THE PRIVACY CASE BOOK:

A Global Survey of Privacy and Security Enforcement Actions with Recommendations for Reducing Risks

CHAPTER 2
Deceptive Trade Practices

Margaret P. Eisenhauer, Esq., CIPP
Privacy and Information Management Services – Margaret P. Eisenhauer, P.C.

CHAPTER TWO
DECEPTIVE TRADE PRACTICES

Virtually all regulators have the authority to address deceptive trade practices; companies that make false or misleading statements can be confident that their conduct is actionable universally. Many of the earliest privacy cases were brought to address deceptive trade practices, such as misrepresentations in company privacy notices.

Under Section 5(a) of the FTC Act, the Federal Trade Commission may address deceptive trade practices. Each state has a similar statute, enforceable by the state attorney general. As noted above, **deceptive trade practices** are commercial conduct that includes false or misleading claims, or claims that omit material facts. Consumer injury does not have to result, the mere fact that a company has engaged in a deceptive trade practice is actionable.

Privacy and Security Promises

THE MICROSOFT CASE (DECEMBER 2002)[56]

Respondent: Microsoft Corporation

Regulator: Federal Trade Commission

Basis for Complaint: Deceptive Trade Practices, Violation of Section 5 of the FTC Act

Facts and Allegations: In 1998, Microsoft acquired a start-up software company called Firefly and its namesake online behavioral targeting technology. Microsoft subsequently renamed the technology "Passport" and deployed it across a number of partner and affiliate websites. The technology collected and stored personal information from consumers, which could be passed to other websites that had enabled the Passport technology.

Shortly after the product's launch, a complaint was filed by a consumer group maintaining that Microsoft had misrepresented Passport's underlying security measures as well as the information it collected. The FTC investigated Microsoft in response to this complaint.

The FTC complaint alleges that:

- Despite representations to the contrary by the company, Microsoft failed to implement and document procedures reasonable and appropriate to protect personal information because Microsoft did not use reasonable methods to (i) prevent and detect unauthorized access, (ii) monitor potential vulnerabilities, and (iii) record information to perform security audits;

- Microsoft collected certain information it claimed it did not, such as records of the sites to which a Passport user signed in, along with dates and times of sign in; and

- Purchases made through Passport were not safer and more secure than those made without Passport because the security procedure with or without Passport was identical.

Outcome: The FTC entered into a consent decree with Microsoft, ordering:

Bar on Misrepresentation: Microsoft shall not misrepresent its information practices, including:

(1) The personal information collected;

(2) Its efforts to maintain or protect the privacy, confidentiality or security of any personally identifiable information;

(3) The steps it will take with respect to personal information it has collected in the event of a change in privacy policy; and

(4) Parents' ability to control the information their child can provide to participating sites or the use of such information.

Security Program: Microsoft shall establish and maintain a written security program that is (i) designed to protect the security, confidentiality and integrity of personal information, and (ii) appropriate for the size and complexity of Microsoft, the nature and scope of activities and the sensitivity of the information collected.

Security Program: Requirements of Security Program shall include:

(1) Designation of a responsible employee(s);

(2) Identification of risks to the security, confidentiality and integrity of consumer information that could result in unauthorized disclosure or misuse of information;

(3) The designation and implementation of safeguards through risk assessment, testing and monitoring of the safeguards; and

(4) Evaluation and adjustment of the security program as a result of the assessments, changes to Microsoft's business or other circumstances which may have a material impact on the program.

Third Party Audit: Within one year and on a biannual basis thereafter, Microsoft must obtain an assessment and report from an independent third-party which certifies that the security program:

(1) Meets or exceeds the protections set forth above; and

(2) Is operating with sufficient effectiveness to provide reasonable assurance that consumer information has been protected.

Maintenance of Relevant Documents: For a period of five years Microsoft shall provide (upon request):

(1) A copy of each representation made to consumers regarding the collection, use and security of collected information;

(2) All plans, reports or other materials relating to Microsoft's compliance with the order; and

(3) Any document that contradicts, qualifies or questions Microsoft's compliance with the order.

Delivery of Order: Microsoft shall deliver to each current or future director, employee, agent or representative a copy of the FTC order.

Reporting: Microsoft shall notify the FTC of any change which may affect its compliance with the order. Within 120 days after service of order and thereafter as requested, Microsoft shall file a report with the FTC setting forth its compliance with the order.

Fine Imposed: None

The Eli Lilly cases demonstrate how conduct can create enforcement risk for companies at both the Federal and the state levels.

THE ELI LILLY CASE (MAY 2002)[57]

Respondent: Eli Lilly and Company

Regulator: Federal Trade Commission

Basis for Complaint: Deceptive Trade Practices, Violation of Section 5 of the FTC Act

Facts and Allegations: Respondent, a large U.S.-based pharmaceutical company, offered consumers an online reminder service called Medi-messenger. This service sent automated, personalized messages to registered consumers via electronic email that reminded them to take or refill their depression medications as individually prescribed.

Using a new software program, an Eli Lilly employee inadvertently sent an e-mail notice to all subscribers of the Medi-messenger service. This notice contained (for all to see) the e-mail addresses of all 669 individuals who were registered to the service at that time.

The FTC complaint alleged that Eli Lilly failed to implement or maintain reasonable and appropriate measures to protect consumer information including a failure to properly train employees, provide oversight, and implement appropriate checks and controls.

Outcome: The FTC entered into a consent decree with Eli Lilly, ordering:

Bar on Misrepresentation: Eli Lilly shall not misrepresent the extent to which it maintains and protects the privacy or confidentiality of the collected personal information.

Security Program: Eli Lilly shall establish and maintain a security program for the protection of its collected personally identifiable information.

Requirements of Security Program: The program shall include:

(1) Designation of personnel to coordinate and oversee the program;

(2) Identification of risks to the security, confidentiality and integrity of personal information;

(3) An annual written review conducted by qualified persons to evaluate the effectiveness of the program and recommended changes; and

(4) Adjustments to the program based on the reviews, monitoring or any material changes in operations of Eli Lilly that affect the security program.

Third Party Audit: Not specified in the FTC order. However, Eli Lilly is required to have its annual internal written review examined and certified by an independent auditor. (Additionally, per the multi-state voluntary assurance agreement with certain state attorneys general (discussed below), Eli Lilly must undergo five annual, independent compliance reviews and report the findings of those reviews to the states.)

Maintenance of Relevant Documents: For a period of five years, Eli Lilly shall provide (upon request):

(1) A copy of each representation made to consumers regarding the collection, use and security of collected information;

(2) All plans, reports or other materials relating to, Eli Lilly's compliance with the order; and

(3) Any document that contradicts, qualifies or questions, Eli Lilly's compliance with the order.

Delivery of Order: Eli Lilly shall deliver to each current and future director, employee, agent or representative a copy of the FTC order.

Reporting: Eli Lilly shall notify the FTC of any change which may affect its compliance with the order. Within 120 days after service of order and thereafter as requested, Eli Lilly shall file a report with the FTC setting forth its compliance with the order.

Fine Imposed: None

THE ELI LILLY CASE – STATE ATTORNEYS GENERAL (JUNE 2002)[58]

Respondent: Eli Lilly and Company

Regulator: Attorneys General of California, Connecticut, Idaho, Iowa, Massachusetts, New Jersey, New York, and Vermont (the "States")

Basis for Complaint: Various state consumer protection and trade practices statutes, such as California Bus. & Prof Code §§ 17200 et seq. and 17500 *et seq.;* the Connecticut Unfair Trade Practices Act, Conn. Gen. Stat. §§ 42-110a et seq.*;* and the Idaho Consumer Protection Act, Idaho Code §§ 48-601 et seq.

Facts and Allegations: The facts and allegations mirrored those in the FTC case regarding Medi-messenger discussed above.

Outcome: The States entered into an Assurance of Voluntary Compliance and Discontinuance Agreement with Eli Lilly, ordering:

Bar on Misrepresentation: Eli Lilly shall not misrepresent the extent to which it maintains and protects the privacy or confidentiality of collected personally identifiable information.

Security Program: Eli Lilly shall (a) establish supervisory procedures designed to achieve compliance with the Assurance, and (b) establish and maintain a security program for the protection of its collected personally identifiable information.

Requirements of Security Program: The program shall include:

(1) Appropriate safeguards that are designed to protect personally identifiable information against unauthorized access, use or disclosure and against reasonably anticipated threats to its security or integrity;

(2) Automated barriers that ensure only pre-authorized and designated personnel can gain access to the personally identifiable information;

(3) Designation of personnel to coordinate and oversee the program;

(4) Identification of risks to the security, confidentiality and integrity of personal information;

(5) Training relevant employees to monitor compliance using materials and procedures that are current;

(6) Documenting the means of implementing the program;

(7) Within ninety days (and annually thereafter), a written review conducted by qualified persons to monitor compliance, evaluate the effectiveness and recommended changes to the program, in addition to monitoring the conformance of its practices to its representations; and

(8) Adjustments to the program based on the reviews, monitoring or any material changes in the operations of Eli Lilly that affect the security program.

Third Party Audit: The annual audit may be performed by a qualified and independent third party. If the audit is performed internally then Eli Lilly is required to have its written review examined and certified by an independent third party that will report its results in writing to the States.

Maintenance of Relevant Documents: For a period of five years, Eli Lilly shall maintain and provide (upon request): a copy of each representation made to consumers regarding the collection, use and security of personally identifiable information; all plans, reports or other materials relating to Eli Lilly's compliance with the order; and any document that contradicts, qualifies or questions, Eli Lilly's compliance with the order.

Delivery of Order: Within thirty days of date of Assurance, Eli Lilly shall deliver a copy of the Assurance to all principals, officers, directors, managers, employees, agents, representatives and contractors having responsibility relating to the Assurance. The Assurance shall be delivered to future individuals and entities within thirty days of assuming their responsibilities.

Fine Imposed: $160,000

International data protection authorities also use enforcement proceedings to address deceptive trade practices, such as inaccuracies in privacy statements.

THE DFAIT CASE (JUNE 2005)[59]

Respondent: Department of Foreign Affairs and International Trade (DFAIT)

Regulator: Office of the Privacy Commissioner of Canada

Basis for Complaint: Violation of Privacy Act (regulating Federal government agencies)

Facts and Allegations: DFAIT offers an email media news service. When registering, Canadian subscribers were required to provide their e-mail address, city, province, postal code, telephone number and company affiliation. (International subscribers were only being asked for their e-mail address and country of origin.)

The complaint alleged that the data collection was overbroad, in violation of PIPEDA. However, the investigation revealed that DFAIT required telephone numbers to allow contact with subscribers in the event of technical problems with e-mail addresses. Postal code and company affiliation information was required so that some media releases can be targeted to a particular region or a particular type of business.

The Privacy Commissioner's Office concluded that DFAIT was allowed under the Act to collect the subscriber information in order to facilitate access to and distribution of the media releases. The complaint was therefore considered to be not well-founded.

However, the Commissioner's Office noted that the DFAIT privacy notice suggested that the provision of the personal information was voluntary. (Only participation in the subscription activity itself that was voluntary.) The Office concluded that the use of the word "voluntary" in the DFAIT privacy notice was misleading.

Outcome: DFAIT agreed with the Commissioner's conclusion and revised its privacy notice to make it more accurate.

Fine Imposed: None

Early cases addressing security incidents were brought as deceptive trade practices cases, based on the companies' security promises in their privacy notices. As a result of these actions, many companies revised their privacy notice language to avoid making promises about security. The regulators responded by interpreting the unfairness doctrine to encompass insufficient security. These cases are discussed in Chapter 4.

THE PETCO CASE (NOVEMBER 2004)[60]

Respondent: Petco, Inc.

Regulator: Federal Trade Commission

Basis for Complaint: Deceptive Trade Practices, Violation of Section 5 of the FTC Act

Facts and Allegations: Petco sells pet food, supplies, and services through its stores and on its website. Visitors communicate with the website using a web application to obtain product information and to supply transaction information such as credit card number and contact information. The Petco website has a posted privacy

statement that promised appropriate privacy and security of the personal information provided to the company via the web application.

Since February 2001, the Petco website had been vulnerable to Structured Query Language (SQL) searches and other online exploits. In June 2003, a visitor conducted a SQL search and was able to read, in clear text, the credit card numbers stored within Petco's database.

The FTC alleged that:

- Despite Petco's representations to the contrary, personal information obtained from consumers was not maintained in an encrypted format and was thus accessible to persons other than the consumer providing the information; and

- Such information, including credit card numbers, was accessible through commonly known technical attack methods thereby failing to maintain reasonable and appropriate measures to protect personal information.

The FTC characterized Petco's actions as deceptive, but did not allege consumer injury.

Outcome: The FTC entered into a consent decree with Petco, ordering:

Bar on Misrepresentation: Petco shall not misrepresent the extent to which it maintains and protects the privacy, confidentiality, security, or integrity of any personal information collected from or about consumers.

Security Program: Petco shall establish and maintain a comprehensive security program reasonably designed for the protection of its collected personally identifiable information. In creating the program, Petco shall:

(1) Designate personnel to coordinate and oversee the program;

(2) Identify risks to the security, confidentiality and integrity of personal information through an assessment focusing on employee training, information systems, and potential system failures;

(3) Design and implementation of reasonable safeguards to identified risks; and

(4) Evaluate and adjust its program according to assessment and material changes in business.

Third Party Audit: Within 180 days after service of order and thereafter biannually for ten years, Petco must obtain an assessment and report from an independent, third party that (i) sets forth the specific safeguards implemented and maintained by Petco, (ii) explains how such safeguards are appropriate for the size and complexity of Petco, the nature and scope of Petco's activities and the sensitivity of the information, (iii) explains how the safeguards meet or exceed the protections above; and (iv) certifies that Petco's security program is operating with sufficient effectiveness to provide reasonable assurances that consumer information is protected.

Maintenance of Relevant Documents: For a period of five years, Petco shall provide (upon request):

(1) A copy of each representation made to consumers regarding the collection, use and security of collected information;

(2) All plans, reports or other materials relating to Petco's compliance with the order; and

(3) Any document that contradicts, qualifies or questions Petco's compliance with the order.

Delivery of Order: Petco must deliver a copy of this order to all current and future principals, officers, directors, managers and all employees with managerial responsibility.

Reporting: Petco shall notify the FTC at least 30 days prior of any corporate change which may affect its compliance with the order. Within 180 days after service of order and thereafter as requested, Petco shall file a report with the FTC setting forth its compliance with the order.

Fine Imposed: None

Pretexting

Making false or misleading statements in a privacy notice is not the only deceptive conduct privacy regulators enforce. Regulators also bring action when personal information is collected via deceptive means.

Pretexting is the practice of using false pretenses to gather personal information. Using pretexting to collect financial information is prohibited by the Gramm-Leach-Bliley Act, and the Federal Trade Commission has brought numerous enforcement actions to address this deceptive practice.[61] State laws commonly prohibit the use of pretexting to obtain sensitive data, such as financial records or telephone records. The following summary presents a state attorney general action for pretexting.

THE HP CIVIL CASE (DECEMBER 2006)[62]

Respondent: Hewlett-Packard Company

Regulator: Attorney General of the State of California

Basis for Complaint: The California AG filed civil and criminal complaints against HP and certain officers/directors for violations of various California laws. This case summary details the civil case, in which the AG alleged that HP used "false and fraudulent pretenses" (*i.e.,* pretexting) to obtain confidential information (such as individual calling records and billing records) from a phone company in violation of CA Penal Code section 538.5.

The civil complaint also alleged HP violated Penal Code section 502(c)(2) by willfully and knowingly accessing, and without permission using, computerized telephone account data belonging to the victims. Additionally, the complaint alleged that HP violated California's identity theft statute (Penal Code section 530.5) by willfully obtaining personal identifying information about the victims, then using that information for an unlawful purpose, according to the complaint. The claims in the civil case mirror those in the criminal filings.

Facts and Allegations: The cases arose as a result of actions taken by HP and third party investigators hired by HP to probe leaks of confidential board documents and discussions to the media. In the course of the investigation, phone records of various news reporters were obtained by false pretenses. Other information was obtained about the reporters, in an attempt to determine whether any reporters had access to insiders at HP who had divulged confidential information. The investigators also sought information about those HP board members who were suspected of sharing information with the reporters.

Although HP denied knowledge of the fact that the third party investigator had used false pretenses to obtain telephone records, the Chairman of the Board had authorized the investigation. In the wake of the scandal, the Chairman resigned. She was later charged with felony criminal counts related to the investigation, along with the HP ethics office and three of the private investigators. (*California v. Dunn,* Cal. Super. Ct., DA No. 061027481, 10/4/06). The civil complaint was filed shortly thereafter.

Outcome: HP settled the civil matter by agreeing to institute significant changes in its corporate governance processes, paying civil penalties and creating a Privacy and Piracy Fund to support enforcement efforts by the AG's office.

With regard to corporate governance, HP agreed to:

- Establish an independent director to serve as the Board's watchdog on compliance with ethical and legal requirements. The director will have specific responsibilities for carrying out oversight functions and reporting violations to the Board, other responsible HP officials and the Attorney General;

- Expand the oversight of its chief ethics and compliance officer (CECO). The CECO will review HP's investigation practices and make recommendations to the Board and also report to the Board's Audit Committee as well as to the General Counsel. Additionally, the CECO will have authority to retain independent legal advisors;

- Expand the duties of its chief privacy officer to include review of the firm's investigation protocols to ensure they protect privacy and comply with ethical requirements;

- Establish a new Compliance Council, headed by the CECO, to develop and maintain policies and procedures governing HP's ethics and compliance program; and

- Enhance its ethics and conflict-of-interest training and create a separate code of conduct, for use by outside investigators that addresses privacy and business ethics issues.

HP agreed to provide the AG with $13,500,000 to fund the Privacy and Piracy Fund. The Fund will be used to support law enforcement activities related to privacy and intellectual property rights. Additionally, HP agreed to pay $650,000 in civil penalties and $350,000 to cover the Attorney General's investigation and other costs.

Note: settlement of the civil case did not affect the criminal cases that had been filed. One of the investigators pled guilty to charges; the court dismissed the charges against the HP Chairman and the investigators.

Fine Imposed: $14,500,000

Concerns about pretexting have been raised by international data protection authorities as well. In a highly-publicized incident, the Privacy Commissioner of Canada was a target of a news report on the distribution of phone records by United States data brokers. According to the Privacy Commissioner's report:[63]

> *The November 21, 2005, edition of* Maclean's *magazine contained an account of how the magazine obtained records of telephone calls made by the Privacy Commissioner of Canada, Ms. Jennifer Stoddart, from her home telephone and Office BlackBerry numbers, as well as the cell phone records of an unnamed* Maclean's *senior editor. The records in question were purchased by the reporter from Locatecell.com, a*

U.S. data broker, which had, in turn, obtained them from Canadian telecommunications companies, Bell, TELUS Mobility, and Fido. Concerned about how these disclosures could happen, the Assistant Privacy Commissioner initiated complaints against the Canadian companies.

The investigations revealed that Locatecell.com had used "social engineering" to successfully circumvent the customer authentication procedures of Bell and TELUS Mobility. Social engineering is a collection of techniques used to manipulate people into performing actions or divulging confidential information. Pretexting is one such technique and is the act of creating and using an invented scenario to obtain information from a target, usually over the telephone. In the cases at hand, there was no evidence that anyone had hacked into the companies' systems or that the disclosures were made by rogue employees.

The Privacy Commissioner brought actions against the Canadian phone companies that had supplied the records to the United States broker, Locatecell.com. Concerns about jurisdiction limited the investigation into Locatecell.com's activities. These jurisdictional concerns may have been unfounded.

In December 2004, the Canadian Internet Policy and Public Interest Clinic ("CIPPIC") asked the Privacy Commissioner to investigate another United States data broker, Abika.com. Although Abika.com did not have operations in Canada, it distributed information about Canadians via its website, allegedly in violation of Canada's federal privacy law, **The Personal Information Protection and Electronic Documents Act** (PIPEDA). The CIPPIC specifically asked the Commission to reconsider its position that it could not investigate companies merely because they were wholly-located in the United States.[64]

When the Commission refused to initiate the investigation based on purported lack of jurisdiction, the CIPPIC filed an application for judicial review in the Federal Court of Canada, challenging the Privacy Commissioner's determination regarding her jurisdiction. The court was asked to consider the scope of the Commissioner's powers under PIPEDA.

The court released its decision in February 2007,[65] finding that the Privacy Commissioner had jurisdiction under PIPEDA to investigate cross-border data flows. The court noted that, although the company and the website were located in the United States, the collection and distribution of the Canadian personal information occurred in Canada.

The court noted that both parties agreed that if the Privacy Commissioner had jurisdiction, she was required to investigate. Section 12 of PIPEDA provides: "The Commissioner shall conduct an investigation in respect of a complaint…" Accordingly, since the Privacy Commissioner is required to

investigate complaints where jurisdiction exists, the matter was remanded to her office for investigation.[66]