THE PRIVACY CASE BOOK:

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

CHAPTER 1
General Theories of Liability

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

Chapter One
GENERAL THEORIES OF LIABILITY

Companies face two main types of legal claims from regulators as a result of their information handling practices: (1) claims that the company has violated a specific law or regulation, and (2) claims that the company has violated a general consumer protection law, such as a legal obligation to conduct business in a fair and non-deceptive manner.[1] Regulators bring such claims as a result of privacy or security incidents, consumer complaints or independent regulatory inquiry.

Regulators

A **regulator** is any government agency with the ability to investigate a company's information handling practices or bring an action against a company for privacy or security violations.

In countries with national data protection laws, regulators include the **data protection authorities**, agencies established by these laws to oversee and implement the laws as well as those government agencies that enforce consumer protection and labor laws. In the United States, the **Federal Trade Commission** (FTC) and **state attorneys general** aggressively enforce privacy laws and consumer protection laws. Other regulators also include **functional regulators**, those government agencies that oversee companies engaged in specific businesses or activities, such as financial services, insurance, education, healthcare, or telecommunications. These regulators are described in more detail below. The figure below lists some of the regulators that commonly bring privacy and security enforcement actions.

Figure 1.1: The Privacy Enforcement Powers of Certain Regulators

Country	Regulator	Jurisdiction	Enforcement Powers
Argentina	Dirección Nacional de Protección de Datos Personales[2]	Independent public office which has responsibility to implement the Argentine Personal Data Protection Law (Ley de Protección de los Datos Personales), including maintaining the data processing registry	Receives complaints, conducts investigations and brings actions to enforce the law; may apply sanctions including warnings, suspensions, and fines, and may order deletion of data, files or databases

Country	Regulator	Jurisdiction	Enforcement Powers
Australia – Federal	Office of the Privacy Commissioner[3]	Independent public office which has responsibilities under the federal Privacy Act 1988, over personal information processing by Federal and ACT government agencies, and many private sector organizations, including large companies, health service providers, credit reporting agencies and credit providers, and users of personal tax file numbers	Receives complaints, conducts investigations and brings actions to enforce the Privacy Act as well as the Data-Matching Program (Assistance and Tax) Act 1900 and Guidelines, the Tax File Number Guidelines, and the Guidelines under section 135AA of the National Health Act 1953. Conducts audits under the Telecommunications Act of 1997
Australia – New South Wales (NSW)	Office of the New South Wales Privacy Commissioner[4]	Oversees NSW privacy laws, including the management of personal information by New South Wales public sector agencies pursuant to the Privacy and Personal Information Protection Act 1998 and the management of health information by public and private sector organizations under the Health Records and Information Privacy Act 2002	Receives complaints and conducts investigations and conciliation proceedings; refers matters to Director of Public Prosecutions for additional legal action, if needed; also refers matters to the Federal Privacy Commissioner as needed
Canada – Federal	Privacy Commissioner of Canada[5]	Independent office that oversees compliance with the Privacy Act (which applies to the federal government) and the Personal Information Protection and Electronic Documents Act (PIPEDA), Canada's private sector privacy law.	Receives complaints, conducts investigations and brings actions to enforce the Privacy Act and PIPEDA
Canada – Ontario	Information and Privacy Commissioner/ Ontario (IPC)[6]	Independent office that oversees Ontario provincial and municipal governments, and health information custodians, as defined in the Ontario Freedom of Information and Protection of Privacy Act, the Municipal Freedom of Information and Protection of Privacy Act, and the Personal Health Information Protection Act (the Acts)	Receives complaints, conducts investigations and brings actions to enforce the Acts
Dubai International Financial Centre (DIFC)	Commissioner of Data Protection[7]	Oversees and enforces the DIFC Data Protection Law over DIFC registered entities; maintains registry and issues permits for sensitive data processing and data transfers	Investigates and brings actions to enforce the Data Protection Law

Country	Regulator	Jurisdiction	Enforcement Powers
France	Commission nationale de l'informatique et des libertés (CNIL)[8]	Independent office that oversees the implementation of the French Data Protection Act (Decree No 2005-1309 of 20 October 2005 enacted for the application of Act No 78-17 of 6 January 1978 on Data Processing, Files and Individual Liberties amended by Act No 2004-801 of 6 August 2004) including maintaining the data processing registry	Receives complaints and conducts investigations; may also issue warnings to the persons responsible for the files or inform the Public Prosecutor of any offences
Germany – Brandenburg[9]	Brandenburg State Commissioner for Data Protection and Access to Information[10]	Oversees German data protection law; collaborates with Federal DPA and other Länder DPAs	Receives complaints, conducts investigations and brings actions to enforce data protection laws against public bodies within the Länder
Germany – Brandenburg	Ministry for the Interior	Oversees German data protection law	Receives complaints, conducts investigations and brings actions to enforce data protection laws against private entities within the Länder
Germany – Federal	Federal Commissioner for Data Protection and Freedom of Information Bundesbeauf-tragter für den Datenschutz, (or BfDI)[11]	Independent federal agency that supervises the Federal Data Protection Act (BDSG) as well as the Federal Freedom of Information Act, including monitoring the compliance with the provisions of the BDSG by public bodies; collaborates with the 16 Länder DPAs	Receives complaints, conducts investigations and brings actions to enforce the BDSG against German federal public bodies
Hong Kong, China	Office of the Privacy Commissioner for Personal Data (PCPD)[12]	Independent statutory body set up to promote, monitor and oversee the enforcement of the Personal Data (Privacy) Ordinance	Accepts and resolves complaints; investigates and issues enforcement notices if the Ordinance has been contravened
Israel	Israeli Law and Information Technologies Authority (Ministry of Justice)[13]	Authority established in 2006 to enforce the Privacy Protection Act 1981, the Digital Signature Act 2001 and the Credit Reporting Act 2002; includes maintaining the data processing registry	Receives complaints, conducts investigations and has authority to issue fines
Japan	Financial Services Agency[14]	Ministry issues guidelines and oversees implementation of the Personal Information Protection Act and other laws as applied to businesses handling personal information in the financial sector	Receives complaints, conducts investigations and brings actions to enforce the PIPA and ministerial guidelines against financial services companies

Country	Regulator	Jurisdiction	Enforcement Powers
Japan	Ministry of Economy, Trade and Industry (METI)[15]	Ministry issues guidelines and oversees implementation of the Personal Information Protection Act (PIPA) as applied to businesses handling personal information in the METI-regulated (general commercial) sector	Receives complaints, conducts investigations and brings actions to enforce the PIPA and ministerial guidelines against companies in the general commercial sector
Japan	Ministry of Health, Labor and Welfare[16]	Ministry issues guidelines and oversees implementation of the Personal Information Protection Act (PIPA) as applied to businesses handling personal information for employee administration	Receives complaints, conducts investigations and brings actions to enforce the PIPA and ministerial guidelines against employers
United Kingdom	Information Commissioner's Office (ICO)[17]	Independent public body set up to oversee the UK Data Protection Act (including maintaining the data processing registry), the Freedom of Information Act, the Environmental Information Regulations, and the Privacy and Electronic Communications Regulations	Receives complaints, conducts investigations and brings actions to enforce the Data Protection Act (and other statutes)
United States – Federal	Federal Trade Commission (FTC) – Bureau of Consumer Protection[18]	Regulates the organization, business, conduct, practices, and management of any person, partnership, or corporation engaged in or whose business affects commerce, excepting banks, savings and loan institutions, Federal credit unions and common carriers	Receives complaints, conducts investigations and brings civil actions to protect consumers against unfair or deceptive trade practices; enforces Federal consumer protection laws and FTC rules; investigates company and industry practices Criminal actions referred to the US Department of Justice for prosecution
United States – Federal	Federal Communications Commission (FCC) – Enforcement Bureau[19]	Regulates interstate and international communications by radio, television, wire, satellite and cable in the 50 states, the District of Columbia and U.S. possessions	Receives complaints, conducts investigations and brings actions to enforce the Communications Act and FCC rules
United States – Federal	Department of Health & Human Services – Office of Civil Rights (OCR)[20]	OCR investigates complaints of noncompliance with and makes decisions regarding the interpretation, implementation, and enforcement of the HIPAA Privacy Rule; authority delegated to the Director, OCR by the Secretary of the Department of HHS	Receives complaints, conducts investigations and brings actions to enforce the HIPAA Privacy Rule

Country	Regulator	Jurisdiction	Enforcement Powers
United States – Federal	Department of Health & Human Services – Centers for Medicare and Medicaid Services (CMS)[21]	CMS investigates complaints of noncompliance with and makes decisions regarding the interpretation, implementation, and enforcement of the HIPAA Security Rule; authority delegated to the Administrator, CMS by the Secretary of the Department of HHS	Receives complaints, conducts investigations and brings actions to enforce the HIPAA Security Rule
United States – Federal	Department of the Treasury – Office of the Comptroller of the Currency (OCC)[22]	Charters, regulates and supervises all national banks, and supervises the federal branches and agencies of foreign banks	Brings supervisory actions against banks that do not comply with laws and regulations or that otherwise engage in unsound banking practices; OCC can remove officers and directors, negotiate agreements to change banking practices and issue cease and desist orders as well as civil money penalties
United States – States and Territories	Attorneys General (AG)[23]	Varies due to constitutional and statutory mandates, but each AG serves as chief legal officer of its state, has jurisdiction over persons and entities within (or doing business within) its state, and represents the state and state agencies generally	Receives complaints, conducts investigations and brings actions to enforce Federal or State laws and addresses deceptive trade practices

Specific Privacy and Security Laws

Many countries have enacted specific privacy and security laws. Some countries have enacted **comprehensive data protection laws** that regulate virtually all processing of personal information. Countries with comprehensive laws include those in the European Union and European Economic Area, as well as Canada, Australia, New Zealand, Japan, Switzerland, Russia, Argentina, Israel, Hong Kong, Tunisia, the Dubai International Financial Centre, and the Bahamas (to name a few).

A few countries have limited data protection laws. These laws apply general data protection theories to a subset of data processed by companies in the country. For example, the Korean data protection law only applies to companies in certain industries, such as telecommunications companies, internet service providers, website operators, travel agencies, hotels, airline carriers, and educational institutions.[24] In Taiwan, the Computer-Processed Personal Data Protection Law regulates the processing of personal information by government agencies and a defined list of private-sector entities such as credit reporting agencies, hospitals, schools, and financial institutions.

Other countries, such as the United States, regulate data processing as needed to address specific types of harms. Many countries' laws provide specific privacy protections for information handled by financial institutions, telecommunications companies, or healthcare providers, or for activities such as consumer reporting or targeted marketing. These countries may have a wide-array of different laws, each of which must be understood and respected.

Corporate liability for violating a specific law or regulation is quite straight-forward. All laws generally specify a regulatory agency responsible for compliance oversight and provide for regulatory agency enforcement in the event the terms of the law are contravened. In this case, the regulator generally investigates the company and initiates an action, based on its powers and the requirements of the law.[25]

The law may also enable individuals to bring a private action against a company, if they have been harmed by the company's breach – this ability to sue is called a **private right of action**.

Consumer Protection Laws

Most jurisdictions have a general consumer protection statute. These laws prohibit commercial behavior that is deceptive, fraudulent or misleading. The law may also give the regulator the power to address commercial conduct that unreasonably harms individuals. For example, consumer protection laws require companies to disclose material facts about goods and services and/or take reasonable steps to protect the health and safety of consumers.

In the United States, Section 5(a) of **the FTC Act** (discussed below) provides the **Federal Trade Commission** with the power to protect consumers from unfair and deceptive trade practices. Every state has a similar consumer protection statute, prohibiting deceptive acts and practices. These statutes are generally enforced by the **attorneys general**, the chief legal officers of the states, and they often provide for a private right of action as well. The attorneys general can often enforce Federal laws (such as the Children's Online Privacy Protection Act and the Fair Credit Reporting Act), for violations that occur in their states.

According to the National Association of Attorneys General ("NAAG"):

> *State Attorneys General have primary responsibility in their states for the enforcement of their state's consumer protection laws. These broad general statutes are supplemented in all jurisdictions by laws that address specific industries or practices. The State Attorneys General have varied tools and authority to address abuses and illegalities in the market place. These include civil and criminal litigation, mediation, public and business education, creating and commenting on state and federal legislative proposals, and cooperative enforcement ventures with state, local, and federal enforcement agencies. The consumer protection work of State Attorneys General over the past year has run the gamut from telemarketing to telecommunications and from prescription drugs and privacy to price-gouging.*[26]

Many of the attorneys general participate in the NAAG Consumer Protection Project. This group works to improve the enforcement of state and federal consumer protection law. It also supports multistate consumer protection enforcement efforts, including information exchange among the states with respect to investigations, litigation, consumer education and legislation.[27]

Most countries outside the United States have enacted national and/or local consumer protection laws as well. In Europe, for example, there are a number of consumer protection directives that member states have implemented to provide a framework for consumer rights. The European Union has also established a European Commissioner for Consumer Protection. In each jurisdiction, these consumer protection laws are complemented and supplemented by specific privacy and data protection statutes.

General Powers of Regulatory Agencies

Oversight of international data protection laws often rests in the hands of national (and/or provincial) regulators, data protection authorities. Data protection authorities include national and provincial "privacy commissioners" and "information commissioners."

Data protection authorities (DPAs) are independent government agencies established to protect privacy and oversee compliance with Data protection laws. Data protection authorities are generally responsible for enforcement of their national (or provincial) data protection laws. As discussed below, data protection authorities typically have the power to hear complaints from individuals, investigate data processing activities, impose sanctions (such as fines) and institute civil and criminal proceedings. In many cases, data protection authorities can also order the deletion of inappropriately-collected data or the cessation of inappropriate data processing, and block proposed transfers of personal information to third parties.

In October 2006, the Organization for Economic Cooperation and Development (OECD) published the OECD *Report on Cross-Border Enforcement of Privacy Laws* (the "Report").[28] The Report examined the regulatory and enforcement mechanisms that have been established in countries to resolve consumer

complaints and address non-compliance with privacy laws. In preparing the Report, OECD surveyed twenty-two national regulatory agencies regarding their enforcement capabilities.[29] It defined the term '**enforcement**' to include efforts by government authorities to i) secure legal remedies for individuals that have been harmed; ii) carry out regulatory audits and inspections; and iii) secure compliance by formal legal action of an administrative, civil, or criminal nature."[30]

According to the survey results, many countries have national-level enforcement mechanisms:

- Many countries have dedicated data protection law regulators who are responsible for enforcement of their respective laws. For example, Austria, France, Germany and Italy have a national data protection authority that has primary responsibility for all activities associated with enforcement of their respective national data protection laws.
- Some countries, such as Canada and Australia, have both national and provincial/state data protection authorities that enforce privacy laws, reflecting the national/provincial regulatory regimes that exist.
- Germany has a national authority as well as state (Länder) authorities who enforce the laws against public-sector entities, but private-sector enforcement is primarily done by independent regional authorities.
- Other countries have officials in established government departments and ministries that handle privacy oversight. For example, in Japan, the Cabinet Office has general policy oversight of privacy protection, but complaints are dealt with by the National Consumer Affairs Center of Japan and other bodies. Relevant ministers can issue enforcement orders within the industry sectors over which they have oversight.
- In Korea, the principal enforcement authorities are the Ministry of Information and Communications (MIC) and the Korea Information Security Agency (KISA).

The Report considered different types of enforcement processes, such as responding to consumer complaints, conducting regulatory oversight, and imposing sanctions. Every country that responded to the survey had at least one authority that could consider consumer privacy complaints, and several countries had multiple authorities that handled consumer complaints. The regulatory agencies generally had discretion with regard to their response to the complaints, but some countries (such as Canada) mandate an investigation of all complaints. Additionally, all of the regulators that accepted complaints accepted them by mail, and most allowed complaints to be made by telephone or online/email as well.

The regulatory agencies provided information about their powers of supervision, such as the ability to initiate audits or investigations regarding compliance. Only the Korea Information Security Agency reported that it did not have the power to investigate on its own initiative, but the Ministry of Information and Communications can do so. According to the Report, "the general picture is that typically authorities combine the roles of complaint handling and regulator or enforcer."[31]

The regulators' investigative powers do differ widely. The report distinguishes investigations from onsite audits. While most regulatory agencies have the ability to conduct onsite audits, the Federal Trade Commission, the Korea Information Security Agency and the competent Japanese ministers do not have such powers. Even where the power to conduct onsite audits does exist, some authorities hedge the use of the power with protections for the companies being investigated. For example, in the United Kingdom, an onsite audit usually cannot occur without the consent of the *data controller*.[1] Authorities in Albania, Belgium, Canada, Hungary, Italy, and the Korean Ministry of Information and Communications are required to have reasonable grounds for believing that there has been non-compliance with the law. Other countries (such as the Czech Republic, France, Germany, Iceland, the Netherlands, and Poland) appear to have "little formal constraint on their powers."[32]

The Report also notes that

> *[t]he powers available to many authorities when conducting investigations seem to be extensive. Most authorities can require a data controller to provide information and documents. Most authorities have similar powers in relation to third parties [such as data processors], but this is a smaller group than in the former case and excludes Japan, Korea, the United Kingdom and typically the German states. Again, most, but not all, authorities can enter premises without consent. This is a power which often requires judicial warrant, as is the case for Australia, France, Italy, the United Kingdom and the United States. It was also reported that the large majority of authorities could require the temporary or permanent cessation of processing…*[33]

With regard to sanctions:

- Nineteen regulatory agencies can determine that the law has been violated; for ten agencies, that decision has legal effect by itself;
- Sixteen of the agencies can issue legally-enforceable orders;

---

[1] A "*data controller*" is the entity that controls the means and purposes of the data processing. Controllers are distinguished from data processors, which are entities that handle data for the data controller and only process the data in accordance with the data controllers instructions.

- Sixteen agencies can seek financial or other penalties;
- Fifteen agencies can issue warnings or reprimands; thirteen of these agencies can make the reprimand public;
- Ten authorities can seek injunctions in the courts;
- Seven authorities can institute criminal proceedings; the other agencies submit a request to a public prosecutor to initiate proceedings;
- Six authorities can negotiate fines or other settlements; and
- Agencies in Australia, Norway, and the United States can order compensation for individuals.[34]

With regard to settlements, the Report noted that some of the authorities (such as Australia) believe that negotiated settlements are the best approach. Similarly, the Canadian Federal Commissioner may attempt to resolve complaints through mediation and conciliation which could include a settlement. The Report added: "France, however, noted that a regulatory authority that can impose a decision has no need to negotiate settlements – a response that may apply to other authorities with strong enforcement powers." [35]

With regard to remedies available through the national courts, all of the countries reported that they provide some form of remedy through their courts or special tribunals. The judicial remedies may include the issuance of court order, compensation for individuals, civil penalties, criminal fines and imprisonment following conviction. Regulatory agencies and the national judicial system generally work collaboratively to resolve issues of non-compliance. The Report observes: "So, for example, the Korea Information Security Agency has rather limited powers, but a wide range of sanctions is available through the Korean courts including compensation for individuals and fines and imprisonment on criminal conviction."[36]

Data protection authorities take their oversight roles very seriously, and several authorities have received additional enforcement power in recent years. France, for example, revised its data protection law in 2004, giving the French Commission nationale de l'informatique et des libertés (CNIL) significant new powers to impose administrative and financial penalties ranging from €150,000 to €300,000.[37] The United Kingdom's Information Commissioner is currently seeking additional powers to conduct audits and issue fines.[38]

Other data protection authorities have long had the power to impose significant fines and other penalties. In Spain, serious violations of the law are punishable by fines of up to €600,000.[39] In October 2007, the BNA Privacy Law Watch[40] quoted the director of the Spanish Agencia Espaola de Proteccin de Datos (AEPD) as explaining why the Spanish data protection authority aggressively imposed fines:

"It's true that industry ... is not very happy with the fines, of course… but fines are the "tool" that produce respect for individuals' privacy rights," adding, "I can confirm that sanctions ... have been a real way to guarantee data protection."[41]

In Germany, the maximum fine is €250,000 or a prison sentence of up to two years.[42] In Ireland, the fine is up to €100,000.[43] Greece's data privacy laws provide for fines in excess of €140,000.[44]

Data protection authorities are not reluctant to use their enforcement powers. On September 4, 2006, the French CNIL announced its first fine against a private-sector entity (a €45,000 fine against the French bank Credit Lyonnais), and has also imposed sixteen additional fines totaling €168,300 according to its 2006-2007 annual report.[45] The Spanish AEPD's 2006 annual report revealed that it conducted almost 1,300 investigations and imposed €24.4 million in fines.[46]

Outside of Europe, the Privacy Commissioner of Canada reported that in 2006 her office had received over 6,000 inquiries as well as 424 complaints regarding private sector entities, initiated two major audits, and filed two court actions where companies failed to adopt her recommendations.[47]

The Hong Kong Privacy Commissioner for Personal Data reported that, from March 2006-April 2007 it received over 1,050 complaints (of which 69% were against private sector entities).[48] The Hong Kong Privacy Commissioner resolved 142 cases through mediation (issuing advice/recommendations to 71 companies), and issued sixty enforcement notices to prevent continued or repeated violations.[49]

In Europe, the risk of data flow disruptions is also very real. Data protection authorities and national courts have intervened to block the transfer of even seemingly innocuous personal information from European nations. For example, the data protection authority for the German Länder Schleswig-Holstein in 2003 ordered the global subsidiaries of a multinational corporation to delete the personal data of a former German employee, based on the employee's complaint that the company did not have a legal basis for transferring his data into the company's United States-based HR system.[50]

Finally, it is important to note that the enforcement risks internationally are likely to escalate. On January 15, 2008, the French CNIL announced plans to drastically increase on-site inspections of companies where privacy law violations were alleged.[51] Other data protection authorities have also committed to increasing "spot checks"—the process by which officials show up at a company's office unannounced and demand immediate access to computer systems and stored data, and to collaborate in multi-DPA investigations. Similarly, the OECD is exploring ways to break down barriers to cross-border investigations and enforcement proceedings; the OECD Report discussed above was

complemented by a companion document entitled "The OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy."[52]

The trend toward increased enforcement is not limited to Europe. For example, Dr. Omer Tene notes that Israel created a new data protection agency in 2006 to address concerns about weak enforcement of the Israeli data protection law.[53] He writes:

> *As part of the effort to increase data protection compliance and law enforcement, Israel established a new data protection authority in 2006, the Israeli Law and Information Technologies Authority (ILITA). The ILITA has been charged with enforcing three statutes, the Privacy Protection Act 1981 (PPA), the Digital Signature Act 2001 and the Credit Reporting Act 2002. The ILITA is better funded and staffed than the Database Registrar, and most importantly, it intends to focus on compliance and enforcement. Moreover, under recent regulations, the ILITA has been authorized to administer fines under the Administrative Offences Regulations: Administrative Fines - Privacy Protection, 2004.*

The Authority of the US Federal Trade Commission

In the United States, the **Federal Trade Commission** (FTC) is the Federal government agency primarily charged with consumer protection. In this role, it aggressively protects consumers, enforces company-made privacy and security promises and enforces obligations imposed on companies by specific privacy and security laws.

The basic consumer protection statute enforced by the Federal Trade Commission is Section 5(a) of the FTC Act, which provides that "unfair or deceptive acts or practices **in or affecting commerce are declared unlawful**" (15 U.S.C. Sec. 45(a)(1)).[54] Understanding the meanings of (and differences between) unfair and deceptive trade practices is crucial for interpreting Federal Trade Commission actions.

- **A deceptive trade practice** is 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.

- **An unfair trade practice** is commercial conduct that (1) causes (or is likely to cause) substantial injury to consumers (2) that consumers cannot reasonably avoid themselves, and (3) without offsetting benefits to consumers or competition.

Accordingly, if a company makes a privacy or security promise, and then fails to live up to that promise, it has likely engaged in a deceptive trade practice. For example, if a company promises in a privacy notice not to share personal information, and then it shares the information, it has engaged in deceptive conduct.

If a company puts consumers at risks, with no offsetting benefit, this may be an unfair trade practice. For example, even if a company does not promise to have reasonable security for its website, if the company collects sensitive data (such as credit card numbers) without having reasonable security, the company has likely engaged in an unfair trade practice.

In addition, the Federal Trade Commission enforces a variety of specific consumer protection statutes, such as the Children's Online Privacy Protection Act (COPPA), the Fair Credit Reporting Act (FCRA), the privacy and safeguards regulations promulgated under the Gramm-Leach-Bliley Financial Services Modernization Act of 1999 (GLBA), the Telemarketing Sales Rule (TSR) and the CAN-SPAM Act.[55] The authority to enforce specific laws (and to promulgate rules under these laws) is provided in the laws themselves. For example, COPPA, GLBA and the CAN-SPAM Act expressly give the Federal Trade Commission the power to make rules and to enforce the Acts and the rules.

It is important to note that the Federal Trade Commission's authority is limited in some respects. For example, the FTC Act states that the Federal Trade Commission may not regulate or enforce against certain industries that are otherwise regulated, such as financial institutions subject to jurisdiction of the Office of Comptroller of the Currency, the Federal Reserve, et al., and common carriers. The Federal agencies that regulate these industries often work closely with the Federal Trade Commission on privacy regulations, however. For example, the Federal Trade Commission works with a group of Federal financial institution regulators on GLBA rules, and it works with the Federal Communications Commission on telemarketing and email privacy rules as they relate to both financial institutions and common carriers.

Additionally, even where Federal Trade Commission authority does exist, companies are often subject to additional regulatory scrutiny. For example, companies often face both Federal Trade Commission and state attorney general actions for privacy or security breaches. Because the state attorneys general have independent authority, Federal Trade Commission actions do not preclude or supersede state action. In many cases, the consent decrees entered into with the state attorneys general for breaches exceed the Federal Trade Commission's requirements. Fines are also common at the state level.

Regulatory Processes

As described above, regulators generally have broad powers to receive complaints, conduct investigations, resolve matters informally, and to bring formal enforcement actions. For example, if the Federal Trade Commission suspects that a company has not complied with applicable laws, it will typically launch an investigation of the company. Depending on the situation, the Federal Trade Commission may work with the company to resolve the matter informally. For more egregious

breaches, or where the Federal Trade Commission detects a pattern of non-compliance, the Federal Trade Commission may bring a formal enforcement action against the company. These actions generally result in the Federal Trade Commission and the company entering into a settlement agreement or consent decree. The Federal Trade Commission has authority to include many different types of provisions in consent decrees, consistent with its role as a consumer protection agency.

Additionally, regulators often have broad discretion with regard to the terms they require to resolve investigations of companies. The case summaries illustrate the variety of provisions that regulators may demand. However, in the United States, there are also some common elements that are included in most settlement agreements. These common elements include:

(1) A prohibition on misrepresentation of privacy or security program protections, and/or a prohibition on any further unfair, deceptive or non-compliant conduct;

(2) A requirement to establish and maintain an appropriate compliance program or information security program; including, for security programs, (i) training and proper oversight of employees and agents, (ii) identification of reasonably foreseeable risks, (iii) the design of reasonable and appropriate controls and safeguards, and (iv) regular evaluation of the program;

(3) An order to delete inappropriately collected information or disgorge inappropriately obtained revenue; and

(4) An obligation to maintain certain records and documents related to the company's programs and compliance and to provide these records and documents upon request from the regulator; in some cases the company may be required to proactively notify the regulator of any change which may affect the company's compliance.

In many cases, regulators will also require the company to pay a fine or provide money for restitution to the individuals who were harmed by the violation.

Studying the various cases described in this guide can provide insight into the types of enforcement priorities that regulators have established as well as the steps that regulators believe are important for proper consumer protection in the privacy and security arena.

Analysis of an FTC Consent Decree

The following diagram presents a published Federal Trade Commission consent agreement, with annotations explaining the various parts and provisions. The particular agreement presented is the final order in the matter of the Federal Trade Commission vs. BJ's Wholesale Club. You can compare this original document to the case summary presented in Chapter 3 to understand the case summary process as well.

Figure 1.2: Dissection of a Standard FTC Consent Decree
(Source: the author, 2008)

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

In the Matter of BJ'S WHOLESALE CLUB, INC., a corporation.	FILE NO. 0423160 AGREEMENT CONTAINING CONSENT ORDER

The Federal Trade Commission has conducted an investigation of certain acts and practices of BJ's Wholesale Club, Inc., a Delaware corporation ("proposed respondent"). Proposed respondent, having been represented by counsel, is willing to enter into an agreement containing a consent order resolving the allegations contained in the attached draft complaint. Therefore,

IT IS HEREBY AGREED by and between BJ's Wholesale Club, Inc., by its duly authorized officers, and counsel for the Federal Trade Commission that:

1. Proposed respondent BJ's Wholesale Club, Inc. is a Delaware corporation with its principal office or place of business at One Mercer Road, Natick, Massachusetts 01760.

2. Proposed respondent admits all the jurisdictional facts set forth in the draft complaint.

3. Proposed respondent waives:

   A. any further procedural steps;

   B. the requirement that the Commission's decision contain a statement of findings of fact and conclusions of law; and

   C. all rights to seek judicial review or otherwise to challenge or contest the validity of the order entered pursuant to this agreement.

4. This agreement shall not become part of the public record of the proceeding unless and until it is accepted by the Commission. If this agreement is accepted by the Commission, it, together with the draft complaint, will be placed on the public record for a period of thirty (30) days and information about it publicly released. The Commission thereafter

Identifies the "respondent" – in this case, the respondent is BJ'S Wholesale Club, Inc., a legal person (a corporation) under Delaware law.

The facts relate to a security incident involving credit card data.*

The respondent agrees to enter this order and waives various procedural rights. The respondent cannot later challenge the validity of the order or dispute the underlying facts. These provisions provide the FTC with a clear path for future action, if the respondent fails to meet the terms of this consent decree.

may either withdraw its acceptance of this agreement and so notify proposed respondent, in which event it will take such action as it may consider appropriate, or issue and serve its complaint (in such form as the circumstances may require) and decision in disposition of the proceeding.

5. This agreement is for settlement purposes only and does not constitute an admission by proposed respondent that the law has been violated as alleged in the draft complaint, or that the facts as alleged in the draft complaint, other than the jurisdictional facts, are true.

6. This agreement contemplates that, if it is accepted by the Commission, and if such acceptance is not subsequently withdrawn by the Commission pursuant to the provisions of Section 2.34 of the Commission's Rules, the Commission may, without further notice to proposed respondent, (1) issue its complaint corresponding in form and substance with the attached draft complaint and its decision containing the following order in disposition of the proceeding, and (2) make information about it public. When so entered, the order shall have the same force and effect and may be altered, modified, or set aside in the same manner and within the same time provided by statute for other orders. The order shall become final upon service. Delivery of the complaint and the decision and order to proposed respondent's address as stated in this agreement by any means specified in Section 4.4(a) of the Commission's Rules shall constitute service. Proposed respondent waives any right it may have to any other manner of service. The complaint may be used in construing the terms of the order. No agreement, understanding, representation, or interpretation not contained in the order or in the agreement may be used to vary or contradict the terms of the order.

7. Proposed respondent has read the draft complaint and consent order. It understands that it may be liable for civil penalties in the amount provided by law and other appropriate relief for each violation of the order after it becomes final.

The respondent does not admit that it has violated any law. This statement is designed to limit the ability of other litigants to use this consent decree against the respondent.

Specific acknowledgement that the consent order may include a civil penalty (*i.e.,* a fine).

ORDER

DEFINITIONS

For purposes of this order, the following definitions shall apply:

1. "Personal information" shall mean individually identifiable information from or about an individual consumer including, but not limited to: (a) a first and last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name that reveals an individual's email address; (d) a telephone number; (e) a Social Security number; (f) credit and/or debit card information, including credit and/or debit card number, expiration date, and data stored on the magnetic stripe of a credit or debit card; (g) a persistent identifier, such as a customer number held in a "cookie" or processor serial number, that is combined with

Terms that are used in the order are defined to ensure that the respondent understands its obligations.

* The complaint is online at http://www.ftc.gov/os/caselist/0423160/050616comp0423160.pdf.

other available data that identifies an individual consumer; or (h) any other information from or about an individual consumer that is combined with (a) through (g) above.

2. Unless otherwise specified, "respondent" shall mean BJ's Wholesale Club, Inc. and its successors and assigns, officers, agents, representatives, and employees.

3. "Commerce" shall mean as defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 44.

I.

IT IS ORDERED that respondent, directly or through any corporation, subsidiary, division, or other device, in connection with the advertising, marketing, promotion, offering for sale, or sale of any product or service, in or affecting commerce, shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the personal information collected from or about consumers, including:

A. the designation of an employee or employees to coordinate and be accountable for the information security program.

B. the identification of material internal and external risks to the security, confidentiality, and integrity of personal information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management; (2) information systems, including network and software design, information processing, storage, transmission, and disposal; and (3) prevention, detection, and response to attacks, intrusions, or other systems failures.

C. the design and implementation of reasonable safeguards to control the risks identified through risk assessment, and regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures.

D. the evaluation and adjustment of respondent's information security program in light of the results of the testing and monitoring required by subparagraph C, any material changes to respondent's operations or business

arrangements, or any other circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of its information security program.

II.

IT IS FURTHER ORDERED that respondent obtain an assessment and report (an "Assessment") from a qualified, objective, independent third-party professional, using procedures and standards generally accepted in the profession, within one hundred and eighty (180) days after service of the order, and biennially thereafter for twenty (20) years after service of the order that:

A. sets forth the specific administrative, technical, and physical safeguards that respondent has implemented and maintained during the reporting period;

B. explains how such safeguards are appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the personal information collected from or about consumers;

C. explains how the safeguards that have been implemented meet or exceed the protections required by Paragraph I of this order; and

D. certifies that respondent's security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of personal information is protected and, for biennial reports, has so operated throughout the reporting period.

Each Assessment shall be prepared by a person qualified as a Certified Information System Security Professional (CISSP) or as a Certified Information Systems Auditor (CISA); a person holding Global Information Assurance Certification (GIAC) from the SysAdmin, Audit, Network, Security (SANS) Institute; or a similarly qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580.

Respondent shall provide the first Assessment, as well as all: plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, whether prepared by or on behalf of respondent, relied upon to prepare such Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) days after the Assessment has been prepared. All subsequent biennial Assessments shall be retained by respondent until the order is terminated and provided to the Associate Director of Enforcement within ten (10) days of request.

The meat of the consent decree: these paragraphs explain what the respondent must do (or not do) going forward.

In the complaint, the FTC alleged that:

> "the respondent's failure to employ reasonable and appropriate security measures to protect personal information and files caused or is likely to cause substantial injury to consumers that is not offset by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers. This practice was an unfair act or practice."

The steps ordered here are designed to provide the security necessary for fair trade practices. The respondent must implement specific controls and also have those controls assessed periodically by an independent third party. The respondent must provide copies of the initial assessment report to the FTC. Subsequent assessment reports are provided to the FTC upon request.

These provisions are common in FTC consent decrees involving claims of inappropriate security.

III.

IT IS FURTHER ORDERED that respondent shall maintain, and upon request make available to the Federal Trade Commission for inspection and copying, a print or electronic copy of each document relating to compliance, including but not limited to:

A. for a period of five (5) years: any documents, whether prepared by or on behalf of respondent, that contradict, qualify, or call into question respondent's compliance with this order; and

B. for a period of three (3) years after the date of preparation of each biennial Assessment required under Paragraph II of this order: all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, whether prepared by or on behalf of respondent, relating to respondent's compliance with Paragraphs I and II of this order for the compliance period covered by such biennial Assessment.

Consent decrees generally require the respondent to maintain compliance documents and provide them to the FTC upon request.

IV.

IT IS FURTHER ORDERED that respondent shall deliver a copy of this order to all current and future principals, officers, directors, and managers, and to all current and future employees, agents, and representatives having managerial responsibilities relating to the subject matter of this order. Respondent shall deliver this order to such current personnel within thirty (30) days after service of this order, and to such future personnel within thirty (30) days after the person assumes such position or responsibilities.

Consent decrees generally require the respondent to deliver copies of the order to individuals associated with the company (such as officers and employees) to ensure awareness of the obligations by everyone affected.

V.

IT IS FURTHER ORDERED that respondent shall notify the Commission at least thirty (30) days prior to any change in the corporation that may affect compliance obligations arising under this order, including, but not limited to, a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor corporation; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in either corporate name or address. *Provided, however*, that, with respect to any proposed change in the corporation about which respondent learns less than thirty (30) days prior to the date such action is to take place, respondent shall notify the Commission as soon as is practicable after obtaining such knowledge. All notices required by this Paragraph shall be sent by certified mail to the Associate Director, Division of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580.

Consent decrees generally require the respondent to notify the FTC if any events occur that may affect the company's compliance posture, such as a change of corporate ownership.

VI.

IT IS FURTHER ORDERED that respondent shall, within one hundred and eighty (180) days after service of this order, and at such other times as the Commission may require, file with the Commission an initial report, in writing, setting forth in detail the manner and form in which it has complied with this order.

Consent decrees generally require the respondent to confirm in writing to the FTC that the company has complied with the order.

VII.

This order will terminate twenty (20) years from the date of its issuance, or twenty (20) years from the most recent date that the United States or the Federal Trade Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order, whichever comes later; *provided, however*, that the filing of such a complaint will not affect the duration of:

A. any Paragraph in this order that terminates in less than twenty (20) years;

B. this order's application to any respondent that is not named as a defendant in such complaint; and

C. this order if such complaint is filed after the order has terminated pursuant to this Paragraph.

Provided, further, that if such complaint is dismissed or a federal court rules that respondent did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order will terminate according to this Paragraph as though the complaint had never been filed, except that the order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

The term of this consent decree is generally 20 years, so long as another complaint is not filed alleging a violation of the order.

Under the FTC Act, violations of an FTC order are punishable by a civil penalty of up to $11,000 per violation.

Signed this seventeenth day of May, 2005

BJ's WHOLESALE CLUB, INC.

By: _____
BJ's WHOLESALE CLUB, INC.

_____
DAVID MEDINE
JAMES W. PRENDERGAST
Wilmer Cutler Pickering Hale and Dorr LLP
Counsel for respondent BJ's Wholesale Club, Inc.

The company and the FTC sign the consent decree, asserting their assent to the terms. When signed, this is a binding agreement.

The FTC will sign after a vote of the Commissioners.

FEDERAL TRADE COMMISSION

By: _____
ALAIN SHEER
Counsel for the Federal Trade Commission

APPROVED:

_____
JOEL WINSTON
Associate Director
Division of Financial Practices

_____
LYDIA B. PARNES
Director
Bureau of Consumer Protection