American Bar Association
27th Annual Forum on Franchising

PRIVACY ISSUES THAT AFFECT FRANCHISING

Paul D. Jones
Barrister, Solicitor & Trade-mark Agent
Toronto, Canada

and

David W. Koch
Wiley Rein & Fielding LLP
Washington, D.C.

October 6-8, 2004
The Sheraton Wall Centre Hotel
Vancouver, British Columbia

I. INTRODUCTION

Privacy law compliance is a potential concern for almost any business these days. Businesses that collect personal information from individuals must comply with applicable data protection rules. Businesses that use telemarketing, "broadcast" faxes, email, or "spyware" to promote goods and services now face a panoply of privacy rules (and proposed rules) specific to each marketing channel.

Franchisors collect data and use these marketing techniques. Franchisees collect data and use these marketing techniques. Each confronts the privacy challenges and risks that go along with such activities, like any other business.

But franchising adds another level of complexity. Two fundamental aspects of franchising complicate privacy issues for both franchisors and franchisees. First, the businesses in a franchise network are united by a common brand, and it is usually the brand by which the public knows them. There is a possible disconnect between consumers' expectations of uniform privacy practices across the brand and the actual privacy practices of the independent businesses in the network, which may vary.

Second, franchisors and franchisees constantly share information with each other about the business. Thus, franchising implies a continuous series of data transfers between non-affiliated (in the ownership/corporate control sense) entities. Such data transfers are more sensitive than data transfers between offices of a single entity or even between offices of affiliates. Of course, most companies have business partners of some kind (vendors, strategic alliance partners, etc.) with whom they wish to exchange data, but franchise networks entail a higher order of day-to-day integration, collaboration, and communication.

This paper tackles a huge and fast-changing subject. Part II provides context by setting out basic principles of privacy. Part III identifies emerging privacy issues for franchising, as a lead-in to substantive discussion of current privacy laws in the U.S.A. (Part IV) and in the rest of the world (Part V). (Note: Part IV focuses mostly on *federal* law, which is a big enough subject by itself. Practitioners should check for, and will often find, analogous legal developments at the state level.) Finally, Part VI explores possible strategies for franchise networks to address compliance concerns.

II. WHAT IS PRIVACY LAW?

Privacy is notoriously difficult to define. Is it the right to be let alone? Or is it the right to control information about you? To go even further, do you own your personal information or just control it? There are a range of possibilities suggested by these questions, but can these questions even be answered without knowing the context in which they are asked? For example, does Osama bin Laden have a right to be left alone? Obviously not – security concerns must be balanced against privacy concerns. Does Mr. bin Laden have the right to control the commercialization of his image? That is a more difficult question. Generally, even persons convicted of a crime retain some rights with respect to their person, some right to their identity.

In a commercial context, what rights do individuals have to be let alone, free from unwanted mail, or telephone calls, or e-mails? This question balances commercial rights, sometimes described as "commercial speech," against individual preferences. If privacy is the right to be left alone, then presumably individuals have the right to refuse to receive commercial speech.

The marketer would still be free to retain the individual's file in the database for some other type of approach, or perhaps an approach by a different person, but if privacy is the right to control information about an individual, then the individual can insist that her file be deleted from the marketer's database, or made anonymous. And finally, if the individual owns her personal information, even anonymous information derived from the individual's personal information must be deleted on request.

On a practical level, the challenge is for the law to find the appropriate balance between privacy and other important societal policies such as defense and security, freedom of speech, a competitive marketplace, and respect for the rights of others. Privacy law is an evolving concept. Prosser classified four basic kinds of privacy rights[1]:

1. Unreasonable intrusion upon the seclusion of another, such as tapping a telephone. This is clearly "the right to be let alone."

2. Appropriation of a person's name or likeness. This is sometimes known as the right of publicity, but a distinction is sometimes drawn between the right of publicity, said to protect against unauthorized commercial exploitation, and privacy that protects against injury to personal feelings.

3. Publication of private facts.

4. Publication that places an individual in a false light, similar to defamation, but broader, in that the facts may be true, but manipulated to create the false impression.

Others have developed much more prosaic classifications of privacy. For example:

- Privacy of the person - protection from body searches and tests.

- Territorial privacy – protection of homes and property.

- Communications privacy – protection of what we say to others.

- Privacy of personal information – protection of what is known about us.

It is this later category, the privacy of personal information (sometimes known as "data protection"), that has become the subject of so much recent concern. The dramatic rise of e-commerce and the Internet, and the increased use of computers, have transformed concepts of customer goodwill. Previously, the customer goodwill attached to a brand was often intangible, something that could only be estimated based on sales. Now, depending somewhat on the product, brand managers can more easily develop methods to build customer databases and focus their efforts on improving the relationship with targeted customers. Customers are not as anonymous as they once were.

[1] *Restatement (Second) of Torts* §§ 652A-652I.

While these possibilities have delighted marketing professionals, the same factors have contributed to heightened awareness and concerns amongst individuals worldwide regarding the information collected about them and its use. As will be discussed later, these concerns first found expression in laws in the German state of Hesse, in Sweden and in France. By 1980 the concerns were general enough that the OECD issued its now famous Guidelines.[2] The Guidelines identified what it called the "Basic Principles of National Application." These are:

> *Collection Limitation Principle.* There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
>
> *Data Quality Principle.* Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
>
> *Purpose Specification Principle.* The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
>
> *Use Limitation Principle.* Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except: (a) with the consent of the data subject; or (b) by the authority of law.
>
> *Security Safeguards Principle.* Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.
>
> *Openness Principle.* There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
>
> *Individual Participation Principle.* An individual should have the right: (a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; (b) to have communicated to him, data relating to him (1) within a reasonable time; (2) at a charge, if any, that is not excessive; (3) in a reasonable manner; and (4) in a form that is readily intelligible to him; (c) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and (d) to challenge data

[2] "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," Recommendation of the Council of the Organization of Economic Co-operation and Development adopted on September 23, 1980. Available on-line at *http://www.oecd.org/dsti/sti/it/seur/prod/PRIV-EN.HIM*.

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

Accountability Principle. A data controller should be accountable for complying with measures which give effect to the principles stated above.

These principles have been succinctly summarized by the Federal Trade Commission for use in an American context as "Notice, Choice, Access and Security."[3] In other words:

1. Individuals must be given notice of the proposed collection, including use and disclosure, of personal information, and the specific purposes for such activity.

2. In order for the data to be collected, used or disclosed, appropriate consent must be obtained with respect to the specified purposes.

3. The data collected must be protected by appropriate security.

4. The individual must have access to the data collected, and to details of its use and disclosure.

Informational privacy legislation, as is being discussed in this paper, is based on what might be called a "contract" model. An offer is made to an individual to collect, use or disclose the individual's personal information for a specified purpose. The individual has the choice of agreeing or declining. In this way individuals have the option of defining privacy in their own way, to their own particular sensitivity.

As with contracts, problems have developed with the nature of the consumer's understanding of the contract that is being proposed, the meaning of some of the terms, and the balancing of interests or fairness of the contract or consent. In traditional contract law these are often referred to as problems of "unconscionability" or "good faith." Thus significant variations are developing between jurisdictions with respect to the limitations or restrictions that they impose on privacy contracts.

For example, as will be discussed later in this paper, a number of European jurisdictions prescribe various types of personal information that must be considered sensitive, and either require more explicit consent, or prohibit collection of such personal information altogether. In Canada the federal privacy law requires that organizations collect, use and disclose personal information "…only for purposes that a reasonable person would consider appropriate in the circumstances."[4]

On the other hand, in the United States under the Gramm-Leach-Bliley Act regarding financial institutions, there is no such limitation, and marketers are free to seek the consent of the individual for the collection of their personal information for any purpose that they choose. This

[3] In a Canadian context the words would be "Purpose, Consent, Access and Safeguards." "Notice" and "Choice" are very similar to "Purpose" and "Consent", but they are not the same.

[4] Section 5(3) of Canada's Personal Information Protection and Electronic Documents Act.

has resulted in what some might see as abuses. One bank said that it would make two kinds of disclosures. The first was to "Financial Service Providers." The second was to "Non-financial Service Providers." Another had a list of categories of organizations with which it would share information. The final category was "Other." [5]

Several of the other principles identified could be explained as the state prescribing certain basic terms to the contract, such as an obligation to keep the personal information secure, to grant the individual access to her own file, to disseminate basic information about the relationship, in order to correct market failures in the negotiation of the contract.

Another common problem with consumer contracts is that they are seldom read, and even less often fully understood. So it is with privacy policies. The question then arises as to what may be inferred in such situations. Did the individual consent to the 'contract' or not? For a marketer who sends out mass mailings of a flyer with a privacy notice on the back, the choice of presumptions is critical. If the individual is required to opt-in to further mailings, say by ticking a box and mailing back the notice, failing which the individual's name and address must be deleted from the marketer's mail list, then the marketer will probably lose most of the names on the list. On the other hand, a presumption that failure to respond implies consent, known as "opt-out", is open to considerable abuse in certain circumstances. Consider the example provided earlier from certain banks. Was that even a real choice?

In some jurisdictions the solution to this conundrum is to vary the nature of the permitted consent with the sensitivity of the information and its proposed use or disclosure in the context of the material facts of the transaction. This approach was discussed in the "Detailed Comments" to the OECD Guidelines,[6] but it is not an approach that is easily reduced to specific rules. While some jurisdictions have tried to define the concept of "sensitivity" with respect to personal information, others have left it to the courts to determine on the facts of each particular case.

Such vagueness is not necessarily such a bad thing. While businesses are concerned that some of their practices may fall into a grey area with respect to compliance, an individual is also less likely to commence a costly court action if the chances of winning are less certain. While the consumer may complain, the most appropriate and cost-effective dispute resolution procedure for both parties in these circumstances is negotiation and mediation. And this is in fact what many privacy commissioners do.

Such a solution, however, does not produce a very bright-line test that gives the certainty so often desired by clients. But outside of the United States that tends to be how privacy law is structured. The practice of privacy law may well require the development of the ability to judge what, for example is sensitive personal information, without the aid of specific rules.

[5] John Swartz, *Privacy Policy Notices Are Called Too Common and Too Confusing*, New York Times, May 7, 2001.

[6] See Paragraph 45.

III. EMERGING ISSUES FOR FRANCHISING

Some of the emerging privacy questions for franchising have been identified in past ABA Forum materials.[7] But those questions still have few answers, and new questions have been added. For example:

Who owns the customer list? If the franchisor asserts ownership, is the franchisor also assuming responsibility for proper use of the information and for its security, wherever it resides within the network? For providing consumers access to their information?

Can the information in the customer list be transferred between franchisor and franchisee (or among franchisees) without the consent of the individuals involved? If not, who is responsible for obtaining the consent?

Is information collected from prospective franchisees "personal information" to which the privacy laws apply, or is it business information? And for existing franchisees?

What form of privacy notice to consumers should appear on a franchisor's website? Should the notice differ depending on whether franchisees (a) operate independent websites, or (b) are given a page on the franchisor's website?

Are the new Do Not Call, Do Not Fax, and Do Not Email rules going to limit systemwide communications from franchisor to franchisees?

If a franchisor performs centralized marketing services for franchisees, either for a fee or using common marketing funds, does compliance with applicable telemarketing, unsolicited fax, and commerical email rules reach back to the franchisees for whom the service is performed?

Is there a legitimate risk of franchisor vicarious liability for a franchisee's privacy violations (or vice versa)? Does it depend on whether the franchisor has the right to control privacy practices for the system? On whether the franchisor actually exercises control?

Might government enforcers look to franchisors in enforcing privacy standards against franchisees? Franchisors have had that experience in other areas.[8]

The analysis of at least some of these questions will differ depending on where the franchise network operates. The following sections set in stark contrast the "sectoral" approach of U.S. privacy law (Part IV) versus the "general principles" approach dominant in the rest of the world (Part V).

---

[7] See David W. Koch & Meredith Fuchs, *Online Privacy 101: A Franchisor Survival Guide*, FRANCHISE LAW JOURNAL, vol. 19, no. 2 (ABA Fall 1999); *Essentials of E-Commerce*, 24th Annual Forum on Franchising (ABA Oct. 10-12, 2001) at 66.

[8] For example, the U.S. Department of Justice sought to hold a franchisor liable for its franchisee's failure to comply with the Americans With Disabilities Act – another area of high public sensitivity and active government enforcement. The United States Court of Appeals for the Eighth Circuit upheld the government's position. *United States v. Days Inns of America, Inc.*, 151 F.3d 822 (8th Cir.), *cert. denied*, 119 S. Ct. 1249 (1999).

IV. PRIVACY LAWS IN THE USA

In the U.S.A., the term "privacy law" is about as imprecise as "franchise law." One reason for the lack of precision is that the "privacy" label has long been applied to both distinct prongs of privacy – one being the collection and use of personal information, and the other what is colloquially termed "the right to be let alone."

Until recent decades, the "law of privacy" principally referred to common law causes of action for invasion of privacy and to U.S. Supreme Court decisions exploring implied rights of privacy under the federal Constitution (e.g., the *Roe v. Wade* decision) or interpreting the Fourth Amendment guarantee of the right of the people to be secure in their persons, houses, papers and effects against unreasonable searches and seizures. But starting in about 1970 – coinciding with a vast expansion in data collection under government social programs, the rise of credit cards, and the beginnings of computer networks – concerns about disclosure and use of personal data became a legislative issue. Congress enacted the Fair Credit Reporting Act of 1970[9] to force open credit bureau practices and to limit disclosure of their data; enacted the Privacy Act of 1974 to limit federal agencies' handling of personal information; and amended the federal wiretapping statute repeatedly to guard telephone calls and other forms of electronic communication from interception. States enacted similar laws to protect consumer credit reports, government records, and electonic communications, though a few states went further, adding express rights of privacy to their state constitutions or recognizing such rights by statute.[10]

In the 1990s, the explosion of telemarketing started a new round of "privacy" legislation, including the Telephone Consumer Protection Act of 1991 (requiring telemarketers to check their "don't call" list before making calls) and the Telemarketing and Consumer Fraud and Abuse Prevention Act of 1994 (requiring telemarketers to identify themselves, restricting calling hours, and prohibiting calls to persons who have asked not to receive them).

But the emergence of the Internet shifted public concern to the "data protection" prong of privacy. In 1998, Congress enacted the Children's Online Privacy Protection Act to regulate how website operators collect and use personal information from children under age 13. The following year, Congress passed the Gramm-Leach-Bliley Act, which restricted the ability of "financial institutions" to disclose non-public personal information about consumers to non-affiliated third parties.[11] And pursuant to the Health Insurance Portability and Accountability

---

[9] 15 U.S.C. §§ 1681-1681(u).

[10] *E.g.*, Mass. Gen. Laws Ann. ch. 214 § 1B ("A person shall have a right against unreasonable, substantial or serious interference with his privacy").

[11] 15 U.S.C. §§ 6801-6809 (also known as the Financial Services Modernization Act). The Act's privacy provisions apply both online and off, and apply broadly to any company engaged in financial services with consumers, not just entities traditionally thought of as financial institutions. Initial concern in the franchise community about Gramm-Leach-Bliley seems to have faded as it became clear that few franchisors would come within the definition of a "financial institution." Accordingly, this paper does not discuss Gramm-Leach-Bliley requirements. However, Forum members may be relieved to know that on April 30, 2004, the federal disctrict court in Washington , D.C. granted summary judgment against the FTC in actions brought by the New York Bar Association and the American Bar Association, concluding, as a matter of law, that "Congress did not intend for the G-L-B's privacy provisions to apply to attorneys who provide legal services in the fields of real estate settlement, tax-planning and tax preparation." Judge Walton "declared and decreed" that the FTC's decision to assert jurisdiction over lawyers was "beyond the

Act,[12] when Congress failed to legislate standards for protection of individually-identifiable health information by August 21, 1999, the Department of Health & Human Services was charged with commencing a rulemaking to set such standards.

Meanwhile, the Federal Trade Commission took the lead among federal agencies in studying broader online privacy issues.[13] In reports to Congress in 1998 and 1999,[14] the FTC articulated a set of "Fair Information Practices" while urging lawmakers to refrain from legislating in order to give the private sector a chance to address public concerns. In a 2000 report, a divided FTC reversed its position, concluding that the market response to online privacy concerns had been inadequate.[15] However, there is still no generally-applicable federal law setting standards for

---

FTC's statutory authority" and "an arbitrary and capricious agency action." Judge Walton's April 30, 2004 ruling relied primarily on his August 11, 2003 opinion denying the FTC's motions to dismiss. *New York State Bar Ass'n v. FTC*, 276 F.Supp.2d 110 (D.D.C. 2003).

[12] 42 U.S.C. § 1306. HIPAA is, for the most part, specific to health care providers and insurers, and too far afield from franchising for analysis in this paper. However, it is worth noting that the statute also imposes certain obligations on all employers that sponsor employee health plans.

[13] For a history of the FTC's early role in online privacy, see David W. Koch & Meredith Fuchs, *Online Privacy 101: A Franchisor Survival Guide*, supra n. 7.

[14] *Online Privacy: A Report To Congress* (FTC June 1998); *Self Regulation And Privacy Online: A Report To Congress* (FTC July 1999). According to the 1998 report, the FTC synthesized these "widely accepted" principles from government studies in the U.S., Canada, and Europe dating as far back as 1973. The "Fair Information Practices" principles are:

Notice/Awareness. Consumers should be given notice of a franchisor's online information practices so that the consumer can make an informed decision about disclosing their personal information. The notice should identify who is collecting the data, the uses to which it will be put, others with whom it may be shared, the nature of the data collected, the means of collection (if not obvious to the consumer), the consequences of refusing to provide data, and the data collector's measures to ensure security and quality of the data.

Choice/Consent. Consumers should have a choice as to the use and dissemination of information collected from or about them. In practice, the choice has usually been presented as "opt in" (requiring affirmative steps by the consumer to allow collection and use) or "opt out" (requiring affirmative steps by the consumer to prevent collection and use), but other variations are possible.

Access/Participation. Consumers should have access to the information collected about them and a practical means to contest its accuracy and completeness.

Integrity/Security. Data collectors should take adequate steps to ensure the security and integrity of the information they collect. These steps may include cross-checking information against other sources and encrypting data or using passwords to prevent unauthorized access.

Enforcement/Redress. Consumers should have a mechanism to ensure compliance with the substantive principles and recourse for failure to comply. The mechanism could be external regulation (private rights of action and/or government enforcement) or self-regulatory regimes, including external compliance audits, third-party certification programs, and conditioning association membership on compliance with a code of Fair Information Practices.

[15] *Privacy Online: Fair Information Practices in the Electronic Marketplace – A Report to Congress* (FTC May 22, 2000).

online privacy (see Section IV.D below). Nor has the FTC asserted that a failure to adopt or follow the Fair Information Practices, in and of itself, is a violation of the Federal Trade Commission Act – the Fair Information Practices essentially constitute a voluntary standard. On the other hand, FTC officials have stated publicly that the Commission will apply the same standards to both online and offline privacy practices.[16]

As the foregoing introduction demonstrates, any snapshot of the "law of privacy" in the USA is doomed to fade quickly. The "privacy" label continuously sweeps in new areas, both online and off, at both the federal and state levels, and in the private sector. And as new areas of privacy concern emerge, the FTC continues its practice, begun in the 1990s, of holding public workshops to study them.[17]

In the last two or three years, priority seems to have shifted back to the "right to be left alone" prong of privacy. Franchise systems, no less than other businesses, must understand a new set of "Do Not" rules and determine whether those rules apply to their business activities. In the following sections, this paper reviews the legal developments in privacy that have attracted the greatest concern and publicity in the last two years or so. Again, please note: Part IV focuses mostly on *federal* law, and does not attempt to survey legal developments at the state level.

A. Do Not Call

On January 29, 2003, the FTC amended its Telemarketing Sales Rule (TSR),[18] the trade regulation rule implementing the Telemarketing and Consumer Fraud and Abuse Prevention Act.[19] Among the changes to the TSR, one stood out: the creation of a National Do Not Call (DNC) Registry. The original TSR, issued in 1995, prohibited telemarketers from calling consumers who had asked to be removed from that telemarketers' call list. But entity-specific do-not-call lists did not satisfy the public demand for relief from intrusive telemarketing calls.

The Federal Communications Commission (FCC) enforces the Telephone Consumer Protection Act (TCPA),[20] which also regulates telemarketing. The FTC has no authority over intrastate solicitation calls, nor over telemarketers exempt from FTC jurisdiction, such as common carriers, most financial services providers, insurance companies and some non-profit organizations, if these entities conduct their telemarketing in-house. However, FCC rules cover telemarketers and intrastate calls that are not subject to FTC enforcement.[21] Together, the FTC

[16] The FTC's web site provides comprehensive information on the Commission's privacy initiatives. See *http://www.ftc.gov/privacy/index.html*. The website also offers a number of guides to help businesses comply with privacy-related regulations, such as restrictions on telemarketing.

[17] For example, on April 19, 2004, the FTC held a workshop on "spyware" (discussed in Section IV.E below), and on June 21, 2004, a separate workshop on radio frequency identification (RFID) technology (not discussed in this paper).

[18] 16 C.F.R. Part 310.

[19] 15 U.S.C. § 6101 *et seq*.

[20] 47 U.S.C. § 227.

[21] 47 C.F.R. § 64.1200.

and the FCC have jurisdiction over nearly all telemarketing calls placed to U.S. consumers, and the TSR and the TCPA regulations apply similar rules.

The national DNC program had a bumpy start, despite its overwhelming popularity. In September 2003, a federal district court enjoined the FTC from enforcing its DNC rules after determining that the rules violate commercial free-speech rights.[22] Consequently, the FTC shut down access to the DNC registry before the program's anticipated launch on October 1, 2003. But on October 7, the U.S. Appeals Court for the Tenth Circuit granted the FTC's request to stay the injunction, thereby allowing the DNC program to go into effect pending resolution of the legal challenges by telemarketers. Meanwhile, in order to foreclose the argument made in the district court that the FTC had exceeded its statutory authority in creating the DNC program, Congress passed a bill ratifying the FTC's actions.[23]

Although the FTC was briefly enjoined, the FCC began enforcing its DNC rules as scheduled on October 1. The FCC required telemarketers that had already downloaded the national DNC registry (before the FTC blocked access) not to call numbers appearing on their copies of the list. On October 17, when the FTC rules also came into effect, all telemarketers came under an obligation (1) to download applicable portions of the national DNC list; (2) not to call registered phone numbers unless an exception applies; and (3) to re-access the registry at least every three months.[24]

On February 17, 2004, the U.S. Court of Appeals for the Tenth Circuit upheld the DNC program in four consolidated cases.[25] The Court held that: (1) the Do Not Call Registry is a valid commercial speech regulation, because it directly advances substantial governmental interests and is narrowly tailored; (2) the fees that telemarketers must pay to access the list are a permissible measure designed to defray the cost of legitimate government regulation; (3) it was not arbitrary and capricious for the FCC to adopt an "established business relationship" exception; and (4) the FTC has statutory authority to establish and implement the national Do Not Call Registry.

Telemarketers must use the national DNC Registry to "scrub" their calling lists of numbers that have been registered. Telemarketers may register to access the national DNC list and download the list in a variety of data formats at an FTC-managed website.[26] Consumers' phone numbers are organized by area code, and a telemarketer pays an annual fee based on the number of area codes it wishes to access ($25 per area code, up to $7,375). There is no fee to access five or fewer area codes.

---

[22] *U.S. Security v. FTC*, 282 F.Supp.2d 1285 (W.D. Okla. 2003), *rev'd sub nom Mainstream Marketing Services, Inc. v. FTC*, 358 F.3d 1228 (10th Cir. 2004).

[23] Pub. L. 108-82 (2003).

[24] Beginning January 1, 2005, telemarketers must download the national DNC Registry every month rather than every three months. The FTC changed this rule In response to a March 2004 Congressional mandate. The FCC has proposed a similar change and is on track to complete its parallel rulemaking well before January 2005.

[25] *Mainstream Marketing Services, Inc. v. FTC*, 358 F.3d 1228 (10th Cir. 2004).

[26] The website is *http://telemarketing.donotcall.gov*. In addition, the entity-specific do-not-call provisions of the TSR remain in effect.

The DNC rules provide an "established business relationship" exception for calls to existing or former customers. The "existing business relationship" exception allows a company "to contact a customer for 18 months after a business transaction and three months after an inquiry or application." The rules also provide an "explicit permission" exception, but it requires the consumer's express, written permission, including signature and telephone number.

The DNC rules apply only to outbound calls, not inbound calls from consumers. In addition, these rules apply only to business-to-consumer telemarketing calls, not to business-to-business calls (unless the calls are for the sale of non-durable office or cleaning supplies). Sole proprietors are "businesses," not consumers, if the individual running the business is working outside the home, and the federal Do-Not-Call rules do not apply when calling these persons. Nonetheless, the FCC DNC rules may effectively apply to home businesses, because these businesses technically are "residential telephone subscribers" and indistinguishable from other residential lines.

B. Do Not Fax

Since 1992, as directed by the Telephone Consumer Protection Act of 1991, the FCC has banned faxing "unsolicited ads," defined broadly to cover any material advertising the commercial availability or quality of any property, goods or services.[27] The FCC's ban on fax ads applies regardless of whether the sender or recipient of a fax is an individual, business or non-profit organization. In addition to federal and state agency enforcement, a private suit can be brought against a violator, in which the recipient can recover the actual monetary loss that resulted from the TCPA violation or up to $500 per violation, whichever is greater. The court may triple the damages for each violation if it finds that the defendant willingly or knowingly committed the violation.[28]

Since the mid-1990s, the rule against unsolicited ad faxes has had two exceptions: (1) senders could transmit faxes to recipients with whom they had an existing business relationship (EBR); and (2) senders could transmit faxes to recipients from whom they had received a "prior express invitation or permission." In July 2003, the FCC proposed to eliminate the EBR exception, which is based on the FCC's interpretation of the TCPA, but is not actually written into the statute. The FCC also proposed to stiffen the requirements for the express consent exception.

A fierce outcry ensued from businesses and non-profits, who contended that legitimate and well-established exchanges would be disrupted under the new rule. To avoid sanctions under the new system envisioned by the FCC, senders would have to obtain prior written permission from every recipient on their fax lists, including recipients' signatures and the specific fax numbers to be used. In response to the criticism, the FCC temporarily reverted to the old rule by reinstating the EBR and the less-restrictive consent exceptions until January 1, 2005.

Under the proposed new rules, beginning January 1, 2005:

- It would be unlawful to send an unsolicited advertisement to a facsimile machine without the prior written permission of the recipient of the advertisement;

[27] 47 C.F.R. § 64.1200(a)(3).

[28] See *http://www.fcc.gov/cgb/consumerfacts/unwantedfaxes.html*.

- The business or entity on whose behalf the fax is being sent must identify itself in the top or bottom margin of each page or on the first page of the fax message, and must include its telephone number and the date and time the fax is sent;

- If a facsimile broadcaster (the person or entity transmitting messages to a fax machine on another person's behalf) demonstrates a "high degree of involvement" in the sender's facsimile messages, such as supplying the facsimile numbers to which a message is sent, the facsimile broadcaster must provide its name on the fax;

- A facsimile broadcaster may be liable if it supplies facsimile numbers to a business or entity sending unlawful fax advertisements; and

- Faxes sent to fax servers and personal computers are covered by the faxing rules.

A bill pending in Congress would block some of the FCC's changes from taking effect. H.R. 4600, the proposed "Junk Fax Prevention Act of 2004," would amend the TCPA to add an EBR exception, but with a requirement that unsolicited faxes sent under the EBR exception contain a conspicuous notice and mechanism for the recipient to opt out of future faxes to the same machine. The chief sponsor of the bill cited a U.S. Chamber of Commerce survey that put the cost of complying with the FCC's proposed "prior written permission" requirement at $5,000 per business for the first year and $3,000 for every year thereafter. As of July 23, 2004, H.R. 4600 has passed the House of Representatives and is pending in the Senate Committee on Commerce, Science & Transportation.

C. Do Not Email

1. CAN-SPAM Act

On December 16, 2003, President Bush approved the Controlling the Assault of Non-Solicited Pornography and Marketing Act, better known as the "CAN-SPAM Act." The law took effect on January 1, 2004.[29]

The CAN-SPAM Act affects every business that engages in email marketing. By preempting more than 30 state anti-spam laws (but not state anti-fraud remedies), Congress has created a national standard for commercial emails.

In the broadest terms, the CAN-SPAM Act imposes a number of affirmative requirements on commercial electronic mail messages. It also establishes criminal and civil penalties for a wide range of practices that Congress determined are often used by spammers. Although most of the prohibitions should not pose much risk to legitimate businesses, email marketers must be familiar with both categories of provisions, because the CAN-SPAM Act applies to any business that sends commercial emails, not just so-called spammers.

In particular, the Act:

- Allows businesses to continue to send commercial emails to their customers and prospects, but gives consumers the right to require that a sender of unsolicited

[29] Pub. L. 108-187 (2003).

commercial email cease sending commercial emails to them. This is an "opt-out" approach, also known as "one free shot;"

- Requires senders of commercial email to include a functional "opt-out" mechanism in commercial emails. No one format is mandated; senders may comply by using a functional "unsubscribe" return address or a hyperlink to an Internet site that presents one or more options. This must remain operational for 30 days. However, "opt-outs" are not required in "transactional or relationship messages;"

- Requires senders of commercial email messages to provide "clear and conspicuous" identification that the message is an advertisement or solicitation, unless the recipient has given prior "affirmative consent" to receipt of the message. "Affirmative consent" means express consent in response to a clear and conspicuous request for such consent, or consent given at the recipient's own initiative. The Act does not require the use of "ADV:" in the subject line, but it did direct the FTC to conduct a proceeding to determine whether such labeling on email should be required;

- Allows generally the sale or rental of email lists; however, an email address of a recipient who has "opted out" of further commercial emails may not be transferred to a third party;

- Preempts state and local anti-spam laws, except insofar as such laws prohibit falsity and deception in any portion of a commercial email message;

- Creates criminal and civil sanctions (up to $2 million, which can be trebled) for a number of common practices of spammers, including the use of deceptive or misleading origin information, false or misleading headers, falsified sender identity, deceptive or misleading transmission information, deceptive subject lines and falsely registered IP addresses;

- Assigns law enforcement to the FTC, the Justice Department and state attorneys general. It also permits Internet access providers to bring lawsuits in narrowly defined circumstances. The Act does <u>not</u> create a private right of action except for Internet access providers;

- Directed the FTC to study and report to Congress on, among other things, a possible "Do Not Email" registry (see Section IV.C.2 below);

- Directed the FTC to adopt a rule within 120 days on labeling of emails containing sexually-oriented material;[30]

- Directed the FTC to conduct certain other rulemakings to aid in enforcement of the Act (see below); and

- Directed the Federal Communications Commission, in consultation with the FTC, to conduct a rulemaking to protect consumers from unwanted messages on wireless phones.[31]

[30] On April 19, 2004, the FTC published a final rule requiring that commercial emails containing sexually explicit materials display the words "SEXUALLY EXPLICIT" in the subject line of the email. 69 Fed. Reg. 21024 (April 19, 2004.

The FTC's rulemaking to elaborate on terms used in the CAN-SPAM Act is in the works.[32] The statute directs the Commission to define relevant criteria to determine the "primary purpose" of an electronic message. This is a critical term, because the Act defines "commercial electronic mail message" as "any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commerical product or service (including content on an Internet website operated for a commerical purpose."

The CAN-SPAM Act also gives the FTC discretionary authority with respect to certain other key terms, including "transactional or relationship messages." The latter term is critical because "transactional or relationship messages" are excluded from the definition of "commercial electronic mail message," and therefore from most of the requirements of the Act. Congress authorized the FTC to "expand or contract" the categories of transactional or relationship messages defined in the statute.

The FTC's Advance Notice of Proposed Rulemaking and Request for Public Comment attracted well over 6,000 comments, including a submission from the International Franchise Association.[33] The IFA urged the FTC to make clear that "transactional or relationship messages" would include:

- "all e-mail messages in connection with a franchise agreement, contractual rights, or otherwise relating to a franchise system sent by a franchisor to the franchisees in that same network, or by franchisees in that network to the franchisor and/or to the other franchisees in that same network"

- "e-mails sent to an individual in the capacity of his or her employment by, or by virtue of his or her role as an agent or representative of, a business with which the sender has an ongoing commercial relationship"

- "e-mails sent to a franchisee (as well as individuals employed by or representing the franchisee) by a vendor that has an ongoing commerical relationship with the franchisor or with the franchise network"

- "e-mails sent by a membership association to its members"

The IFA also responded to the FTC's request for comment on situations involving multiple senders of an email (such as "an email message that promotes an upcoming conference and also includes ads from the companies sponsoring the conference"). The IFA urged the FTC to clarify that a franchisor and its franchisees, though united by a common brand, are different senders. IFA's concern is that franchisors and franchisees might inadvertently run afoul of the rule if viewed as a single "sender." For example, the franchisor might send an email to a customer who had opted out with a franchisee, thinking that the opt out would apply to all

---

[31] The FCC initiated a rulemaking in March 2004. See *http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-244843A1.pdf*.

[32] Advance Notice of Proposed Rulemaking and Request for Public Comment, 69 Fed. Reg. 11776 (March 11, 2004).

[33] Letter dated April 20, 2004 from Matthew R. Shay, Vice President and Chief Counsel, International Franchise Association, to Donald S. Clark, Secretary, Federal Trade Commission.

businesses operating under the brand. The IFA cautioned that it would be impractical to treat a franchise system as a single "sender," because "not every franchisee will have the time or resources to check a systemwise opt-out list before sending emails" and "not every franchisee will be willing to share its opt-out list with other franchisees in the same system or even with the franchisor."

2. A Do Not Email Registry?

As noted above, the CAN-SPAM Act imposed a mandate on the FTC to report to Congress on a possible "Do Not Spam" registry. On June 15, 2004, the FTC submitted a report concluding that a "Do Not Spam" registry would be a futile effort.[34] The Commission analyzed three types of possible registries: a registry containing individual e-mail addresses; a registry containing the names of domains that did not wish to receive spam; and a registry of individual names that required all unsolicited commercial e-mail to be sent via an independent third party that would deliver messages only to those email addresses not on the registry.

The report concluded that none of the three alternatives could be enforced effectively. The FTC recommended that anti-spam efforts focus on creating a robust e-mail authentication system that would prevent spammers from hiding their tracks and thereby evading Internet service providers' anti-spam filters and law enforcement. The FTC simultaneously announced that it would sponsor an "Authentication Summit" in Fall 2004 to analyze possible authentication systems and encourage their swift deployment.

3. FTC Anti-Spam Cases

Meanwhile, the FTC has begun enforcement of the CAN-SPAM Act. On April 29, 2004, the FTC filed two civil lawsuits in federal District Court in Chicago, alleging that the defendants violated the CAN-SPAM Act by sending commercial emails that made deceptive claims and failed to meet the act's opt-out requirements.[35] The FTC alleged that Phoenix Avatar used deceptive email messages (containing false headers, "spoofing" as to origin and not including required disclosures) to market a fake diet patch. Similarly, the FTC asserted that Global Web Promotions, an Australian company, sent spam emails marketing fraudulent products, such as human growth hormone products said to help users maintain their physical appearance.

The court issued a temporary restraining order, and susequently a preliminary injunction, against Phoenix Avatar, freezing the company's assets and ordering it not to send spam emails. The FTC also seeks injunctive relief against Global Web Promotions. Because that company is an Australian entity, the FTC has obtained a preliminary injunction against "fulfillment houses" in the United States to prevent delivery of Global's products.

---

[34] *National Do Not Email Registry: A Report to Congress* (FTC June 2004). The report is available at *http://www.ftc.gov/reports/dneregistry/report.pdf*.

[35] *FTC v. Phoenix Avatar, LLC*, No. 04C 2897 (N.D. Ill. filed April 23, 2004); *FTC v. Global Web Promotions, LLC*, No. 04C 3022 (N.D. Ill. filed April 28, 2004).

As a result of its joint investigation, the FTC and the U.S. Attorney's Office for the Eastern District of Michigan also filed a separate criminal complaint under the CAN-SPAM Act and postal fraud statutes against four individuals associated with Phoenix Avatar.[36]

4. Private Lawsuits Under CAN-SPAM

The FTC's actions follow several private lawsuits by Internet service providers under the CAN-SPAM Act. For example, in March 2004, Internet service providers America Online, Earthlink, Microsoft, and Yahoo! reportedly filed suits against hundreds of defendants allegedly responsible for spamming.[37] And in a separate action, America Online obtained a default judgment against three spammers in U.S. District Court for the Eastern District of Virginia on April 27, 2004.[38]

As noted above, the CAN-SPAM Act does not allow private parties other than ISPs to bring causes of action for violations. Moreover, because of the preemptive effect of CAN-SPAM, private parties will lose the right to bring certain claims under state anti-spam statutes. For example, in one of the first decisions in the country to address the preemptive effect of the CAN-SPAM Act, a Utah state court dismissed an individual's claim against an Internet services provider under the state's Unsolicited Commercial and Sexually Explicit Email Act.[39]

D. Do Not Violate Your Online Privacy Policy

There is still no federal law in the U.S.A. that requires the posting of a privacy policy on all websites. As of July 1, 2004, however, there is perhaps the closest thing to a federal law – a California statute. The California law requires commercial websites that collect personally identifiable information from California residents to post a privacy statement and to honor its terms.

1. California Online Privacy Protection Act

The California Online Privacy Protection Act of 2003[40] is the first law in the United States to require generally that websites post privacy statements. Website operators who have sought to avoid making enforceable privacy promises by simply not publishing a privacy statement will have to change their strategy if they wish to continue doing business with California residents.

The act applies to any commercial website (or online service equivalent) that collects personally identifiable information (PII) about individuals residing in California. Under the law, PII is

---

[36] *United States v. Lin*, No. 04-80383 (E.D. Mich. filed April 29, 2004).

[37] Pete Barlas, *Internet Titans Wage Legal War vs. Spam*, Investor's Business Daily (March 11, 2004). Case numbers for these lawsuits could not readily be found.

[38] *America Online, Inc. v. Hawke, et al.*, No. 04-CV-259 (E.D. Va. filed March 9, 2004).

[39] *Ormond v. GTE Net LLC d/b/a Verizon Internet Solutions, et al.*, No. 040400091 (Utah Dist Ct. filed March 31, 2004). Wiley Rein & Fielding LLP represented Verizon in this case.

[40] Cal. Bus. & Prof. Code § 22575 *et seq.*

defined as *any* of the following: (1) first and last name, (2) home or other physical address (including street name), (3) mailing address, (4) telephone number, (5) Social Security number, (6) any other identifier that permits the physical or online contacting of a specific individual and (7) information concerning a user that the website or online service collects online from the user and maintains in personally identifiable form in combination with any of the other identifiers.

The privacy statement required by the California law must:

- Identify the categories of PII that the operator collects through the website and the categories of third-party persons or entities with whom the operator may share that PII.
- Provide a description of any process by which an individual may review and request changes to any of his or her PII collected through the website.
- Describe the process by which the operator notifies consumers of material changes to its privacy policy for that website.
- Identify the privacy statement's effective date.

Most well-written privacy statements already address most of these requirements. For example, websites that participate in the TRUSTe online seal program should need only to add an effective date to their privacy statements, if their statements do not bear one already.

The law sets out four ways to "conspicuously post" a privacy statement, ranging from posting the entire policy on the home page or "first significant page" of the website, to the use of icons or text links to a privacy statement. The law specifies detailed aspects of the design of the text links.

The law gives state and local prosecutors authority to enforce violations under the California Unfair Competition law. However, the law provides that a website operator will be in violation only if it fails to post its policy within 30 days after being notified of noncompliance. Whether California's long-arm jurisdiction will permit enforcement against websites based in Maine or, for that matter, Mongolia, remains to be tested.

2. FTC Enforcement Actions

The FTC treats posted privacy policies as binding promises made by the website operator to consumers who use the web site. In a series of enforcement actions, the FTC has alleged that website operators engaged in unfair or deceptive acts or practices under Section 5 of the FTC Act by making representations about their privacy practices and then failing to honor those representations. Initially, the FTC focused on website operators who sold or shared personal information in ways that were contrary to its stated policy; this area continues to attract the agency's attention.[41] More recently, the FTC has gone after companies for website security breaches – situations where the website operator did not voluntarily disclose or misuse consumers' information, but where outsiders gained access to the information. And in the latest

[41] *E.g., In the Matter of Educational Research Center of America, et al.*, Docket No. C-4079 (FTC final order May 6, 2003); *In the Matter of The National Research Center for College and University Admissions, Inc., et al.*, Docket No. C-4071 (FTC final order January 28, 2003).

action discussed below, the FTC challenged for the first time a company's material change to its privacy policy.

It should be noted that all of the enforcement actions discussed below resulted in negotiated consent orders. By entering into these settlement agreements, the companies involved did not admit to violating any law, so the FTC's legal theories remain untested by adjudication.

a. Retroactive Changes to Privacy Policy

On July 7, 2004, the FTC announced a settlement in the agency's first action to challenge a company's material change to its privacy policy.[42] The FTC charged Gateway Learning Corporation, which markets and sells products under the "Hooked on Phonics" brand name, committed deceptive and unfair practices by renting consumers' personal information to target marketers, contrary to explicit promises made in the company's privacy policy.

Gateway Learning's website privacy policy stated: "We do not sell, rent or loan any personally identifiable information regarding our consumers with any third party unless we receive customer's explicit consent." It also stated that "we do not provide any personally identifiable information about children under 13 years of age to any third party for any purpose whatsoever." The policy also stated that if Gateway Learning changed its policy, it would give consumers the chance to "opt-out" of having their information shared.

According to the FTC's complaint:

In April 2003, Gateway Learning started renting personal information provided by consumers – including their names, addresses, phone numbers, and age ranges and gender of their children – to target marketers to send mailings and make telemarketing calls.

In June 2003, the company revised the privacy policy on its Web site to state that "from time to time" Gateway Learning would provide consumers' personal information to "reputable companies" whose products or services consumers might find of interest.

Gateway Learning did not inform consumers who had already provided their information that the company had revised its privacy policy, nor did it highlight on its Web site the fact that the privacy policy had changed.

The FTC charged that Gateway Learning's practices violated Section 5 of the FTC Act in three ways: First, Gateway Learning's claims that it would not sell, rent, or loan to third parties consumers' personal information unless it received the consumers' consent, and that it would never share information about children, were false. Second, the company's retroactive application of a materially changed privacy policy to previously-collected information was an unfair practice. Third, Gateway Learning's failure to notify consumers of the changes to its privacy policy and practices, as promised in the original policy, was deceptive.

The proposed settlement (which was open for public comment but not final as of this writing) bars misrepresentations about how Gateway Learning will use the data that it collects from consumers. The consent order (1) requires Gateway Learning to obtain affirmative consent

[42] *In the Matter of Gateway Learning Corp.*, File No. 042-3047 (FTC complaint and proposed order published July 7, 2004).

from consumers before sharing any personal information that the company collected from them under the original privacy policy; (2) requires the company to forfeit the $4,608 it had earned from renting consumers' information; and (3) for any future material changes to the privacy policy, prohibits the company from applying the changes retroactively without consumers' consent.

b. Security Breaches

On April 21, 2004, the FTC announced a settlement with Tower Records for posting misleading website security statements.[43] The FTC alleged that Tower Records' privacy policy represented that the company safeguarded all personal information, but a security flaw in the website permitted other web users to access order history information from the site. Outsiders could access personal information such as names, phone numbers and billing addresses. No actual security breaches were reported as a result of the security flaw, but the company agreed to implement an independently audited information-security program as part of its settlement agreement with the FTC.

Tower Records was the fourth FTC enforcement action on security breaches. The third was against clothing maker Guess?, Inc., which settled FTC charges regarding its website security in June 2003.[44] Under the settlement agreement, the company agreed to establish a new security program for its website, GUESS.com.

The FTC's complaint alleged that Guess?, Inc. had exposed customers' personal information to computer hackers after guaranteeing to those customers that the website was secure. The FTC also alleged that Guess?, Inc. failed to detect foreseeable vulnerabilities of the website and failed to use reasonable or appropriate measures to prevent third parties from accessing customers' information.

The FTC's charges arose as a result of Guess?, Inc.'s sale of products to customers through its website, which contained security guarantees, including a privacy policy that promised the site had "security measures in place to protect the loss, misuse and alteration of the information under our control." Customers paid with a credit or debit card and had to provide personal information such as name, address, card number and card expiration date. Guess?, Inc. then stored the information in databases connected to the website. According to the FTC, computer hackers could easily access the stored information, and in 2002 a hacker did access the customer credit card information. Consequently, the FTC asserted that Guess?, Inc. had failed to store the information in an unreadable, encrypted format at all times, as promised by the website's privacy and security policies.

The FTC's first two security breach cases were in 2002. In January 2002, drug maker Eli Lilly & Co. entered into a consent agreement to settle charges related to the accidental disclosure of the email addresses of subscribers to the company's Prozac service.[45] In August 2002,

---

[43] *In the Matter of MTS, Inc., d/b/a Tower Records/Books/Video and Tower Direct, LLC, d/b/a TowerRecords.com*, Docket No. C-4110 (FTC final order May 28, 2004).

[44] *In the Matter of Guess?, Inc. and Guess.com, Inc.*, Docket No. C-4091 (FTC final order July 30, 2003).

[45] *In the Matter of Eli Lilly and Company*, Docket No. C-4040 (FTC final order May 8, 2002).

Microsoft Corp. entered into a consent agreement to settle charges related to the privacy and security of personal information collected online from consumers.[46]

c. COPPA Enforcement

The Children's Online Privacy Protection Act (COPPA)[47] applies to operators of commercial websites directed at children aged 13 or younger, or to websites having actual knowledge that they are collecting personal information from children under 13. COPPA requires such website operators to take specific measures to protect children's privacy, including obtaining verifiable parental consent to the collection and use of personally identifiable information about children. The FTC, at Congress' direction, issued rules to implement COPPA.[48]

The FTC has had an active enforcement record under COPPA – including an enforcement action against a franchisor, Mrs. Fields Original Cookies, Inc.[49] In February 2004, the Commission announced two more enforcement actions. One of the settlements, with Universal Music Group (UMG), resulted in a civil penalty of $400,000, the largest COPPA penalty to date (four times larger than the penalty paid by Mrs. Fields in February 2003).[50]

UMG is a music recording company that operates hundreds of websites promoting its labels and artists, many of which attract child audiences. These websites offer activities such as email newsletters, fan clubs and bulletin boards that require registration to participate. The registration form to access these activities collected personal information such as name, date of birth, email address, home address, phone number, gender and music preferences. Parental consent was not required by UMG before a child completed and returned these forms. UMG did send permission notices to parents in some cases, but only after it had collected the registration information.

The FTC alleged that UMG had collected children's personal information without parental consent in violation of COPPA. The FTC asserted that UMG knew that children were providing them with personal information, without parental consent, because visitors entered birth dates on these registration forms. Tens of thousands of registrants indicated they were under thirteen years of age. In addition, the FTC argued that UMG's website for 13-year-old singer Lil' Romeo, www.lilromeo.com, is a website directed at children. That website used the same registration form and procedure as those used on the other UMG websites.

In a separate consent decree filed in the same court on the same day, Bonzi Software, Inc. agreed to pay a $75,000 civil penalty to settle alleged COPPA violations. A free download from Bonzi's website, BonziBUDDY, is a purple cartoon gorilla that appears on users' screens and

---

[46] *In the Matter of Microsoft Corporation*, Docket No. C-4069 (FTC final order December 20, 2002).

[47] 15 U.S.C. §§ 6501-6505.

[48] 16 C.F.R. Part 312.

[49] *United States v. Mrs. Fields Famous Brands, Inc., et al.*, Civ. Action No. _____ (D. Utah consent decree and order filed February 26, 2003).

[50] *United States v. UMG Recordings, Inc.*, Civil Action No. CV-04-1050 JFW (Ex) (C.D. Cal. Consent decree and order filed February 17, 2004).

entertains them with antics such as telling jokes and asking trivia questions. Like UMG's websites, BonziBUDDY's online registration form required personal information, including date of birth. Consequently, Bonzi was charged with actual knowledge that thousands of children were providing personal information through the registration process. The complaint alleged that Bonzi did not obtain parental consent before collecting this information.

In addition to paying the civil penalties and agreeing to comply with COPPA in the future, both UMG and Bonzi agreed to delete all information they had collected from children.

3. State Developments

a. California Security Breach Law

On July 1, 2003, a statute took effect in California that requires notification to affected individuals in the event of certain breaches of computer security. Anyone conducting business in California "that owns or licenses computerized data that includes personal information" is required to disclose "any breach of the security of the system" following discovery or notification of the breach "to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." The business must make the disclosure "in the most expedient time possible and without unreasonable delay," consistent with the needs of law enforcement.

This law applies to any unauthorized acquisition of personal information from computerized data (e.g., hacking into a company's human resources database). It has a somewhat narrower-than-usual definition of "personal information" that ties in to its objective of preventing identity theft: an individual's first name or first initial and last name *in combination with* any of the following, when either the name or the associated information is not encrypted: the individual's (i) SSN, (ii) driver's license number (or California identification card number), or (iii) account number or credit or debit card number plus access code or password to access to the individual's account.

Notice of a breach may be in writing or electronic format; the statute does not specify content. If the cost of notice would exceed $250,000 or the number of individuals exceeds 500,000, or if the business lacks sufficient contact information, substitute notice may be given by email, conspicuous publication on the company's web site, AND notification to major statewide media (thereby essentially placing security breaches on a par with product recalls). Any customer injured by a violation of the statute may bring a civil action to rcoever damages or seek injunctive relief. Although the law requires notice only to California residents, a company obviously may want to provide equal treatment to all affected individuals.

Enforcement of the statute against businesses located outside of California could conceivably run into challenges under the Commerce Clause of the federal Constitution, but by its terms it applies to any business that "conducts business" in California.

In May 2004, the California state Senate approved a bill (S.B. 1279) to expand this law to apply to unauthorized acquisition of personal information from noncomputerized data (i.e., paper records). The bill was prompted by an incident in which Bank of America sent 3,800 year-end tax statements to the wrong persons.

As of June 2004, New York state lawmakers were considering a bill modeled after the California computer security law.

b. Barnes & Noble

On April 29, 2004, New York State Attorney General Eliot Spitzer announced an agreement with Barnes & Noble involving an Internet security breach on its website that enabled third party access to some consumers' personal information.[51] The agreement followed the AG's investigation into a design flaw in the online book seller's website that left consumers' accounts and personal information unsecured.

The NY security breach resulted from Barnes & Noble's use of "cookie-less" shopping. While the Barnes & Noble system avoided using cookies, the company stored user information in the webpage URL. When users then forwarded the Barnes & Noble web page, they also unknowingly could have forwarded personal information contained in the URL.

The AG's office began the investigation in 2002. The alleged security breaches apparently occurred sometime between 1998 and 2002. Notably, the AG did not discover actual cases where customer information was misused as a result of the security breach. Thus, according to the AG, the agreement's purpose was to ensure that Barnes & Noble complies with its privacy policy in the future. According to the terms of the agreement with the AG, Barnes & Noble must establish an information security program, hire an external auditor to monitor the program, and pay a $60,000 fine.

E. Spyware

The latest entry in public concern about privacy is "spyware" – computer programs transmitted surreptitiously from the Internet that collect information about the recipient and/or interfere with the recipient's use of his or her personal computer. General public awareness of spyware is relatively new, but resentment is growing quickly, triggering the attention of legislators and regulators.

In response to public concerns, the private sector is working diligently on technological solutions. For example, in June 2004, Yahoo! announced that it would begin beta testing a feature proposed for its web browser tool bar, called Anti-Spy, that allows users to easily remove spyware programs from their computers.[52] In the same vein, Microsoft announced in May 2004 that its upcoming release of Windows XP Service Pack 2 would make it much harder to sneak software onto users' computers.[53] However, these private sector developments are in a race with legislative and regulatory initiatives to address the perceived problem.

---

[51] See *http://www.oag.state.ny.us/press/2004/apr/apr29a_04.html*.

[52] Elizabeth Millard, *Yahoo Adds Anti-Spyware to Toolbar,* E-Commerce Times (May 27, 2004) (available at *http://www.ecommercetimes.com/story/security/34070.html*).

[53] *Microsoft to Battle Spyware,* Wired News (May 13, 2004) (available at *http://www.wired.com/news/technology/0,1282,63440,00.html?tw=wn_tophead_4*).

1. FTC Workshop and Testimony

On April 19, 2004, the FTC conducted a full-day public workshop on spyware.[54] In subsequent testimony before the Subcommittee on Commerce, Trade and Consumer Protection of the House Committee on Energy and Commerce, delivered by FTC Commissioner Mozelle Thompson and J. Howard Beales, Director of the Bureau of Consumer Protection, the Commission called spyware "a new and rapidly growing practice that poses a risk of serious harm to consumers."[55] The prepared statement cautioned that spyware may harvest personally identifiable information from consumers, facilitate identity theft by surreptitiously planting a keystroke logger on a user's personal computer, create security risks if it exposes communication channels to hackers, and affect the operation of personal computers, causing crashes, browser hijacking, home page resetting, and the like. According to the Commission, "these harms are problems in themselves, and could lead to a loss in consumer confidence in the Internet as a medium of communication and commerce."

The Commission testimony revealed that the FTC is conducting non-public investigations related to the dissemination of spyware, but warned of "substantial law enforcement challenges" not only in defining "spyware" but also in ascertaining from whom, from where, and how it is disseminated.

The testimony also described the Commission's enforcement action against D Squared Solutions, LLC, in which the defendants allegedly exploited an operating system feature to harm consumers.[56] The Windows operating system uses "Messenger Service" windows to allow network administrators to provide instant information to network users (for example, a message to let users know that a print job has been completed). The FTC alleged that the defendants exploited this feature to send Messenger Service pop-up ads to consumers – in fact, ads for software that supposedly would block such ads in the future. Consumers would receive these pop-up ads as often as every ten minutes. The Commission's complaint alleges that the defendants unfairly interfered with consumers' use of their computers and tried to coerce consumers into buying software to block pop-up ads.

2. H.R. 2929

Congress may be unwilling to wait for further private sector developments and FTC enforcement on spyware. On June 24, 2004, less than two months after the testimony described above, the House Energy & Commerce Committee approved an anti-spyware bill, H.R. 2929. If the bill becomes law, it will require the FTC to adopt regulations governing spyware programs. H.R. 2929 defines "spyware program" as software that has the capability of transmitting, by means of the Internet, without any action by the user, information regarding the computer user, information regarding use of the computer, or information that is stored on the computer.

The bill directs the FTC to:

---

[54] See *http://www.ftc.gov/bcp/workshops/spyware/index.htm*.

[55] See *http://www.ftc.gov/opa/2004/04/spywaretest.htm*.

[56] *FTC v. D Squared Solutions, LLC*, No. 03-CV-3108 (D. Md. 2003).

- Prohibit transmission of a spyware program without the express consent of the computer user (either an affirmative request by the user, or a consent given in response to a clear and conspicuous request for consent by the transmitter of the program).

- Prohibit use of spyware to collect personally-identifiable information (PII) unless notice that the program will be used for that purpose is given (a) in the license or communication with which the program is transmitted, AND (b) in another prominent location to be determined by the FTC. However, the bill defines PII to exclude aggregate data that does not identify a specific person, computer, user, or email address.

- Establish requirements for transmission of spyware, if the transmitter requires the user to agree to a license. These requirements are to include: (a) that the terms of the license and the agreement mechanism appear on the same web page; (b) that the license clearly state that it constitutes consent to transmission of the program; (c) that the license clearly explains the purpose of including the spyware; and (d) that the web page discloses the name of and a valid physical street address for the transmitter, as well as a functioning return email address.

The bill directs the FTC to distinguish "spyware" from "other commonly used programs to share information among computers in an organized network."

If H.R. 2929 becomes law, a violation of the statute will constitute an unfair or deceptive act or practice under the FTC Act, and there will be criminal penalties for violation of the requirement to give notice of collection of personally-identifiable information or knowing violation of any of the other provisions. A counterpart bill (S. 2131) is pending in the Senate.

State legislatures have adopted or are considering similar anti-spyware measures.[57] It seems to be assumed that a federal anti-spyware law, like the CAN-SPAM Act, would preempt state law, though H.R. 2929 does not presently include a preemption provision.

F. Fair and Accurate Credit Transactions Act

The Fair and Accurate Credit Transactions Act of 2003 (known as FACTA or the FACT Act) was signed into law on December 4, 2003.[58] FACTA makes sweeping changes and additions to the Fair Credit Reporting Act (FCRA), which since 1970 has governed the collection, use, and communication of "consumer report" information (i.e., information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living) by "consumer reporting agencies," including national credit bureaus. The primary features of FACTA include making permanent the existing FCRA preemption of state law; adding new provisions to combat identity theft; and adding provisions to enhance accuracy and consumer access to credit information. As in so many other situations, Congress directed the FTC to undertake a series of rulemakings (in many cases in coordination

[57] David McGuire, *States Speed Up Spyware Race*, WashingtonPost.com, May 13, 2004 (available at *http://www.washingtonpost.com/wp-dyn/articles/A24746-2004May13.html*).

[58] Pub. L. 108-159 (2003).

with the Federal Reserve Board and other financial regulators) to further define and implement the new law.

It would be far too ambitious to describe all of the FACTA rulemakings here.[59] All businesses, however, should be aware of a proposed rule regarding the disposal of sensitive consumer report information. Section 216 of FACTA directed the FTC and other agencies to promulgate the "Disposal Rule" as a means to combat identity theft. The FTC published its proposed rule for comment in April 2004.[60]

The proposed rule defines "consumer information" as any record about an individual, whether in paper, electronic, or other form, that is a consumer report or is derived from a consumer report. Information that does not identify any particular consumers would not be covered. The rule would apply to "any person over which the Federal Trade Commission has jurisdiction that, for a business purpose, maintains or otherwise possesses consumer information or any compilation of consumer information." This includes not only consumer reporting agencies and frequent users of consumer reports (such as lenders, insurers, employers, landlords, government agencies, mortgage brokers, and car dealers), but any business that possesses or maintains information covered by the rule. Moreover, companies "that possess consumer information in connection with the provision of services to another entity" are also covered, to the extent that they dispose of the consumer information.

The proposed rule sets a flexible standard: covered persons must "take reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal." Thus, like other aspects of the FCRA, the rule would be process-oriented. It would not require a company to ensure perfect destruction in every instance, as long as the company's prodecures were reasonable. In determining what measures are "reasonable," the Commission expects companies to consider "the sensitivity of the consumer information, the nature and size of the entity's operations, the costs and benefits of different disposal methods, a relevant technological changes." Reasonable measures are "very likely" to require establishment of policies and procedures and employee training.

The comment period on the Disposal Rule closed on June 15, 2004. The proposed effective date is three months from publication of the final rule in the Federal Register.

G. Private Litigation

This section collects a few of the most interesting recent decisions in private lawsuits for alleged privacy violations. It is by no means a comprehensive survey.

1. Privacy Act

On February 24, 2004, the U.S. Supreme Court announced its much anticipated decision in *Doe v. Chao*, construing the private right of action for monetary damages redressing "intentional or willful" government violations of the federal Privacy Act.[61] By a 6-3 majority, the Court held that

[59] See *http://www.ftc.gov/os/statutes/fcrajump.htm* for a complete listing.

[60] 69 Fed. Reg. 21388 (April 20, 2004).

[61] *Doe v. Chao*, __ U.S. __, 124 S. Ct. 1204 (2004).

a plaintiff must prove "actual damages even to qualify for a minimum statutory award of $1,000." In so ruling, the majority expressly acknowledged that it was rejecting the conflicting views of the First, Fifth, Ninth, Eleventh and District of Columbia Circuits.

Doe's suit arose from the Department of Labor's practice of using the Social Security numbers (SSNs) of claimants for Black Lung Benefits as file numbers or docket numbers, with the result that many SSNs were widely disclosed through multi-captioned hearing notices and published decisions. Doe, fearing the risks of identity theft, brought an action for damages under the Privacy Act. It was uncontested that the Department of Labor's conduct met the intentional or willful standard, but whether Doe could recover anything (including reasonable attorneys fees) absent a showing of actual damages was disputed. The U.S. District Court ruled that Doe was entitled to recover the $1,000 statutory minimum. A divided Fourth Circuit panel reversed, holding that actual damages were required and that Doe had not met that standard.

The only issue before the Supreme Court was whether a showing of actual damages is required. The Court affirmed the Fourth Circuit on that issue based on a "straightforward textual analysis." Neither the majority nor the dissenting opinions mentions the statutory construction theory upon which the government's brief principally relied—namely, that any "waiver of sovereign immunity must be clearly and unequivocally expressed in the statutory text." Had that theory been employed by the majority, it might have served to distinguish construction of the Privacy Act from construction of statutes providing for civil actions between private parties, such as the Electronic Communications Privacy Act, which provides for recovery of "actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation, but in no case shall a person entitled to recover receive less than the sum of $1,000." The majority's reliance, instead, on "straightforward textual analysis" may cast a cloud over the ECPA as well.

Moreover, the Court left unresolved the question of what constitutes "actual damages." The majority suggested that "pecuniary expenses" that would "fall well short of $1,000" could include "fees associated with running a credit report, for example, or the charge for a Valium prescription." The dissenters asserted that this interpretation "invites claimants to arrange or manufacture such damages" and found it "dubious to insist on such readily created costs as essential to recovery." They further charged that such examples reveal that the majority's "disagreement with the construction of the Act prevailing in the Circuits" is "ethereal."

2. ***Pharmatrak***

In what may represent the final chapter of litigation addressing the legitimacy of Internet cookies and related technologies, a Massachusetts federal district court ruled that interceptions of communications using such technologies do not *per se* violate the Electronic Communications Privacy Act (ECPA). The case, *In re Pharmatrak, Inc. Privacy Litigation*,[62] was monitored closely, because the United States Court of Appeals for the First Circuit had previously adopted a comparatively narrow definition of "consent" under ECPA. Additionally, the First Circuit had ruled that third-party website monitoring could constitute an "interception" under ECPA. Finally, the First Circuit had left open the question as to whether the use of "Web bugs" or "clear GIFs"—a tiny graphical image not noticeable by the casual user—is inherently illegal.

[62] 220 F.Supp.2d 4 (D. Mass. 2002), *rev'd*, 329 F.3d 9 (1st Cir. 2003), *on remand*, 292 F.Supp.2d 263 (D. Mass. 2003).

The *Pharmatrak* litigation arose from an arrangement by which Pharmatrak provided website monitoring services for a number of pharmaceutical companies. The Pharmatrak service collected information about visitors to the client companies' websites to be used for intra-industry comparisons of website traffic and usage. For example, Pharmatrak tracked whether visitors were first-time or repeat visitors, the "referrer pages" from which they came and similar information. The pharmaceutical companies did not want Pharmatrak to collect personal or identifying data about their site visitors.

Pharmatrak provided its service, called "NETcompare," through the use of a "Web bug" or "clear GIF." HTML code in the pharmaceutical company website would retrieve the Web bug from the Pharmatrak server, and Pharmatrak would place a cookie on the user's computer.

Although Pharmatrak denied any intent to collect personal information, several configurations of website usage in fact caused Pharmatrak to collect personal information about a small number of users of certain sites. In discovery, plaintiffs' expert was able to find detailed user profiles of 232 users on Pharmatrak's servers (Pharmatrak set some 18.7 million cookies during the relevant period).

In their class-action complaint, plaintiffs sued both Pharmatrak and the pharmaceutical companies, averring that the arrangement violated a number of federal and state privacy laws, including Titles I and II of the Electronic Communications Privacy Act, the Computer Fraud and Abuse Act, and several Massachusetts statutory and common laws. The U.S. District Court granted summary judgment to defendants on these claims.[63]

On appeal to the First Circuit, plaintiffs sought review only of the District Court's dismissal of the claim based on Title I of ECPA. Title I of ECPA extended to data and electronic transmissions the protections that prior federal law had accorded to oral and wire communications. Title I, in relevant part, creates a private right of action against a party who "intentionally intercepts…any…electronic communication." "Intercept" is the "acquisition of the contents of any … electronic … communication through the use of any electronic … device." ECPA establishes a defense of prior consent to an interception, which either party to the communication may provide.

The issues before the Court of Appeals were whether Pharmatrak's service had constituted an impermissible "interception" and, if so, whether its pharmaceutical clients had "consented" to such interception. Taking the latter question first, the Court of Appeals held that the burden of proving consent, at least in a civil case, fell upon Pharmatrak.[64] The Court ruled that the party claiming consent must prove either actual consent or, in its absence, show "convincingly" that implied consent was given.

On the facts, the Court of Appeals ruled that consent was not present. The First Circuit found that "deficient notice will almost always defeat a claim of implied consent." The Court also held that Pharmatrak's collection of personal data constituted an "interception" under ECPA.

---

[63] *In re Pharmatrak, Inc. Privacy Litigation*, 220 F.Supp.2d 4 (D. Mass. 2002).

[64] *In re Pharmatrak, Inc. Privacy Litigation*, 329 F.3d 9 (1st Cir. 2003).

In a 1986 amendment, Congress changed the ECPA state-of-mind requirement from "willful" to "intentional," defining "intentional" as being "narrower than the dictionary definition" of the term. Instead, rather than merely being a voluntary act, the conduct or result "must have been the person's conscious objective." The First Circuit had written that Congress made clear that inadvertent interceptions are not a sufficient basis for criminal or civil liability under the ECPA.

The First Circuit remanded the case to the district court for further action on whether the "intent" requirement of ECPA was satisfied. The district court considered whether the activities at issue had been "intentional."[65] The defendants argued that none of the facts in the record supported the conclusion that they had actionable intent because:

(1) only a small amount of personal data was actually found on Pharmatrak's servers;

(2) errors by third parties caused the collection of the personal data; and

(3) the defendants had no knowledge of the existence of the personal data until after the plaintiffs filed their lawsuit.

The district court accepted that the amount of personal information found was almost *de minimis*. Rejecting the plaintiffs' argument that the errors could have been avoided with proper safeguards, the district court agreed with the defendants that this could not be intentional conduct and at most represented negligence. Finally, the district court agreed that there was no evidence in the record to contradict the evidence that Pharmatrak had no knowledge that it had collected personal information until a year and a half after the plaintiffs filed their suit. Based on these conclusions, the court granted the defendants' summary judgment motion.

The district court's ruling is of interest for several reasons. First, it appears to set up a threshold, where, absent collection of a certain amount of information, a court may conclude that the collection is not intentional. Second, plaintiffs seeking to survive summary judgment must be fortunate enough to find a smoking gun of sorts during the discovery process so that they may overcome general denials of knowledge by those collecting the information. Finally, because some of the interception and collection at issue was made possible by third-party activities and technology, a higher premium may be placed on knowledge of the underlying capabilities of technology being utilized.

3. TriWest "Security Breach" Class Action

On October 20, 2003, a federal judge in Arizona dismissed a class action lawsuit that had been filed against TriWest Healthcare Alliance stemming from a security breach at the TriWest facilities.[66] This suit had raised concerns about potential liability arising from the mere fact of a security breach. Its dismissal indicates that courts will continue to scrutinize carefully complaints alleging only theoretical damages.

TriWest, a contractor for the Department of Defense (DoD) health care program, was the victim of a break-in, in which computer-related equipment was stolen. The equipment contained

[65] *In re Pharmatrak, Inc. Privacy Litigation*, 292 F.Supp.2d 263 (D. Mass. 2003).

[66] *Stollenwerk v. TriWest Health Care Alliance Corp.*, No. 2:03cv00185 (D. Ariz. October 20, 2003) (bench ruling)

sensitive, personal information about more than half a million members of the TriCare health care plan sponsored by the Department of Defense.

TriWest's response to this problem may serve as a model. Promptly upon discovering the theft, TriWest issued a release to all its beneficiaries, announcing "that one of TriWest Healthcare Alliance's offices in Phoenix was broken into and computer equipment and data files containing personal information about our TRICARE beneficiaries were stolen. Since the motives for the crime are unknown at this time, it is important that you are aware that there is the possibility that the information may be misused, exposing beneficiaries to the potential of identity theft." TriWest posted ongoing updates on its website about the situation and worked closely with the DoD to mitigate any harm from the situation. Nonetheless, TriWest faced an almost immediate class action suit, purportedly filed on behalf of 562,000 health care plan members whose personal information was allegedly involved in the security breach.

In an oral ruling from the bench, the court dismissed the complaint, finding that the class had suffered no actual damages. "Without damages, it doesn't matter how negligent anyone was," the court. The dismissal was without prejudice, affording the plaintiff an opportunity to amend and re-file the complaint.

The *TriWest* holding is consistent with *Smith v. Chase Manhattan Bank*.[67] In *Smith*, the New York Appellate Division addressed a purported class action to recover damages for alleged violations of New York General Business Law Section 349, which prohibits deceptive practices. According to the complaint, Chase violated its own privacy policies when it sold customer information, including the name, address, telephone numbers and other personal information of the plaintiff and the other alleged class members, to non-affiliated third-party vendors. These customer lists were then provided to telemarketing firms and direct mail agencies, which used the information to conduct solicitations. In return for providing the customer information, Chase allegedly received a commission on purchased products or services.

The court presumed that the allegations of the complaint were true, and indicated that, if true, the allegation that Chase sold confidential customer information to third party vendors in violation of its privacy policy did allege actionable deception. However, in the decision's dispositive holding, the court found that the plaintiffs "have not alleged, and cannot prove, any 'actual injury'" as required by the statute. According to the court, the "harm" at the heart of the purported class action "is that class members were merely offered products and services which they were free to decline. This does not qualify as actual harm." Moreover, the court added that the "complaint does not allege a single instance where a named plaintiff or any class member suffered any actual harm due to the receipt of an unwanted telephone solicitation or a piece of junk mail." Accordingly, the court dismissed the complaint.

4. ***Intel Corp. v. Hamidi***

In *Intel Corp. v. Hamidi,*[68] the California Supreme Court ruled that Intel could not use the common law tort of "trespass to chattels" to stop a former employee from sending emails through the Intel email system to numerous current Intel employees.

---

[67] 293 A.D.2d 598, 741 N.Y.S.2d 100 (N.Y. App. Div. 2002).

[68] 71 P.3d 296 (Cal. 2003).

The key facts in *Hamidi* were undisputed. Hamidi, a former Intel employee, on six occasions over two years, sent to over 30,000 Intel employees emails criticizing the company's employment practices, a total of perhaps 200,000. He offered to, and apparently did, remove recipients from his mailing list upon request. Hamidi breached no Intel security barriers in sending his emails, although he did manage to evade Intel's efforts to block them. The company then sought to enjoin further emails as common law trespass to chattels. The trial court enjoined Hamidi from any further mailings, and the Court of Appeals affirmed.

The California Supreme Court reversed. The majority ruled that, under California law, the tort of trespass to chattels does not encompass "an electronic communication that neither damages the recipient computer system nor impairs its functioning," because such email "does not interfere with the possessor's use or possession of, or any other legally protected interest in, the personal property [i.e., the computer system] itself." As for Intel's claims that it had, in fact, suffered consequential damages from the loss of productivity due to employees reading and reacting to Hamidi's emails, as well as the company's efforts to block the emails, the Court ruled that such harms were not injuries to the company's interest in its computers—the chattel—which continued to work as intended.

Significantly, Intel did not claim that its system was slowed by the burden of delivering the Hamidi emails. On this ground, the Court distinguished cases in which the unauthorized computer use impeded or threatened computer operations.

The dissenting justices contended that the owner of the computer system has a right to forbid the use of its computers to deliver messages. The dissenters also argued that Hamidi's unauthorized emails constituted a (however brief) appropriation of Intel's property for his own purposes that may be enjoined even without proof of actual physical or economic damage.

5. ***Northwest Airlines*** **Privacy Litigation**

On June 6, 2004, the federal district court in Minneapolis dismissed all claims against Northwest Airlines in a proceeding that consolidated seven putative class actions by Northwest customers.[69] The case arose when, in the aftermath of September 11th, NASA requested Northwest to provide certain passenger data in order to assist with a stufy of airline safety. Northwest supplied electronic passenger records containing passenger names, flight number, credit card data, hotel reservations, car reservations, and traveling companions.

The plaintiffs alleged that Northwest's actions violated ECPA, the Fair Credit Reporting Act, and Minnesota's Deceptive Trade Practices Act and constituted invasion of privacy, trespass to property, negligent misrepresentation, breach of contract, and breach of express warranty. The basis for most of the claims was Northwest's website privacy policy, which stated that the company would share customers' information only to make travel arrangements.

As noted above, the court dismissed all claims. There was no violation of ECPA because there was no improper interception of a communication; no violation of the FCRA because Northwest was not a "consumer reporting agency" and the information disclosed to NASA did not constitute "consumer reports": and no violation of the Minnesota DTPA (and no negligent misrepresentation) because those claims were preempted by the Airline Deregulation Act.

[69] *In re Northwest Airlines Privacy Litigation*, No. 04-126 (D. Minn. June 6, 2004).

The court's treatment of the remaining common law claims is even more interesting. The court dismissed the trespass claim because, the court concluded, the compilation of customer data was Northwest's own property. It dismissed the breach of contract and breach of warranty claims because Northwest's website privacy statement, in the court's view, did not constitute a unilateral contract, the breach of which would entitle the plaintiffs to damages. The court pointed to language vesting discretion in Northwest to determine when third parties might need the information. Further, the court held that there was no "offer" and "acceptance" where the plaintiffs failed to allege that they had actually read the privacy statement. These claims also failed because the plaintiffs failed to allege any contract damages arising from the alleged breach.

Finally, the court also dismissed the common law claim for invasion of privacy. To support the claim, the court stated, the plaintiffs had to show that the alleged intrusion would be "highly offensive to a reasonable person."[70] The plaintiffs had voluntarily provided their information to Northwest, and because they had not read the privacy policy, their expectation of privacy was low. Moreover, the disclosure of the information was only to a government agency for an unquestionably proper motive. Given these circumstances, the court decided as a matter of law that the disclosure would not be highly offensive to a reasonable person.

V. PRIVACY LAWS IN THE REST OF THE WORLD

In sharp contrast to the legislative schemes adopted for the protection of privacy in the private sector in the United States, which may be described as a "sectoral approach," many other countries, particularly those in Europe, have adopted private sector privacy laws of general application. Further these laws have taken very similar approaches. Accordingly in contrast to the discussion of the application and effect of a variety of laws as is necessary for any discussion of privacy protection in the United States, privacy laws in the rest of the world may be more easily discussed in general terms.

These laws have used the general principles discussed earlier in this paper. The general principles have been summarized by the FTC as being "Notice, Choice, Security and Access." The precise wording of the laws, however, varies from jurisdiction to jurisdiction. And more importantly, the structures of the laws, and the choice of remedies and enforcement, also vary.

Franchisors wishing to develop an international privacy compliance program will thus find that a general adherence to privacy principles will be effective in most countries, reducing the cost of general compliance and training. But there will need to be legal review for each jurisdiction where compliance is sought to ensure that the general principles and methods of implementation will be effective in the particular jurisdiction, and that the franchisor has conformed to the particular methods for compliance and enforcement used in that jurisdiction.

For example, a privacy policy that is fully compliant with Canada's privacy laws would generally be acceptable in Hong Kong SAR, Australia and the European Union. It may not however have Australia's specific reference to the use of national identifiers (such as social security numbers), and implementation of the policy alone would not be sufficient in the E.U., where notification or registration with the data protection authority of the jurisdiction and the appointment of a local representative would usually be required.

[70] Slip op. at 9, citing *Restatement (Second) of Torts* § 625B.

The variations discussed in this paper may be generally described as falling into two groups. One group is found in those jurisdictions that are part of the European Union[71], or to a lesser extent in jurisdictions that have a civil law system based on the European model, such as Argentina. The other major group of variations is found in common-law jurisdictions such as Canada, Australia and Hong Kong SAR. These will now be discussed separately.

There are two other groups developing in Asia and Latin America. In Asia, Taiwan has had a data protection law for computer processed information[72] since 1995; Japan has passed a law[73] to come into effect April 1, 2005. Korea is still at the stage of proposing a public sector law.[74] In Latin America Chile was the first country to adopt a law in addition to its constitutional protection, but there is no data protection authority, and individuals must enforce the law themselves through court action.[75] Argentina has a law and a data protection authority[76], as well a constitutional protection known as " Habeas Data."[77] Brazil[78], Colombia[79] and Peru[80] have "habeas data" rights in their constitutions, and have specific laws in various stages of development. Mexico is still considering a law.[81] These will not be discussed here. Also due to

[71] Prior to May 1, 2004 the members of the European Union were Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, Netherlands, Portugal, Spain, Sweden and the United Kingdom. On May 1, 2004 Cyprus, Czech Republic, Estonia, Hungary, Latvia, Lithuania, Malta, Poland, Slovakia and Slovenia joined. This discussion is based the laws of the member states prior to May 1, 2004. Further in Germany and Austria, because of their federal structure, each of the 16 German Länder (or states) and the 7 Austrian Länder have data protection laws, and in Germany and Austria organizations must determine which state law will govern their conduct. Spain, despite having autonomous regions, has a single unified law.

[72] *Computer-Processed Personal Data Protection Law* (, or "diannao chuli geren ziliao baohu fa"). There are currently proposals to expand it.

[73] *Personal Information Protection Law*, passed May 23, 2003.

[74] *Citizens' Privacy Bill Proposed by Ministry*, JoonAng Daily, June 1, 2004.

[75] *Ley sobre Protección de la Vida Privada,* Law No. 19628 of August 30, 1999, Oficial Journal August 28, 1999.

[76] *La Ley 25.326 sobre Protección de Datos personales y acción de habeas data,* enacted October 4, 2000, partial promulgation October 30, 2000.

[77] See Articles 18, 19 and 43 of *Constitution de la Nación Argentina* (1994). Article 43 (the "habeas data" right) provides that "Every person may file an action to obtain knowledge of the content and purpose of all the data pertaining to him or her containe din public records or databanks, or in private ones whose purpose is to provide reports; and in the case of falsehood of information or its use for discriminatory purposes, a person will be able to demand the deletion, correction, confidentiality or update of the data contained in the above records. The secrecy of journalistic information sources may not be affected."

[78] Article 5 of the 1988 Constitution of Brazil.

[79] Article 15 of the Constitution.

[80] Article 2 of the Constitution of Peru (1993).

[81] Personal Communication.

space constraints, there will be no discussion of specific privacy laws, such as laws regulating spam.

A. The European Data Protection Model

1. General Introduction

As Warren and Brandeis noted in their seminal 1890 article, "The Right to Privacy" [82], on the balance between free speech and privacy, at that time the right to privacy had already found expression in the law of France, and specifically in the *Loi relative à la presse du 11 mai 1868.*[83] Some, but not all, European countries were early adopters of privacy and data protection laws.

The first law attempting to regulate the collection and use of personal information in computer files was adopted by the German state of Hesse (the area around Frankfurt-am-Main) in 1970[84], and the first national law was adopted by Sweden in 1973.[85] France adopted a national law on data protection in 1978.[86] But other jurisdictions in Europe, despite their close relationship with these countries, and the use of a civil law model derived from the laws of either Germany or France, did not adopt privacy or data protection laws until relatively recently.

For example private sector data protection was introduced in Italy in 1996,[87] and then further developed in a comprehensive privacy code that came into force on January 1, 2004.[88] Spain adopted a law in 1999,[89] and Luxembourg was among the last to adopt a law in August 2002.[90]

The differing rules for the protection of personal information in the European Union interfered with the ability of retailers in particular to operate through the E.U., thus jeopardizing the establishment and functioning of the internal market that is one of the primary goals of the E.U.

---

[82] Samuel D. Warren and Louis D. Brandeis, *The Right to Privacy*, Harvard Law Review, Vol. IV, No. 5 (December 15, 1890).

[83] Currently Article 9 of the French *Code Civil* (which Article had its origin in the *Loi du 22 juillet 1893)* states that "Chacun a droit au respect de sa vie privé", or "Each person has a right to the respect of their private life." This right encompasses protection against attacks on the name, image, voice, privacy, honour and reputation, and biography of an individual.

[84] Now part of *Hessisches Datenschutzgesetz* (HDSG) in der Fassung vom 7 Januar 1999.

[85] *Datalagen*, SFS 1973:289

[86] *Loi No. -78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.*

[87] Law No. 675/1996. *Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali* (Protection of individuals and other subjects with regard to the processing of personal data).

[88] *Codice in materia di protezione dei dati personali* (Personal Data Protection Code), Decreto legislative n. 196 del 30 giugno 2003 (Legislative Decree no. 196/2003).

[89] *Ley Orgánica 15/1999, de 13 diciembre, de Protección de Datos de Carácter Personal.*

[90] *Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel.*

Accordingly, the European Parliament and Council adopted what has since become known as the "European Data Directive"[91] to require the member states to harmonize their laws. It was the adoption of the European Data Directive that led to the adoption of data protection laws in Italy, Spain and Luxembourg.

The European Data Directive thus became the model for all data protection laws of its member states, although only the laws of the individual member states are actually effective and enforceable in a jurisdiction. There are a number of features of the European model of data protection that distinguish it from other models to some degree, and should be noted in order to more easily review and understand the model.

As it arose specifically out of concerns about the use of computers to collect and store personal information on a scale not previously experienced, Article 3 of the Directive limits the scope of application of the Directive to "…the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system." Thus member states are not required to provide protection for personal information that is collected manually other than as part of a filing system.[92]

In much of privacy and data protection law, distinctions are made between the laws applying to the public sector and those applying to the private sector. In Canada, the privacy protection for personal information collected and used by the public sector is generally dealt with in 'Freedom of Information' legislation that is separate from the private sector legislation. In Australia the two are combined into one statute, but operate relatively independently. The European Data Directive applies to the processing of personal information in both the private sector and the public sector (except for criminal and security matters), and the provisions applying to the two sectors are fully integrated. Consequently, care must be taken when reviewing European laws to be sure that it is clear that the relevant provision applies to the private sector, and not just the public sector.

Otherwise, the European Data Directive requires that personal information be collected only for specified, explicit and legitimate purposes, that excessive data not be collected, that the data be accurate and where necessary kept up to date, and be kept for no longer than is necessary.

---

[91] *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, Official Journal L281, 23/11/2003 p. 0031-0050.

[92] The concept of a "filing system" is defined in Article 2(c) of the Directive thus: " 'personal data filing system' (filing system) shall mean any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographic basis." The concept was considered in the U.K. case *Michael John Durant v. Financial Services Authority* [2003] EWCA Civ.1746, Court of Appeal (Civil Division), December 8, 2003. The decision in this case has since caused the U.K. Information Commissioner and the Irish Data Protection Commissioner to issue guidances on what is "manual data" and what is a "relevant filing system." Some regard this decision and the guidances as restricting the application of the U.K. *Data Protection Act 1998* to apply only to computerized personal information which focused on a living individual in a biographically significant way. In May 2004 Mr. Durant filed papers with the European Commission in Brussels claiming that the U.K. Government had not implemented the European Data Directive properly and the European Commission has now asked the U.K. Government to justify its approach (see " UK's data Protection Act might not meet European Union standards" *OUTLAW.COM* , May 19, 2004 and " European Commission suggests UK's Data Protection Act is deficient" *OUTLAW.COM*, July 15, 2004).

Data may only be processed if the data subject has unambiguously given his or her consent or the processing fits within certain other categories set out in Article 7 of the Directive. Article 10 specifies the information that must be given to a data subject, such as identity of the data controller and the purposes for the processing, and Article 12 specifies the data subject's rights of access to data relating to him or her. The data subject also has certain rights to object to the data being processed. And, of course, the data must be kept confidential and secure.

Article 8 prohibits the processing of special categories of data that reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life, unless the processing fits within certain specific exceptions, one of which is if the data subject has given explicit consent. These may be described as "sensitive areas" of personal information. In the opinion of some, the concept of "sensitive information" is key to the effective application of privacy principles to particular situations, and the use of appropriate forms of consent. However, the concept is not defined in Canadian privacy law, for example.

With respect to the consent of the data subject to collection and processing of personal information, the Directive specifies that certain minimum information must be given to the data subject to ensure that the consent is properly obtained.[93] But the provisions in national laws vary significantly in this area. In the Netherlands and the U.K. the requirements are deliberately not specified and an obligation is placed on the data controller to disclose any further information that is necessary, having regard to the specific circumstances in which the data are to be processed, to enable processing in respect of the data subject to be fair.[94] In essence, the requirement is for the disclosure of all things that the data subject would consider relevant in deciding whether or not to consent to such activity.

Generally, the information that must be provided includes the identity and address of the data controller(s) and their representative, the purpose of the processing, the identity of the recipients or categories of recipients of the data, whether provision of certain information is voluntary or required, and the consequences of a failure to provide the information, and the existence of a right of access and a right to rectify data. The development of a form of consent for use across Europe requires the review of each jurisdiction's requirements, and cannot be prepared based only on a review of the Directive.

2. Notification to the Data Protection Authority in Advance

One of the most significant aspects of the European Data Directive is the requirement for notification to the data protection authority by a data controller before processing may commence, as set out in Article 18. The contents of such notification are specified in Article 19. The purpose of such notification is to allow the data protection agency to assess the risk posed to the rights and freedoms of the data subjects by the proposed processing, and to post such information in a national register accessible to all. While this process is intended to be simple and easy to comply with, in practice notification can be more involved and is likely to be the part of the law that a franchisor will have the most contact with.

---

[93] Articles 10 and 11.

[94] Section 2(3) of Part II of Schedule I to the Data Protection Act 1998 in the U.K.; Article 33 of the *Wet bescherming persoonsgegevens* in the Netherlands.

Firstly, data processing is not supposed to start until notification is complete. Different data protection authorities have different positions on when this occurs. The U.K. Information Commissioner takes the position that the notification is complete when a completed form has been filed and the fee of 35 pounds paid, even though it may be some weeks before a receipt is issued. But the College Bescherming Personsgegevens in the Netherlands takes the strong position that processing can not begin until the receipt has been received by the data controller, which in their jurisdiction may not occur for more than a month.

Data controllers such as a foreign franchisor will have to appoint a local representative and name such person on the notification form. Many data protection authorities in Europe have set up web sites where either the forms can be downloaded, or even completed and submitted online. And to assist foreign data controllers with their notifications, a growing number of data protection authorities provide English language translations of their laws and the guidelines for notification. However, the actual notification form is always in the national language, as is any correspondence with the authority.

There may also be a question as to who is a data controller, and who therefore has to be included in the notification. The Directive states that:

> 'controller' shall mean the natural or legal person , public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; [95]…

The precise wording of the definitions varies in the national laws of the member states. Some specifically include all data processors, if not already included as controllers.[96] If an American franchisor wanted to operate an international promotional contest from its head office in the United States, using its local franchisees to do some of the processing in their home jurisdiction, it may be necessary to list both the franchisor and franchisees on the notification.

The penalties for failing to notify, as set out in the various laws, are fairly significant, and constitute a substantial incentive to fully comply with the notification requirements. Remedies and penalties are not dealt with in the Directive, but rather in the national laws. Generally these laws provide for a fine for failing to notify or for supplying incomplete or inaccurate information, and make it an offense punishable by a fine or imprisonment where the failure is deliberate.[97]

3. Transfer of Personal Data outside of the European Union

One of the concerns in privacy law generally is ensuring compliance, and compliance cannot be ensured if the personal data can be freely transferred outside the jurisdiction of the privacy law. Such transfers are particularly easy with respect to information. For this reason the European

---

[95] Article 2(d).

[96] See for example Germany's *Bundesdatenschutzgesetz,* Section 4e(2); Luxembourg's *Loi du 2 août 2002*, Article 13(1)(a).

[97] See for example the Netherlands' *Wet bescherming personsgegevens*, Articles 27 and 28 in the first instance, and Article 75(2) where the failure is deliberate.

Data Directive requires that the member states restrict such transfers to third countries that ensure an adequate level of protection.[98]

There are provisions in the Directive for the assessment of third countries privacy laws, and the European Commission has investigated and issued decisions recognizing that Switzerland, Hungary, Canada, Argentina and the U.S. Department of Commerce's Safe Harbor Privacy Principles, as providing adequate protection.[99] These approvals are often qualified depending upon the scope of the privacy law. In the case of Canada the approval is limited to "…recipients subject to the Personal Information Protection and Electronic Documents Act."[100] The decision provides for a review three years after its notification to the member states.

The Directive also provides for derogations from the requirement that the third country have an adequate level of privacy protection.[101] For a foreign franchisor the exceptions of primary relevance are where:

(a) the data subject has given his or her unambiguous consent;[102]

(b) the transfer is necessary for the conclusion or performance of a contract between the data subject and a controller; and

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of a data subject between a controller and third party.

There is also a derogation to allow a member state to authorize a transfer to a third country if the data controller has ensured an adequate level of privacy protection for the individuals concerned by contractual means. However the local data protection authority is to inform the European Commission regarding each of these transfers, and the Commission reserves the right to object to the transfer. There are serious concerns that not all of these arrangements are being reported. [103]

---

[98] Article 25.

[99] "Commission decisions on the adequacy of the protection of personal data in third countries", available at *http://europa.eu.int/comm/internal _market/privacy/adequacy_en.htm*.

[100] 2002/2/EC Commission Decision of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act (notified under document number C (2001) 4539), *Official Journal L* , 04/01/2002 p. 0013-0016.

[101] Article 26.

[102] As always the law of the jurisdiction should be consulted for the precise wording of the requirement. For example in the U.K.'s Data Protection Act 1998*,* the wording in Schedule 4 regarding the consent required does not use the word "unambiguous."

[103] The first Commission Report on the implementation of the European Data Directive issued May 15,2003 stated that "many unauthorized and possibly illegal transfers are being made to destinations or recipients not guaranteeing adequate protection" (at page 19). As evidence of this was the very limited number of notifications received pursuant to Art. 26(3) of the Directive. Accordingly on August 21, 2003 a notice was sent out reminding national data protection authorities of the reporting requirements.

As a further option the Commission has approved a set of standard contractual clauses for the transfer of data to processors in third countries.[104] These may be used independently or included as part of larger contract. They are an option to assist persons doing business in the E.U. and are not a requirement nor a minimum standard. The advantage is that member states are required to recognize the clauses as providing adequate protection. The clauses also have a restriction regarding onward transfer to countries that do not have adequate protection.

Because the United States has taken a different approach to privacy protection and as such would not be considered as a jurisdiction having adequate protection by the E.U., there was considerable concern that the European Data Directive would become a trade barrier for American companies wishing to do business in the E.U. Negotiations were undertaken between the E.U. and the U.S. Department of Commerce that resulted in the development of the Safe Harbor Principles and the system of self-certification of adherence to the principles.[105]

Organizations wishing to self-certify must be subject to the jurisdiction of either the Federal Trade Commission or the U.S Department of Transportation.[106] They will have to develop a privacy policy that contains the Safe Harbor Principles and appoint a person to administer the policy. The Safe Harbor Privacy Principles consist of seven stated principles entitled Notice, Choice, Transfer to Third Parties, Security, Data Integrity, Access and Enforcement. The policy must also specifically state that the organization adheres to the Safe Harbor Principles, which then becomes a representation to the public, as the policy must be made publicly available.

Finally, under the enforcement principle, the organization must establish an independent recourse mechanism to which individuals can turn for the investigation of unresolved complaints. While it was initially anticipated that most participants would choose organizations such as TRUSTe, BBBOnline, the American Arbitration Association or JAMS, which have developed Safe Harbor compliance programs, a review of the list of participants suggests that a large number have chosen to co-operate with European Data Protection Authorities.

On submission of the self-certification form to the U.S. Department of Commerce, the materials are reviewed for completeness before being posted on the Safe Harbor list. As of July 23, 2004 there were 538 companies listed as adhering to the Safe Harbor Principles. While many privacy advocates have commented on the low rate of participation, this is an increase of almost 200 companies over the previous year's total.

One of the reasons may be that some Europeans, including some representatives of data protection authorities, mistakenly view Safe Harbor adherence as a requirement for American

---

[104] Commission Decision of 27 December 2001 on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC. The "Standard Contractual Clauses (processors)" are attached to the decision as an annex. The are available at *http://europa.eu.int/comm/internal_market/privacy/modelcontracts_en.htm*.

[105] Information about the Safe Harbor is available online at: *http://www.export.gov/safeharbor/index.html*, including the list of corporations that have self-certified and advice on how to self-certify. The self-certification form may be completed online.

[106] For a broader discussion about privacy and the Safe Harbor program, see Charles B. Cannon, "What Franchisors Need to Know About Privacy Rights, a Safe Harbor, and Standard Contractual Clauses Before Exchanging Personal Information with Europeans", *Franchise Law Journal* 176 (Winter 2003).

companies, even if for example the data subject has unambiguously given his or her consent to the transfer of their personal information to the United States. In other words, instead of being a legal alternative, adherence to the Safe Harbor Principles appears to be becoming a marketing or public relations requirement for American companies wishing to transfer personal information on Europeans to the U.S. However, concerns have been expressed about whether all listed companies are truly adhering to the Safe Harbor Principles, as a review indicated that less than half the privacy policies met the standards expressed in the Principles.[107]

4. Some Concluding Thoughts

Europe is often considered to be the leader in data protection law. Certainly it has some of the first laws, and, on paper at least, some of the strictest laws. But the enforcement and awareness of these laws is surprisingly weak. In 2003 there were cases in Sweden[108] and France[109] in which fines of about $500.00 U.S. were imposed for failure to notify the data protection authorities or obtain consent for the use of personal information. It was considered that these cases were notable because they may signal a new approach to enforcement. Generally it is felt that the national data protection agencies are not well funded and have therefore not been vigorous about enforcement.

In contrast, consider how many privacy enforcements have been undertaken in the United States by the Federal Trade Commission, and the class actions that have been filed, despite the absence of a private sector privacy law of general application. Some suggest that as a result American companies are more aware of the potential for privacy complaints than European companies. Certainly not all European counsel are thoroughly familiar with the requirements of their national data protection laws.

Another explanation that has been suggested for these phenomena is that in countries where privacy protection is a relatively recent development, lawyers and regulators are concerned about rights and responsibilities that they are not yet fully comfortable with, while jurisdictions with a long record of data protection feel comfortable with things proceeding as before. But data protection and concerns about privacy are unlikely to remain as before.

---

[107] Rosemary Jay and Angus Hamilton, *Data Protection: Law and Practice – Second Edition*, 227 (London: Sweet & Maxwell, 2003), based on an interim working paper from the E.U. issued February 13, 2002.

[108] *Sweden v. Bodil Lindqvist*, Case C-101/01 (E.C.J. November 6, 2003). Ms. Lindqvist was a volunteer on a church committee. In furtherance of her volunteer work she set up a web site that the church recognized and used. To make her committee appear more approachable she gave personal details about some of the members, including that one had hurt her foot and was off work. When there were complaints she immediately removed the information. Nonetheless criminal proceedings were commenced and she was fined 4,000.00 Swedish Kroner.

[109] *Procureur general pour le Procureur de la République de Villefranche sur Saône c. Roger G.*, Septième Chambre de la Cour d'Appel de Lyon, E.R. 390/03, 25 février 2004. The defendant maintained a web site critical of the Church of Scientology. As part of his commentary he posted personal information about an individual. There was a complaint, and he was fined 450 Euros for failing to send a notification to the Commission Nationale de l'Informatique et Libertés, also known as the "CNIL", the French data protection authority.

B. The British Commonwealth Data Protection Model

In contrast to the rest of Europe, in the U.K. the basic common-law principle was that there was no right to privacy nor any action for invasion of privacy per se. And in countries that adopted the English common-law system, there has been a reluctance to found liability on a privacy right alone. Often the issue was avoided by the use of the more established categories of torts.

In the United Kingdom, the clash of its traditional approach with its membership in the European Union has led to it having both a data protection law, and a debate about whether there is a right to privacy in the U.K.[110] But in countries such as Canada and Australia, New Zealand and in Hong Kong SAR, there may be developing a model for privacy protection that is somewhere between the approaches found in the United States and Europe. For the purposes of this paper it has been labeled the "British Commonwealth" model for the sake of convenience, although the appropriateness of the term may be questionable. There is no explicit link between the jurisdictions such as there is in Europe.[111] Rather, they are bound by a common language and legal heritage, and by the fact that they have adopted privacy laws with similar features.

As has been stated earlier, the general structure of private sector privacy laws is similar in most jurisdictions. The variations usually arise in issues regarding remedies and enforcement. Privacy laws in this group tend to have the following features:

1. There are no requirements to register with, or notify, the privacy commissioner, as there are in Europe.

2. Restrictions on transfers out of the jurisdiction are not as strongly enforced as in Europe.

3. There are usually no fines or criminal penalties for breach of privacy (but Hong Kong SAR and New Zealand may be the exception).

Thus a foreign company wishing to collect, use or disclose personal information about residents of these jurisdictions has no formalities with which to comply. The organization must simply ensure that it has a privacy policy in place that complies with the national and/or state laws (Canada and Australia are federal countries) and that its methods for obtaining consent meet the required standards.

1. Canada

Canada is a federal state, and its constitution presented major problems in the development of a co-ordinated approach to private sector privacy protection. There currently four private sector privacy laws of general application in effect in Canada, as follows:

---

[110] See *Campbell v. Mirror Group Newspapers Ltd.*, [2003] 1 All ER 224 at 61, and *Douglas v. Hello,* [2003] EWHC 786 (Ch) (11 April 2003).

[111] Some of the other Commonwealth countries that might qualify for this group, such as India, Malaysia, South Africa and Singapore, either are still developing privacy laws or have made a decision not to adopt mandatory private sector privacy protection.

1. *Personal Information Protection and Electronic Documents Act*, ("PIPEDA") adopted by the federal Parliament on April 13, 2000, that came into force in stages on January 1, 2001 and January 1, 2004.

2. *Loi sur la protection des renseignements personnels dans le secteur privé* (An act respecting the protection of personal information in the private sector), that came into force in the Province of Québec on January 1, 1994.

3. *Personal Information Protection Act*, which came in to force in the Province of British Columbia on January 1, 2004.

4. *Personal Information Protection Act*, which came in to force in the Province of Alberta on January 1, 2004.

In addition the provinces of Alberta and Manitoba have health sector specific privacy protection in force, and Saskatchewan and Ontario have passed such legislation but the laws are not yet in force. And in Québec the new Code Civil that came in to force January 1, 1994 also provides for privacy protection in Article 35. [112]

Unlike the Constitution of the United States, Canada's Constitution[113] requires that the powers of the federal and provincial governments be mutually exclusive. Privacy as a subject is not mentioned in the Constitution, and accordingly there is some debate as to which government has the power to legislate in this area. When the federal government adopted PIPEDA, it relied on its 'trade and commerce power', and a recent Supreme Court of Canada decision[114] that had expanded the ability of the federal government to use the trade and commerce power to legislate national regulatory schemes, particularly if the provincial governments did not adopt similar legislation. For this reason PIPDEA first came into effect for international and interprovincial matters[115] in 2001, and for matters entirely within a province that had not adopted substantially similar legislation, in 2004.

The exemption for provinces that have substantially similar legislation requires that the federal government pass a regulation to give effect to the exemption. This has been done with respect to Québec's law, has not yet been completed with respect to the laws in B.C. and Alberta. Currently therefore companies conducting business in these provinces must comply with both PIPEDA and the provincial law even though the matter occurs entirely within the province. [116]

---

[112] Article 35 provides as follows: " Toute personne a droit au respect de sa réputation et de sa vie privée. Nulle atteinte ne peut être portée à la vie privée d'une personne sans que celle-ci ou ses héritiers y consentent ou sans que la loi l'autorise. Every person has a right to the respect of his reputation and privacy.

No one may invade the privacy of a person without the consent of the person unless authorized by law."

[113] Now embodied in the *Constitution Act 1867*, (U.K.), 30 &31 Vict., c.3.

[114] *General Motors v. City National Leasing,* [1989] 1 S.C.R. 641.

[115] Including the federally regulated territories of the Yukon, Nunavut and the Northwest Territories.

[116] On July 27, 2004 the Office of the Information and Privacy Commissioner of Alberta posted on its web site a document entitled *Questions and Answers regarding the application of PIPEDA, Alberta and British Columbia's*

In all other provinces, PIPEDA applies to commercial matters both within the province and interprovincially or internationally. But because of the limitations on the federal power as imposed by the Constitution, PIPEDA does not apply within these provinces to provincial matters such as employment relations, charities and their fundraising, and aspects of the health sector. There is no policy reason for these exemptions for privacy protection, and it is expected that in the future, particularly in Ontario, the situation will be corrected, especially with respect to employment.

The substantive provisions to PIPEDA are in a voluntary code[117] that is attached as a schedule to the abbreviated statute that converts the model code into a law. There are ten privacy principles, as follows:

1. Accountability
2. Identifying Purposes
3. Consent
4. Limiting Collection
5. Limiting Use, Disclosure, and Retention
6. Accuracy
7. Safeguards
8. Openness
9. Individual Access
10. Challenging Compliance

In genera,l in Canada the consent of the individual is needed for the collection, use or disclosure of personal information, unless there is a specific exemption from the consent requirement in the legislation. Care should be taken as to jurisdiction in relying on these exemptions because there are differences between PIPEDA and the laws in the provinces. Unlike the provisions under the Gramm-Leach-Bliley Act in the U.S. ,[118] consent may only be obtained for reasonable purposes.[119] This imposes limitations on the uses for which the information may be collected. Broad and opened purposes will be considered unreasonable.

The nature of the consent required varies with the sensitivity of the information and the context, but none of Canada's laws include any guidance as to what personal information will be considered sensitive, and in what circumstances is it more likely to be considered sensitive. Both opt-out and opt-in consent may be used, depending on the circumstances.

As in Europe, there are variations with respect to enforcement. The Privacy Commissioner of Canada has the power to investigate a complaint but does not have the power to make binding decisions. If the organization disagrees with the decision it need not respond, and if the

---

Personal Information Protection Acts (PIPAs) that was prepared in consultation among the offices of the privacy commissioners of Alberta, British Columbia, and Canada. Jurisdiction will depend on the nature of the complaint and where it occurred. It is possible that more than one privacy commissioner will have jurisdiction. The web site is http://www.oipc.ab.ca

[117] The Canadian Standards Association Model Code for the protection of Personal Information.

[118] 15 U.S.C. §§ 6801-6809.

[119] See Section 5(3) of PIPEDA, Section 11 of the B.C. and Alberta laws, and Article 4 of Québec's law.

complainant disagrees, or wishes to be awarded damages, the complainant must start over in Federal Court.[120] In contrast the provincial privacy commissioners can make binding decisions as to the existence of a breach, and make orders to correct such breach[121], but not award damages. To obtain an award of damages, the complainant must go to court and prove such damages.

PIPEDA is silent with respect to the transfer of personal information outside of Canada, which is interesting given the fact that the E.U. has ruled that PIPEDA provides adequate protection. Transfers outside of Canada are thus governed by the requirements that the purpose be reasonable, and that consent be obtained. If the transfer is to a third party processor on behalf of the organization, the information must be protected by a written contract.[122] The practice is not to specifically disclose the location or identity of such suppliers, but to state that suppliers are used. Other transfers outside of Canada may need to be specifically disclosed.

Concern in Canada is developing over the transfer of personal information to the United States under the provisions of the Patriot Act.[123] On July 23, 2004 the Government of British Columbia announced plans to introduce rules forbidding Canadian subsidiaries of American companies from handing over private information to American law enforcement agencies. [124]

It is not clear in Canada that there is a common law right of privacy or cause of action for breach, outside of Canada's privacy laws and outside of Québec. In a recent decision regarding employee rights in Alberta, the judge found that:

> In my view, there is no general right to privacy. Privacy was historically protected by the nuanced operation of the laws of property and trespass and, more recently the laws of harassment. Privacy is an aspect of both ss. 7 and 8 of the Charter. However, neither provision creates a general right of privacy. Rather, the right created is the right to be free of unreasonable state invasion of a reasonable expectation of privacy. [125]

---

[120] See Sections 11 to 17 of PIPEDA inclusive.

[121] See for example Sections 45 – 53, and Section 57 of the B.C. law, Sections 45 – 54 , and Section 60 of the Alberta law. Section 57 of the B.C. law provides that if the order of the commissioner becomes final the complainant "…has a cause of action against the organization for damages for actual harm that the individual has suffered as a result of the breach by the organization of obligations under this Act…".

[122] Paragraph 4.1.3 of Schedule 1 to PIPEDA.

[123] See Office of the Information and Privacy Commissioner for British Columbia, "BC Privacy Commissioner to Examine implications of USA *Patriot Act* on Government Outsourcing", Press Release dated May 28, 2004; Michael Geist, *U.S. Laws Put Canadian Privacy at Risk*, Toronto Star, July 26, 2004; Michael Geist and Milana Homsi, *The Long Arm of the USA Patriot Act: A Threat to Canadian Privacy?- A Submission on the USA Patriot Act to the B.C . Information and Privacy Commissioner,* July 2004, available at *http://www.michaelgeist.ca*.

[124] *B.C. to Guard Privacy Against Patriot Ac*", CBC.ca News, July 24, 2004.

[125] *ATU (Local No. 569) v. City of Edmonton*, 2004 ABQB 280 (Issued April 13, 2004 by the Court of Queen's Bench of Alberta). The question was whether in an arbitration under the Alberta *Labour Relations Code* the employer could rely on video tape evidence obtained surreptitiously.

To assist in the development of a common law tort of invasion of privacy, four provinces have passed legislation simply providing that it is "…a tort, actionable without proof of damage, for a person, willfully and without claim of right, to violate the privacy of an individual." [126] However, these statutes have been rarely relied upon. One of the reasons may be that in each province actions for invasion of privacy must be brought in the superior trial court of the province, which requires significant initial expenditure by the complainant. But damages in privacy actions are uncertain. Damages are dependent on the facts in each particular case, and precise calculations in advance may not be possible.

A franchisor wishing to comply with Canada's privacy laws will need to ensure that it has a privacy policy that complies at a minimum with PIPEDA, that it has appointed a privacy officer and that its privacy notices provide the information required by Paragraph 4.8.2 of Schedule 1 to PIPEDA.[127] There are no requirements to appoint a local representative. And there are no specific restrictions regarding the onward transfer of personal information to third countries, provided that such transfer is reasonable and consent to the transfer has been obtained.

2. Australia

Although Australia, like Canada, is also a federal state, private sector privacy protection is provided primarily by the federal *Privacy Act 1988*[128] as amended by the *Privacy Amendment (Private Sector) Act 2000*, which came into effect December 21, 2001. It was motivated by concerns regarding the implementation of the European Data Directive, among other things. *The Privacy Act 1988* was originally the public sector privacy legislation, but now includes both.

Despite this motivation the *Privacy Act 1988* is limited in its application to small businesses. Businesses with an annual turnover of less than $3 million Australian annually do not have to comply unless they trade in personal information, are related to a larger business, provide a health service or are a contractor to a Commonwealth (federal) agency. Further problems arise because personal information of employees regarding their present or past employment is not covered. In 2001, the Article 29 Data Protection Working Party of the European Commission issued an opinion recommending further work to seek improvements.[129] In other words, the provisions of the *Privacy Act 1988* were not considered to provide adequate protection. In

[126] British Columbia in 1968, see the *Privacy Act*, R.S.B.C. 1979, c.336; Manitoba in 1970, see *The Privacy Act*, R.S.M. 1970, c.74; Saskatchewan in 1974, see *The Privacy Act*, R.S.S. 1978, c.P.24; and Newfoundland in 1981, see the *Privacy Act*, R.S.N. 1990, c.P-22. These were based in part on Sections 50 and 51 of the New York Civil Rights Law.

[127] Paragraph 4.8.2 requires the provision of contact information for the privacy officer, the means of gaining access to personal information held by the organization, a description of the type of information held and its use, copies of general brochures explaining the privacy policy, and what personal information is made available to related organizations.

[128] Act No. 119 of 1988 as amended.

[129] The Working Party on the Protection of Individuals with regard to the Processing of Personal Data, *Opinion 3/2001 on the level of protection of the Australian Privacy Amendment (Private Sector) Act 2000,* Adopted on 26th January 2001.

September 2003 it was reported that the E.U. would reconsider Australia's privacy laws. In the meantime there are no reports of trade having been affected. [130]

The private sector amendments introduced a set of ten "National Privacy Principles" (NPPs) that set out minimum standards for the handling of personal information. They are described as Collection, Use and Disclosure, Data Quality, Data Security, Openness, Access and Correction, Identifiers, Anonymity, Transborder Data Flows and Sensitive Information. The amendments also introduced the option of businesses being regulated by privacy codes developed by their sector, provided that such codes contain the minimum requirements found in the NPPs, and have been approved by the Privacy Commissioner.[131] Currently there are approved codes for the market and social research sector, insurance, and Clubs Queensland. Three more codes are under consideration for casinos, the internet industry, and the Biometrics Institute.

The NPP with respect to Transborder Data Flows specifies that an Australian organization may only transfer personal information to a foreign country if it reasonably believes that the recipient organization is subject to a law, binding scheme or contract that has substantially similar principles, or the individual consents, or other exceptions similar to the requirements of the European Data Directive.

Individuals may complain to the Privacy Commissioner and in accordance with Section 52 the Privacy Commissioner can, after investigating a complaint, make a declaration regarding anything required to remedy a breach, including specifying the amount of damages and costs. The damages may include injury to feelings or humiliation. However the determinations of the Privacy Commissioner may only prohibit future conduct by a private sector organization.[132] Otherwise, application must be made to Federal Court[133] to enforce a determination of the Privacy Commissioner.

Like Canada, Australia did not previously have a common law tort of invasion of privacy. This appears to be changing as the result of the decision in *Grosse v. Purvis*[134] to award damages for the invasion of privacy by a man who stalked his former girlfriend. This was considered the first time that a right to privacy had been upheld at common law rather than under a statutory privacy regime. Previously common law complaints had to be fitted into another recognized tort. The decision is under appeal.

3. Hong Kong Special Administrative Region (SAR)

The final example of privacy laws of this type is from a jurisdiction that is actually part of a civil law country, the People's Republic in China. The *Personal Data (Privacy) Ordinance*[135] came

[130] Simon Hayes, *EU Renews Attack on Privacy*, Australian IT, September 16, 2003.

[131] See Sections 18BA to 18BI.

[132] See Section 52(1B) and Section 55(1).

[133] Section 55A.

[134] [2003] QDC 151(16 June 2003) (District Court of Queensland).

[135] Chapter 486.

into force December 20, 1996, just over six months before the region was handed over to the PRC on July 1, 1997. Through January 2003, there have been over 98,000 enquiries, 3,400 investigated complaints, and 55 appeals heard by the statutory Administrative Appeals Board. [136]

The Ordinance applies to both computerized and manually held data, and to both the private and public sectors. While provisions exist for the establishment of a Register of data users[137], the Commissioner has not yet specified a class of data users for which registration will be required.[138] The privacy principles are given in Schedule 1 to the Ordinance. They are:

1. Purpose and manner of collection of personal data
2. Accuracy and duration of retention of personal data
3. Use of personal data
4. Security of personal data
5. Information to be generally available
6. Access to personal data.

The Privacy Commissioner has a central but not exclusive role in applying the Ordinance. Aggrieved persons are not required to complain to the privacy Commissioner. They have the alternative of first approaching the courts. If monetary damages are sought that is the recommended route. [139]

The Ordinance was adopted with provisions restricting transfers of personal data outside of Hong Kong SAR except in specified circumstances, but the section has never been brought into force.[140] The special circumstances permitting transfer out of the jurisdiction included the consent in writing of the data subject, the organization has reasonable grounds for believing that the receiving jurisdiction has a substantially similar law in place, and that the organization had taken all reasonable precautions and exercised all due diligence to ensure the same protection to the data as it would receive in Hong Kong.

The Ordinance has further similarities to the European model in that it prescribes the act of knowingly or recklessly supplying false or misleading information on a data return as an offence under the Ordinance. However, as noted earlier, currently no group of organizations has an obligation to file data returns.

It is an offense for an organization to contravene an enforcement notice or any other provision of the Ordinance, and in certain circumstances individuals may be held liable, as well as their

[136] Raymond Tang, Privacy Commissioner for Personal Data for Hong Kong SAR, "Foreword" in Mark Berthold and Raymond Wacks, *Hong Kong Data Privacy Law-Territorial Regulation in a Borderless World: Second Editiion* (Hong Kong: Sweet & Maxwell Asia, 2003).

[137] Section 15.

[138] As required under Section 14. See also Berthold and Wacks, *supra* note 136 at p. 312.

[139] Berthold and Wacks, *supra* note 136, at p. 204. See also Section 66(1).

[140] Section 33. See also Berthold and Wacks, *supra* note 136 at p. 269.

organization. The levels of the fines are found under the *Criminal Procedure Ordinance*.[141] The principles are set out in Schedule 1 and are thus not a provision of the Ordinance. In other words it is not an offence to breach the privacy principles, but it is an offense to breach an order of the Privacy Commissioner enforcing a privacy principle.

In resolving complaints the Privacy Commissioner has, and often uses, the opportunity to affect an informal resolution. However, where the Commissioner wishes to compel compliance, the Commissioner has the power to serve an enforcement notice[142] directing a specific remedy for the breach of a privacy principle. Failure to comply with an enforcement notice is a criminal offense punishable by two years imprisonment and a daily fine of $1,000.00 Hong Kong Dollars.[143] The Commissioner does not have the right to award compensation, but the Ordinance specifies that an individual who suffers damage by reason of contravention of a requirement under the Ordinance shall be entitled to compensation form the organization for such damage, including compensation for "…injury to feelings."[144]

The Ordinance was, not surprisingly, influenced by the European influence in the U.K. when it was drafted. It will be interesting to see how it fares as the influence of Hong Kong's return to China lengthens. The influence may be in either direction. The PRC is still preparing a draft of a comprehensive civil code for presentation to the National People's Congress. In December 2002, when it was rumored that a draft would be presented to the next meeting of the NPC in the spring, it was also rumored that the draft would contain clear provisions on the protection of the privacy of individuals.[145]

4. Some Concluding Thoughts

The "British Commonwealth Data Protection Model", a label invented for this paper, is obviously not a cohesive group. It is perhaps better described as the influence of the European Data directive on the privacy protection models adopted in countries having an English common law legal system.

The truly distinctive feature appears to be the lack of, or in the case of Hong Kong the unwillingness to implement, a notification or registration system. And to varying degrees these jurisdictions are not as restrictive as the European Data Directive with respect to transfers of personal information outside the jurisdiction. Together, these are very important distinctions for

---

[141] Schedule 8, or see Berthold and Wacks, *supra* note 136 at p.368.

[142] Section 50.

[143] Section 50.

[144] Section 66. Such damages were awarded in *Yuen Sha Sha v. Tse Chi Pan* [1998] Equal Opportunities Action No.1, DCE01/98 in the amount of $50,000.00HK (about $6,400.00 US) where a peeping tom video taped a student undressing. See also Berthold and Wacks, s*upra* note 136 at p. 372.

[145] *Civil Code Document Submitted*, China Daily, Beijing, December 24, 2002. See also Nailene Chou Wiest, *Draft Private Property Laws Debated,* South China Morning Post, Hong Kong, December 24, 2002, and *Private Property Owners Win with Reform*, People's Daily Online, Beijing, December 24, 2002.

franchisors and others wishing to implement marketing programs in these jurisdictions. A comprehensive and properly implemented privacy policy, such as might be prepared for adherence to the U.S. Department of Commerce's Safe Harbor Principles, or for use in Canada, would be largely compliant in these jurisdictions. Adjustments may of course, be necessary for particular issues and sensitivities.

VI. STRATEGIES FOR COMPLIANCE

A. Introduction

The primary effect of privacy laws on franchisors and the franchise systems arises out of their effect on marketing and customer relationship issues. Prior to the passage of privacy laws customer information could be collected, used and exchanged between franchisees and franchisors almost without restriction. Now all such activities in many parts of the world must have the consent, either explicit or implied, of the individual customers and transfers of customer specific information to the United States in particular must comply with national privacy requirements. The nature of the form of consent used must take into account the "sensitivity" of the personal information.Thus certain sectors, such as child care and financial services, will be affected much differently than vendors of hamburgers and pizza.

The international franchisee application forms of all franchisors will have to be revised to take into account the world's new privacy laws, and in particular, the notice provisions of the various laws. Consent can only be obtained for identified purposes. Some retail sectors are having difficulty training staff to effectively communicate the purposes for the collection and use of personal information.

Manufacturers and franchisors may no longer simply require by contract that their dealers and franchisees turn over customer information in order to build a customer database and ensure ownership of the customer list. Now the franchisee must obtain the consent of the customer not only to collect and use the information, but also obtain consent to disclose the information to its franchisor, and for the franchisor's proposed uses of the information. While consent to the collection and use of such information in a store may often be implied from the actions of the customers, the same cannot always be said for the disclosure to the franchisor. Further customers cannot be required to provide personal information beyond that "…..required to fulfill the explicitly specified, and legitimate purposes…." of a transaction.

Insofar as marketing programs are administered centrally by the franchisor, they will be affected by the new consent requirement. Examples include marketing surveys, warranty programs, direct mailing, contests and games, data mining, and customer support.

B. Basic Privacy Compliance

Set out below are what might described as the basic steps for any organization in developing and implementing a privacy policy. In the next sections there will be discussions on particular issues in implementation for franchisors, and some comments specifically on developing international compliance.

1. Appoint a Compliance Officer

The first step is to put someone in charge of the process, or at least to chose a coordinator, and have that person be the compliance officer required by privacy laws such as in Canada. The

individual should obtain copies of the relevant legislation and regulations, and knowledgeable legal and other support. The individual may then assemble a team to oversee and/or conduct the audit and implementation steps that will be described in the next sections. The Compliance Officer and her team should then develop a draft plan to implement policies and practices to comply, that will be finalized after the conduct of the audit.

The plan should address:

a) implementing procedures to protect personal information;

b) establishing procedures to receive and respond to complaints and enquiries;

c) training staff and communicating to staff information about the organization's policies and practices;

d) developing information and to explain the organization's policies and procedures; and

e) ensuring the accuracy of the personal information held by the organization and updating and retention policies.

2. Conduct a Privacy Audit

The purpose of the audit is to establish what personal information is currently being collected, used or held, or disclosed by the organization, and how it is currently stored and protected.

The audit should also identify all jurisdictions where personal information is being collected, as it may be necessary to comply with other privacy laws. For commercial organizations privacy issues arise in the following areas:

- marketing and sales
- human resources
- online operations (items such as cookies)
- government relations (lobbying)
- client or customer files
- security services

Particular care should be taken to identify personal information that is disclosed to subcontractors such as: employee information to payroll services, marketing information to ad agencies, information submitted on-line to service fulfillment providers or data analyzers, lobbying information to trade associations, and mailing information to outside mailing firms. Copies of the contracts with each subcontractor should be reviewed with respect to privacy protection.

3. Develop a List of Approved Purposes

After having conducted the audit, the organization should then examine the purposes for which it is collected, and the nature of the information collected, to determine the organization's long term policy as to purposes and the type of information that is truly necessary to fulfill those purposes. Many organizations have discovered that they are collecting more information than is reasonably necessary.

This information will not only become the basis for the drafting of the official privacy policies and guidelines, but also the various consent forms that will be used, or other methods of collection.

4. Prepare Privacy Polices, Brochures and Consent Forms

Having made decisions about the overall purposes for which the organization will collect personal information, the next step is to implement the decision by preparing the organization's privacy policies and guidelines. The preparation of consent forms or privacy statements for other collection methods will require decisions as to the degree of consent and disclosure required based on the sensitivity of the personal information being collected. Will explicit or implicit consent be used? How will the privacy policy be positioned on the home page of your website? Will a "click-through" consent be required?

5. Consider a New Filing System

Experience in other jurisdictions, such as Québec, has shown that one of the keys to low cost compliance with access requests is having a filing system that segregates personal information with respect to each individual according to the purpose for which the information was collected, yet has links and controls on the setting up of new files with respect to any individual. If files are computerized, this generally means that the databases in membership and other areas should be linked. Experience recently in the United States with respect to the Gramm-Leach-Bliley Act has suggested that where this linking is not done, or cannot be done, compliance will be lower and costs will be higher.

Not all purposes require the collection of equally sensitive personal information, and if all information regarding an individual is in one file, then that file must have safeguards appropriate to the most sensitive aspect of the file. If an access request is made, and there are grounds for denying access to one portion of the file, then the file will have to be reviewed item by item to determine what must be severed, and what may be disclosed to the individual.

6. Initiate the Privacy Plan

Obviously, the decisions mentioned earlier will have to be implemented. The implementation is often coordinated so that the organization is comfortable that from a certain date forward, the organization generally complies with the privacy requirements. It is also necessary to review existing files containing personal information and to either ensure that there is appropriate consent for the retention and use of the information, or that the information is safely deleted. This may require a mailing or other communication with the individuals to announce and explain the new privacy policy and obtain the new consent.

Implementation may also require changes to any websites that the organization has to ensure, among other things, that persons using the website have access to a copy of the privacy policy or statement every time personal information is submitted. At this point the required safeguards

for the personal information should be in place, whether physical, technological or in staff policies regarding employee access. The policy regarding the handling of complaints should be ready, as well as the policy on whether to charge any amount to individuals requesting access. Contracts with subcontractors should clearly spell out the compliance measures necessary on their part, and provide the organization with a right of audit.

7. Maintaining Compliance

Set out below are some of the things to be considered after implementation to maintain compliance with privacy laws and other privacy standards:

Policies should be developed to ensure that evidence and documentation exists for (a) each individual's consent, for each database and purpose; (b) all uses of, or disclosures from, each database are properly recorded and protected, and are in accordance with the purposes; (c) and reviews of the databases for accuracy in accordance with the sensitivity of the information.

Responsibility for compliance may be better separated from responsibility for collection, use and disclosure. Collecting, use, and disclosure should not be able to proceed without authorization from the compliance officer.

Provisions should be made for the regular training of new staff, and for review and update of the policies.

The development and application of privacy laws should be monitored, particularly as the business expands into new markets.

A response plan in the event of allegations of a privacy breach should be developed.

Provisions should be made for internal or external compliance audits.

C. Compliance Issues for Franchisors

The most fundamental decision to be made by a franchisor in implementing a privacy compliance program is the decision about the breadth of the program. Will there be one privacy policy and compliance program for the franchise system (that is including franchisees) or will the franchisor's privacy policy and compliance program be mandatory only for the franchisor, and franchisees will only be required to comply with the relevant privacy law. And if the privacy policy is system wide, will it be for customers only, or also for employees?

In making these choices, the franchisor will have to take into account the degree to which privacy is relevant to the customer satisfaction associated with brand, and the risk of the assumption of liability for non-compliance with the privacy policy by a franchisee. If a privacy policy is system wide, who will respond in the event of a compliant, and how will the costs of a defence be allocated? These issues should be worked out in advance.

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

For example, a financial services franchisor may consider that concerns about client privacy are a very real part of the services being offered, are accordingly there are significant marketing benefits that might arise from prominent and uniform approach. Implementation may not be as costly as some other sectors because financial professionals already conform to practices that ensure the confidentiality of client information. And, for the same reason, the increased risk of liability may not be significant.

On the other hand, generally little or no customer information is collected in the sale of hamburgers, and customer privacy is not generally considered part of the service. There would be considerable training costs to introducing privacy concepts and concerns to the franchisee's frontline staff. This would appear to be a system where the franchisor would be better off simply requiring franchisees to comply with all privacy laws.

But consider the marketing used by take-out or delivery pizza chains. Orders are generally made by telephone, and many pizza chains collect and maintain significant computerized databases regarding their customer's preferences and the frequency of purchases. Consent is now required to continue this practice. On the other hand, many individuals do not consider their preferences in pizza to be particularly sensitive personal information, and thus it may be possible to use implied consent to continue the marketing practices. If the franchisees accept payment by credit card over the telephone however, there are significant possible security and identity theft issues. How long is the card information retained? Is it adequately secured from theft? What is adequate security in the context of a pizza take-out store operated by teen-agers?

As has been noted earlier, the primary branding issue to be taken into account is the degree to which customers consider a certain level of privacy protection to be part of the image associated with the brand. However such associations may also be important for employee relations, if part of the branding image is that a franchisor is a progressive employer. Particularly relevant to the branding image will be clear communication as to the purposes for the collection, use or disclosure of personal information. As noted above, this has already proven to be a problem in some retail sectors.

Balanced against any benefits to be gained by having a uniform privacy policy are the costs of ensuring that the privacy policy is implemented uniformly by the franchisees, and the associated liabilities to the system and the brand associated with non-compliant individuals. Another liability concern will be the franchisor's liability to franchisees for advice on how to comply that is later determined to be inappropriate by a privacy commissioner. As was noted earlier, privacy law is new to Canada, and issues in Canada, and in fact much of the world, are still being worked out. Accordingly, there is a distinct possibility that despite best efforts on the part of the franchisor and its advisors some issues in a privacy policy may be challenged by a customer and/or a privacy commissioner.

As was discussed earlier in the section on remedies, most challenges, while embarrassing, may not result in significant financial liabilities. But security issues have the potential to result in significant class action law suits. In Canada there has already been one class action filed resulting from the theft of a hard drive containing names, address and financial information on approximately one million Canadians. Payment information, such as credit card numbers, is particularly vulnerable to identify theft and abuse. These factors should be taken into account when designing any system wide file structure and privacy policy. Depending on the magnitude of this liability issues, it may be necessary to disclosure such issues in the franchise disclosure document.

Even if the franchisor decides not to implement a system-wide privacy policy, it may wish to provide its franchisees with support in developing their own compliance strategies. Obviously to lessen the risk of liability, the franchisor will wish to ensure that any such support documents carry clear disclaimers and warnings regarding the responsibility of the franchisees to develop their own compliance program. Such support options include creating a separate "franchisee" privacy policy and requiring compliance with it; supplying the franchisees with the franchisor's privacy policy and requiring compliance; or requiring the franchisees to submit their privacy policies for franchisor approval.[146]

D. International Compliance

While privacy laws in many countries have substantial similarities with respect to their general requirements, a franchisor may prefer to have only national privacy compliance, rather than system wide compliance, to limit liability.

The development of e-commerce by the franchisor and/or the development of uniform franchisee web-sites, particularly on an international basis, may be an incentive to have a uniform policy system wide. Obviously web-sites present greater opportunity for profiling customers. Electronic payment options also increase the need for uniform security standards. As mentioned earlier European privacy laws require notification to data protection agencies in advance, failing which there are significant civil penalties and possibly even criminal penalties. Enforcement of these laws is increasing. Generally organizations have found that once a significant part of their operations are required to comply with a certain privacy standard, it may be cost effective to implement such standard across the organization.

Centralized control is probably the key to cost effective international privacy compliance. As was pointed out with respect to the so-called 'British Commonwealth Data Protection Model' a privacy policy prepared for one of these jurisdictions may be effective for most if not all of the other jurisdictions in this group. Franchisors may wish to consider having counsel in one jurisdiction prepare a draft privacy policy for that jurisdiction, and then having comments obtained on that draft from other relevant jurisdictions. In Europe the national data protection authorities have been known to provide different answers to questions of interpretation, and there is a need to co-ordinate and evaluate these responses when deciding on the risks and benefits of alternate methods of compliance.

Most of the costs of compliance are usually in the initial development and implementation of a plan. Ongoing maintenance of notifications does not require a significant effort. Other maintenance costs will vary with the degree of new activity in marketing or other areas by the franchisor.

[146] For a discussion of these support options, see Andraya C. Frith and Megan Hill, *PIPEDA for Franchise Lawyers,* The Lawyers Weekly, June 25, 2004.