes being sent), there exists a potential windfall for bringing a class action.

The situation is similar with many state laws. For example, the California Song-Beverly Credit Card Act allows consumers to sue retailers if they are asked for personal information such as an address or telephone number, in connection with a credit card sale. The penalty is $250 for the first violation and $1,000 for each subsequent violation, with no requirement that the consumer suffer any loss. Once again, by the very nature of the violation, it is most likely that the retailer will have made this error not once, but hundreds or thousands of times. As such, it is a profitable class action to bring as the burden is not very high for plaintiffs, and the potential liability is high.

Recently, FACTA has become a hot source of federal class actions. FACTA imposes liability on the entity that generates the receipt. If the franchisor's proprietary system generates the receipt, and the franchisee has limited, if any, ability to control what prints on it, presumably the franchisor would be the responsible party.

The first FACTA class actions were filed the day after the Act went into effect.162 Over 100 lawsuits seeking nationwide class action status have been filed in California federal courts, against companies such as In-N-Out Burger, El Pollo Loco, California Pizza Kitchen, IKEA and Costco. Plaintiffs' attorneys are requesting the full extent of damages for willful violations, and are pointing to the three year delay between FACTA's enactment and becoming effective as

161 Id. at 18-19 & n.19.
having given companies plenty of time to come into compliance. California and Pennsylvania are where most of these FACTA class actions are being filed because those two circuits (the 9th and 3rd Circuits, respectively) are the easiest in which to meet the burden for willfulness. In addition, a U.S. District Court in Central California has held that FACTA does provide for a private right of action for consumers.

Class actions have been filed under various other privacy laws, including class actions against: Ohio University, BJ’s Wholesale, Department of Veterans’ Affairs, Wells Fargo, and TJX Companies.

2. Problems Unique To The Franchisor/Franchisee Relationship

Given the various privacy statutes and the potential liability, it is important that franchisors carefully consider the implications of these new laws and how their system can best comply with those that apply.

In adopting privacy policies, franchisors should examine how information is gathered and shared by franchisees and the franchisor. The parties should carefully consider and frequently review what information each is collecting from customers in light of what they really need so as to avoid accumulation of unnecessary data. The policy should take into account how long each party needs to retain customer data and who is responsible for protecting it and for destroying unneeded data and how. Finally, a privacy policy should not be so limited as to prevent future revisions.

We suggest that franchisors and their franchisees who may be subject to privacy laws consider putting together a crisis management team and procedure appropriate to the franchise system so that they will be ready in case of a security breach—given the short amount of time companies have to respond if it happens. The parties may need to have a procedure in place well before a breach occurs so they can give the proper notices within the statutorily-required time restrictions. Another item worthy of advance planning might be how to address the public relations issues that follow such notices.

We believe that franchisors and franchisees have yet to see more than the proverbial tip of the iceberg as to the impact of privacy laws. In our view, the emerging privacy laws will impact many aspects of the franchisor-franchisee relationship, including affecting decisions as to who “owns” or has the right to access and use customer data, affecting decisions as to whether a certain compilation of customer data is a trade secret, and affecting decisions as to the enforceability of certain contractual provisions. Likewise, the steps that franchisors have taken to protect customer data as their trade secrets (or their property rights in customer data) will affect determinations as to who has what rights and obligations under various privacy laws. In some franchise systems, these issues may be insignificant; in others they may be major considerations. Franchisors in new systems should make carefully considered decisions as to the extent to which they should address all these issues. In existing systems, franchisors and

---

franchisees may have a unique opportunity to address how their system will comply—often dealing with the reality that, at the time they entered their contract no one anticipated such things. Both parties to franchise relationships have an interest in addressing these issues before they have to do it in response to governmental action or an image-damaging public event.

IV. CONCLUSION

In conclusion, franchise systems for which customer data has value are well advised to draft focused contract provisions and implement thoughtful policies and procedures to confirm and preserve desired ownership rights to the extent possible. Otherwise enforcement may not be available at times when needed. Even with a good contract, enforcement can be difficult if policies and practices have not been consistent with protecting the data. To be sure, not all systems will regard customer data as valuable, but all systems nonetheless face risks from ignoring the obligations and consequences from possessing such data, whether valuable or owned or not. One must consider the evolving laws protecting customers’ rights to privacy and security in non-public information about them. Although, as with ownership, the parties may address privacy issues by contract, they must also have thoughtful policies in place and implement and enforce those policies consistently. By doing so, they may reduce exposure to claims and adverse publicity under such laws. This is a rapidly evolving area of law and counsel ignores it at some peril.
Exhibit A – Status of State Adoption of Uniform Trade Secrets Act

1979 Uniform Act

Arkansas ARK. CODE ANN. § 4-75-601 (1981)
California CAL. CIV. CODE § 3426 (1985)
Indiana IND. CODE § 24-2-3-1 (1982)
Rhode Island R.I. GEN. LAWS § 6-41-1 (1986)

1985 Uniform Act

Alaska ALASKA STAT. § 45.50.910 (1988)
Arizona ARIZ. REV. STAT. § 44-401 (1990)
Colorado COLO. REV. STAT. § 7-74-101
Delaware DEL. CODE ANN. tit. 6, § 2001 1982 (Amended 1997)
Florida FLA. STAT. § 688.001 (1988)
Georgia GA. CODE ANN. § 10-10760 (1990)
Hawaii HAW. REV. STAT. § 482B-1 (1989)
Illinois 765 ILL. COMP. STAT. § 1065/1 (1988)
Iowa IOWA CODE § 550.1 (1990)
Kansas KAN. STAT. ANN. § 60-3320 (1981)
Kentucky KY. REV. STAT. § 365.88 (1990)
Maine ME. REV. STAT. ANN. tit. 10 § 1541 (1987)
Maryland MD. CODE ANN., COM. LAW § 11-1201 (1989)
Minnesota MINN. STAT. ANN. § 325C.01 (1981)
Mississippi MISS. CODE ANN. § 75-26-1 (1990)
Montana MONT. CODE ANN. § 30-14-401 (1985)
Nebraska NEB. REV. STAT. § 87-501 (1988)
Nevada NEV. REV. STAT. ANN. § 600A.010 (1987)
New Mexico N.M. STAT. ANN. § 57-3A-1 (1989)
Ohio OHIO REV. CODE ANN. § 1333.61 (1994)
Oklahoma OKLA. STAT. ANN. tit 78, § 85 (1986)
Oregon OR. REV. STAT. § 646.461 (1988)
South Dakota S.D. CODIFIED LAWS § 37-29-1 (1988)
<table>
<thead>
<tr>
<th>State</th>
<th>Statute Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>U.S. Virgin Islands</td>
<td>V.I. CODE tit. 11, § 1001 (2005)</td>
</tr>
<tr>
<td>Vermont</td>
<td>VT. STAT. ANN. tit. 143 § 4601 (1996)</td>
</tr>
<tr>
<td>West Virginia</td>
<td>W. VA. CODE § 47-22-1 (1986)</td>
</tr>
<tr>
<td>Wisconsin</td>
<td>WIS. STAT. § 134.90 (1986)</td>
</tr>
</tbody>
</table>

The following states have statutes protecting trade secrets but have not adopted the UTSA:

<table>
<thead>
<tr>
<th>State</th>
<th>Statute Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Massachusetts</td>
<td>MASS. GEN. LAWS ANN. ch. 93 § 42 (1969, Amended 1983)</td>
</tr>
</tbody>
</table>
Exhibit B – Definitions

**Botnets**: Networks of hijacked personal computers used by spammers to conceal their identities while spammers send spam and viruses.

**Bugs**: The use of electronic devices for electronic eavesdropping.

**Click Stream Data**: When a person visits a website, the website can record information about the person and how the person navigates the website.

**Cookie**: Small files stored on a user’s hard drive by the user’s web browser such as Internet Explorer or Netscape. Cookies are created at the request of a website, unless the user has disabled that function in his or her browser. A website can only access its own cookies or those of an affiliated website. Cookies allow websites to “remember” facts about a visitor, such as a login ID and password, as a visitor browses through a site. Without cookies, users would be forced to login anew at every page visited at a secure website. Cookies also enable websites to track the browsing habits of viewers. Each cookie is assigned a number, and a site, by requesting the cookie’s identification number each time a page is loaded, can monitor which links a particular user is following. Advertising vendors also use cookies to target advertisements to particular users based on their browsing history.

**Databrokers**: website operators who obtain unauthorized access to CPNI in order to later sell CPNI. Often obtain unauthorized access through false pretenses, either deceive the telecommunications service’s representative into disclosing CPNI or establish fraudulent online accounts. These false pretenses are often referred to as “pretexting.”

**Keylogger**: A program which records the keystrokes and sometimes the mouse-clicks entered by a computer user. Most such programs then transmit the recorded keystrokes to a predetermined location. Keyloggers are often used by hackers to obtain victims’ passwords and account information in order to illegally access those accounts.

**Screen Capture**: A program which may capture, store, and transmit the images displayed on a computer screen every few seconds, in order to monitor the emails and websites viewed by the user. By collecting and reviewing such images in sequence, a third party may be able to ascertain what websites a person is visiting and what emails or instant message they are sending or receiving.

**Spam**: Unsolicited emails, typically sent by online marketers in mass quantities for advertising programs. Spam has also been linked with fraudulent business schemes, chain letters, and offensive sexual and political messages. The problems associated with Spam range from the inconvenience and annoyance they cause to email users, to damage to the hardware and networks that make up the internet. Often clogs available bandwidth.

**Spyware**: Software that can track or collect the online activities of personal information of internet users, change setting on users’ computers, to cause advertising messages to pop up on users’ computer screens. Internet users are often unaware that Spyware has been downloaded into their computers. Spyware was designed to be extremely difficult to remove.

**Web Bug**: Another information collection device, secretly uses pixel tags to gather data about the user.
BIOGRAPHICAL SKETCHES

Robert L. Ebe is a litigation partner in the San Francisco office of Bingham McCutchen LLP. He has litigated on behalf of clients in many industries in franchise and distribution-related disputes for over thirty years, and is a co-chair of Bingham McCutchen’s Distribution and Franchise Practice.
Howard E. Bundy has been a member of the Forum for 21 years. He is a principal and founder of Bundy & Morrill, Inc., P.S. of Seattle, Washington. He practices almost exclusively in the area of franchise law, representing franchisees in dispute resolution and representing franchisors in transactional practice, including drafting agreements and disclosure documents and handling registrations. He drinks coffee in the rain.
Robert L. Ebe is a litigation partner in the San Francisco office of Bingham McCutchen LLP. He is a co-chair of the firm’s Distribution and Franchise Practice. Bob is listed as a business litigation “Super Lawyer” in *Law & Politics* and *San Francisco* magazines. He has litigated on behalf of clients in many industries in franchise and distribution-related disputes for over thirty years. Bob is a past co-chair of the California State Bar Business Section’s Franchise Law Committee, and member of that section’s Executive Committee. Bob also serves as a neutral arbitrator for the Large, Complex Commercial dispute panel of the American Arbitration Association, and is on the neutral arbitration panel of the CPR Institute for Conflict Prevention & Resolution and a member of its franchise mediation panel.

Bob received his B.A. with distinction from DePauw University in 1973 and his J.D. *cum laude* from the University of Chicago Law School in 1976, where he was an associate editor of the *Law Review* and a member of Order of the Coif.

Bob is an avid long distance cyclist, fly fisherman, backpacker and skier.
HOWARD E. BUNDY

Howard E. Bundy is a founder and principal of Bundy & Morrill, Inc., P.S., a Seattle, Washington firm that practices primarily in the area of franchise law. Howard represents franchisees in dispute resolution and represents franchisors in drafting franchise agreements and disclosure documents and in franchise registration matters. He has been practicing primarily in the area of franchise law since 1981.

Mr. Bundy has been a member of the ABA Forum on Franchising since 1986. He is a member of the Solo and Small Firm Group of the Forum. Since 1995 he has served as a member of the Advisory Committee to the Franchise & Business Opportunities Working Group of the North American Securities Administrators Association. Howard has recently presented at a CLE on franchising in Seattle and has previously presented at the ABA Forum on Franchising.

Howard received his J.D. from the University of Puget Sound Law School (now Seattle University Law School) in 1981, after serving as Lead Articles Editor of the University of Puget Sound Law Review. He is admitted to practice in the State of Washington and before several federal courts.