ANTITRUST PUBLICATIONS – USER MANUAL -
Section 1 - Chapter Creation for Chapter Authors
BASE TEMPLATE + CHAPTER MACRO

This section of instructions covers the use of the Base Template and the Chapter Macro for creating and formatting Chapters.

Base Template

ABA.dotm – This template will format your manuscript and has the Custom Styles your manuscript needs to run all the necessary macros.

Chapter Macro

ABA_Chapter.docm – This macro is used to format all Chapter files. This Macro puts vital information into the Word document that will affect the running headers, footer page numbers, footnotes, restarting the sub-heading numbers, and preparing the Chapter for the other macros that will be run later in this process. Make sure your manuscripts end with the document extension (.doc) or (.docx).

STEP 1

A. Chapters Already Started in Word

If you have already created your Chapter in a Word document using typical default Word styles, you will need to rename the styles to match the Custom Styles shown below. This step is necessary because the Base Template and Chapter Macro are designed to search for these Custom Styles. If you do not take this step to re-name your styles, the Base Template and Macros will not run properly on your Chapter, and your formatting will be incorrect. Exhibit A identifies the relevant Custom Styles and locations. For example, if your original manuscript labeled the first level outline header for a paragraph as “Paraheading,” you must re-name it “Heading 1.”

<table>
<thead>
<tr>
<th>CUSTOM STYLES</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABA Paragraph</td>
</tr>
<tr>
<td>Affiliation</td>
</tr>
<tr>
<td>AppendixNumber</td>
</tr>
<tr>
<td>AppendixTitle</td>
</tr>
<tr>
<td>AppendixTitle-2lines</td>
</tr>
<tr>
<td>AckHeading</td>
</tr>
<tr>
<td>Block Quote</td>
</tr>
<tr>
<td>BMHead 1, BMHead 2, etc. (for Backmatter headings only)</td>
</tr>
<tr>
<td>ChapterNumber</td>
</tr>
<tr>
<td>ChapterTitle</td>
</tr>
<tr>
<td>ChapterTitle-2lines</td>
</tr>
<tr>
<td>DedHeading</td>
</tr>
<tr>
<td>Footnote Block Quote</td>
</tr>
<tr>
<td>Footnote Text Para</td>
</tr>
<tr>
<td>ForewordHeading</td>
</tr>
<tr>
<td>FrontMatterHeading</td>
</tr>
<tr>
<td>Glossary Paragraph</td>
</tr>
<tr>
<td>GlossaryTitle</td>
</tr>
<tr>
<td>Heading 1</td>
</tr>
<tr>
<td>Heading 2</td>
</tr>
<tr>
<td>Heading 3</td>
</tr>
<tr>
<td>Heading 4</td>
</tr>
<tr>
<td>Heading 5</td>
</tr>
<tr>
<td>IntroHeading</td>
</tr>
<tr>
<td>PrefaceHeading</td>
</tr>
<tr>
<td>List Number, List Number 2, etc</td>
</tr>
<tr>
<td>List, List 2, etc (UNNUMBERED)</td>
</tr>
<tr>
<td>List Bullet, List Bullet 2, etc</td>
</tr>
</tbody>
</table>
B. **Chapters Not Yet Started**

If you have not started typing your Chapter in Word already and are starting your document from scratch, you will need to open the Base Template file (ABA.dotm) and immediately SAVE the file following the naming conventions below before you begin typing the Chapter. Then begin typing your manuscript.

**Example of file name:**

- 01-Chapter_1.docx or 01-Chapter_1.doc
- 02-Chapter_2.docx or 01-Chapter_2.doc
- 03-Chapter_3.docx or 01-Chapter_3.doc

- Do not use SPACE in the file name, instead use hyphen or underscore. You can use .doc or .docx (Word 2010 and later) extension, but only one of these at a time. You must be consistent in the document extensions or the macros will not run properly.

**After your Styles are correctly named and your Chapter text is complete move to Step 2 to continue formatting the Chapter.**

**STEP 2**

**A. Running the Chapter Macro on your Chapter file(s).**

*(You need to run the Chapter Macro on ALL Chapters created, including the ones using the Base Template.)*

1. Create a FOLDER on your Desktop (name it whatever you like).

2. Place the **ABA.dotm** (Base Template) file in the FOLDER on your Desktop.
3. Place the **ABA_Chapter.docm** (Chapter Macro) file in the FOLDER.

![Image of folder with files]

4. Now place the Word document that needs formatting in the FOLDER.

![Image of folder with files]

5. Double click on **ABA_Chapter.docm** (Chapter Macro). The macro and template rules will be automatically applied to the Chapter Word Document placed in the FOLDER. A small dialog box will prompt you to enter the title of the book you are currently working on.

![Image of dialog box]

6. Enter the title and press OK. After you click OK, the macro rules and formats will be applied to the document file.
If the document is styled in a different manner or the Chapter Title style is not included in the document, the following prompt will appear.

7. Click OK and enter the chapter title.

8. A "Process Completed" window will appear after a successful run of the Chapter Macro.

9. Click OK and return to the FOLDER on your Desktop and open Chapter Word document 01-Chapter_01.docx to see the results.

10. You can place multiple Chapter files in the FOLDER and run the Chapter Macro on multiple Chapters all at once if necessary.

To assemble and properly format the entire manuscript, including the Forward, Table of Contents, etc., go to Section 2 which is the Guide for Manuscript Formatting and Completion.
EXHIBIT A

EXAMPLES OF LOCATIONS
OF CUSTOM STYLES IN
YOUR CHAPTER
A. Constitutional Recognition of Privacy

While the United States Constitution does not contain an explicit "right to privacy," privacy protections are implicit in the Fourth Amendment, which provides for the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." The Fourth Amendment applies to government actions and protects an individual against government intrusion.

The Supreme Court has held that a "search" occurs when the government infringes upon "an expectation of privacy that society is prepared to consider reasonable," whether an expectation of privacy is reasonable, the Court should consider whether the victim has manifested a subjective expectation of privacy, and second, whether society is willing to recognize that expectation as reasonable. If a reasonable expectation of privacy exists, then the government must obtain a warrant to conduct the search.

In United States v. Katz, the Supreme Court extended the Fourth Amendment's protections to certain physical areas (in this case, a telephone booth), that an individual "seeks to preserve as private." In

4. Id., at 351.
United States v. Jacobsen, the Court expanded the protection to written communications.5

The Supreme Court has yet to decide whether there is a reasonable expectation of privacy in electronic communications (e.g., emails, and other data). The Court has suggested that a search of an individual’s email without a warrant would be tantamount to an unreasonable search of the person.6 In 2010, the Sixth Circuit following the Jacobsen and Katz precedents, became the first circuit to find a reasonable expectation of privacy in emails delivered through a commercial Internet Service Provider (ISP).7 During the 2012 term, the Supreme Court unanimously held in United States v. Jones8 that warrantless tracking by a GPS-surveillance device constitutes an illegal search under the Fourth Amendment.

B. Regulatory Structure

1. Federal Trade Commission

The Federal Trade Commission (FTC) is the only federal agency with consumer protection and competition authority over broad sectors of the economy. Established in 1914, the FTC was initially given a mandate to regulate “unfair methods of competition.”9 In 1938, the FTC Act was expanded to protect consumers against “unfair or deceptive acts or practices in commerce.”10 In the absence of an overarching federal data protection law, the Commission often reviews putative privacy

5. Jacobsen, 466 U.S. at 114 (“Letters and other sealed packages are in the general class of effects in which the public at large has a legitimate expectation of privacy.”).
6. City of Ontario v. Quon, 130 S. Ct. 2619, 2631 (2010) (implying that “searching a personal e-mail account” is as intrusive as “a wiretap on that individual’s home phone line”).
violations as a potentially unfair or deceptive act. The FTC is also authorized by statute to enforce the following sectoral privacy acts: Gramm-Leach-Bliley, the Fair Credit Reporting Act, and the Children’s Online Privacy Protection Act. Together with the Federal Communications Commission, the FTC also enforces marketing communications laws, such as the Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act and Telephone Consumer Protection Act (TCPA) of 1991.

2. Federal Communications Commission

The Federal Communications Commission (FCC) is authorized to prescribe certain privacy rules under the CAN-SPAM Act and the TCPA. The FCC protects Customer Proprietary Network Information (CPNI), including “some of the most sensitive personal information that telecommunications carriers and interconnected VoIP providers have about their customers as a result of their business relationship,” by requiring those carriers and providers to annually certify CPNI compliance.


13. The FTC specifically addressed an instance where compliance with the HHS rule would be deemed compliance with the FTC regulation:

Thus, in those limited circumstances where a vendor of personal health information renders a service directly with these individuals on behalf of a HIPAA-covered entity, information provided to such entity at the same time that it provides such notice at the same time that it provides an FTC-mandated notice to its direct customers for the same breach, the FTC will deem compliance with HHS requirements.
Another significant aspect of PIPEDA is that it requires consent for the collection, use, and disclosure of what many would consider to be publicly available information, such as information contained in public records or posted on a website.

a. Department of Commerce

The Department of Commerce, through its International Trade Administration (ITA), plays a key role in "promoting policy frameworks to facilitate the free flow of data across borders, as well as the growth of digital commerce and international trade." The ITA also administers the EU Safe Harbor framework, which requires that US-based signatories grant access, provide adequate notice, and offer opt-out rights to European data subjects. In addition to the ITA, two other Commerce departments—the National Institute of Standards and Technology (NIST) and the National Telecommunications and Information Administration (NTIA)—work closely with the Executive Office of the President and U.S. industry to develop international standards for cybersecurity and data privacy. For example, in 2010 the Internet Policy Task Force began conducting a comprehensive review of the nexus between privacy policy and the Internet economy and since 2012 has been facilitating multistakeholder meetings on various topics such as facial recognition technology and how mobile devices handle personal data.

---

Footnote Text Para


(1) Department of Health and Human Services

Under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Department of Health and Human Services (HHS) is authorized to promulgate rules to protect the privacy and security of personal health information. The HIPAA Privacy and Security Rules, which were finalized in 2003, are enforced by HHS and the State Attorneys General.

(2) State Legislatures and State Attorneys General

Many state legislatures have addressed privacy and data security issues. In addition, the State Attorneys General are the chief legal officers of their respective states, charged with (among other duties) the enforcement of their state statutes, including state consumer protection statutes. These statutes contain prohibitions against “unfair or deceptive acts and practices” and are often referred to as “UDAP” statutes. Using their consumer protection authority, the Attorneys General have brought actions against DoubleClick for failure to disclose the use of cookies, and Toys "R" Us for failing to obtain user consent prior to sharing personal data with a third party.16

(A) THE SECTORAL APPROACH TO DATA SECURITY

The federal government’s legislative and regulatory approach on information security, data, and privacy protection issues has to date mostly been reactive. As new technologies were developed, or new practices for existing technologies were devised, security and privacy concerns quickly emerged, as privacy implications were often ignored. Legislative responses, where forthcoming, generally lagged developments in technology and came into force only well after new technologies or practices had already become widespread. In some instances, particular technologies or practices had already been supplanted by even newer ones not even in existence when legislation was being crafted.

16. Id...
Unlike Europe, the United States currently has not legislatively created general data protections or enforceable privacy rights protecting individuals’ privacy and personal information, outside of specific actions in certain contexts. Instead, federal laws that regulate information security, data, or privacy in the United States do so largely only in particular contexts, although they often share characteristics with similar laws operating in related contexts. Within these contexts, some federal laws and regulations that address information, data, and privacy issues have remained virtually unchanged for decades, yet technology and behavior have changed, the FTC has significantly. Other laws, however, have been regularly updated or amended. Since the last publication of this Handbook in 2008, to highlight only two of the changes, the FTC has issued major regulatory guidance to protect children’s information online, and has fostered and evaluated a self-regulatory regime for advertisers targeting consumers based on information collected online.

Further reflecting the pace of change at the federal level, Congress has heard scores of hearings within the last two sessions related to data security and privacy issues, and at least twelve bills have been introduced in the current Congress that relate to data security or breaches, ‘geo-location’ privacy, and electronic communications, or that otherwise address consumer or commercial privacy protections. Against this dynamic backdrop, an overview of the existing federal laws and regulations governing data security and privacy issues is provided below, organized into three contexts that may help to frame a review and analysis of the laws operating within this environment:

1. Laws that directly regulate public (federal agencies), rather than private, behavior;
2. Laws that regulate specific types of information, or private industries; and
3. Laws developed in law enforcement or intelligence contexts, frequently having both criminal and civil components.

Where Congress has passed federal legislation affecting information security or privacy protections in the private sector, it has done so largely sector-by-sector, responding to particular concerns raised by practices in those sectors. Within this “sectoral” approach, federal legislation specifically regulates several particular industries’ use of information viewed as meriting unique protections, including: financial or credit data; health or medical data; children’s data; proprietary information or trade secrets; and varying types of personal information collected and used by telecommunications, cable, or video providers, and the states. Supplementing this industry-by-industry approach to the private sector are certain data security and privacy protections derived from the FTC Act’s prohibition against deceptive or unfair acts or practices, and certain self-regulatory regimes also fostered by the FTC that operate under a mix of rules and principles that have guided and encouraged their development.

18. See generally 15 U.S.C. § 45 (FTC Act’s prohibition against unfair or deceptive trade practices). The FTC Act generally empowers the FTC to prevent unfair methods of competition and unfair or deceptive acts or practices. Additionally, the Act also allows action where any particular practice inflicts substantial harm on consumers that could reasonably be avoided, and doesn’t offer offsetting benefits. 15 U.S.C. § 45(n).
While this overall sectoral approach has generated both criticism and recognition that in some ways it may provide more benefit than a more comprehensive framework, in practice many industry-specific restrictions often overlap and mutually reinforce each other. Notably, the FTC often brings enforcement actions alleging that single practices violate multiple laws. In these areas, analyzing on broad themes and general enforcement priorities pursued by the FTC often provides more insight than focusing on only each statute’s prohibitions.

Consumer Privacy

Although some nuances have developed in applying Section 5 to data security or privacy practices, the FTC’s authorities and legal standards for determining if acts or practices are unfair or deceptive are generally the same as in other contexts. Under Section 5 of the Act, a representation, omission, or practice may be considered deceptive if (1) it is likely to mislead consumers acting reasonably under the circumstances, and (2) it is material, that is, likely to affect consumers’

19. Such criticisms include: creation of data or privacy protections on a “piece-meal” basis that impose extra compliance burdens because of lack of standardization and uncertainty for consumers to anticipate how their information may be used in any context. Further, having no lead or single agency with primacy on data security or privacy relegates the issues subordinate to other agency responsibilities, ensures many issues that do not fall within the purview of any particular agency remain largely unaddressed, and lessens the opportunity for administrative continuity, knowledge, or incremental development of initiatives.

conduct or decisions with respect to the product at issue. An act or practice may be considered unfair if the injury it causes or is likely to cause to consumers is (1) substantial, (2) not outweighed by countervailing benefits to consumers or to competition, and (3) not reasonably avoidable by consumers themselves.

Application of these criteria to often rapidly changing technologies or business practices can be both challenging and problematic. As consumers' and businesses' interactions evolve through various mediums and methods, expectations about what is reasonable consumer behavior, what practices might be considered reasonably avoidable, and how beneficial countervailing benefits might be at any given moment, continue to evolve. To address these challenges, the FTC regularly issues policy guidance, organizes workshops, and provides educational materials and outreach. FTC policy guidance is mostly developed through varying degrees of stakeholder participation, and can sometimes reflect consensus between agency policy-makers and interested actors (e.g., industry, academia, civil society, consumers generally). In addition, FTC policy guidance can signal agency concerns over emerging practices or technologies that might constitute deceptive or unfair acts, or might warrant an enforcement action, even if such statements do not rise to the level of legally enforceable provisions. Finally, FTC policy guidance may also provide a signal to Congress—specifically congressional committees with FTC oversight—about particular industry practices or privacy concerns.

21. Stouffer Foods Corp.... 118 F.T.C. 746, 798 (1994); Kraft, Inc...., 114 F.T.C. 40, 120 (1991); aff'd, 970 F.2d 311 (7th Cir. 1992); Remoucheron Int'l Corp...., 111 F.T.C. 206, 308-09 (1988) (citing, for example, Southwest Sunsets, Inc. v. FTC, 785 F.2d 1431, 1436 (9th Cir.)); International Harvester Co., 104 F.T.C. 949, 1056 (1984);

b. Policy

The FTC has developed numerous policy guidance documents relating to unfair and deceptive acts or practices in a variety of contexts. A key document is the FTC’s Policy Statement on Deception and Unfairness, which provides a baseline by which specific policies relating to online disclosures, data security, and general privacy practices can be evaluated.

The FTC’s Policy Statement on Deception describes three general conditions necessary to find an act or practice deceptive:

1. There must be a representation, or practice that is likely to mislead a consumer;
   a. the act or practice must be considered from the perspective of a reasonable consumer;
   b. improve notice, disclosure, and consent procedures to streamline, shorten, and improve their relevance and usability for consumers; and
2. The representation, omission, or practice must be material.

Similarly, although the contours of practices considered unfair has changed substantially over time, the FTC’s Policy Statement on Unfairness currently depicts unfair practices as:

As commerce has moved online, and as consumers and Congress have expressed growing concern over data collection and sharing over the Internet, the FTC has found it necessary to supplement these general guidelines with more specific policy statements that further refine its

---

25. For an historical review of the development of the FTC’s use of its authority to prohibit unfair practices, see J. Howard Beales, III, The FTC’s Use of Unfairness Authority: Its Rise, Fall, and Resurrection, available at http://www.ftc.gov/speeches/beales/unfair0603.shtm.
authority to prohibit certain privacy and data security practices as unfair and/or deceptive. 26

In 2012, the FTC issued its final privacy report Protecting Consumer Privacy in an Era of Rapid Change. This new framework, which built on the principles identified in the 2010 FTC Staff report, 27 attempts to harmonize FTC policies and existing law with developments in technology, and with other executive branch activities. Building upon the OBA Self-Regulatory Principles, the Privacy Reports expanded the framework beyond OBA and established an overall framework for consumer privacy.

Privacy and data protection requirements in Canada originate from a number of sources, depending on the nature of the information in question and the jurisdiction from which the information was collected or in which it is held.

(1) Baseline Data Security and Privacy Guidelines

In March 2007, the FTC released Protecting Personal Information: A Guide for Business, 28 intended as a practical guide for businesses in developing and maintaining a sound data security plan. The guide urges businesses to develop a data security plan based on the following five principles, and provides recommendations on how to implement these principles in practice:

26. For instance, to address the practice of online behavioral advertising, the FTC issued self regulatory principles for industry to follow when tracking a consumer's activities, over time, “in order to deliver advertising targeted to the individual consumer’s interests.” See FTC, Online Behavioral Advertising: Moving the Discussion Forward to Possible Self-Regulatory Principles (Dec. 20, 2007), available at http://www.ftc.gov/os/2007/12/P859900stmt.pdf.


Know the kinds of personal information to collect;
- Keep only the information they need;
- Protect the information that they have, including:
  - Maintaining physical security;
  - Maintaining electronic security;
  - Maintaining security practices for contractors and service providers;
- Dispose of information properly; and
- Plan ahead, so they know how to react in case of a security breach.

In its *Dot Com Disclosures*, the FTC provides guidance on the related topic of how businesses should continue to follow general principles of advertising law when operating online. 29 Rather than addressing data security protections, the *Dot Com Disclosures* provide practical guidance on how businesses should provide disclosures of additional terms or conditions of online advertisements, including what should be done to ensure they are “clearly and conspicuously” displayed. 30

Although both sets of guidelines remain useful, they have been somewhat overshadowed by more recent FTC privacy guidance and frameworks. The 2009 *Self-Regulatory Principles for Online Behavioral

---

30. The FTC in May 2012 hosted a conference, *In Short: Advertising and Privacy Disclosures in a Digital World*, addressing the need for revisions to the twelve-year old *Dot Com Disclosures* as well as emerging issues related to mobile privacy disclosures. For a webcast and related workshop materials, see http://ftc.gov/bcp/workshops/inshort/index.shtml.
Advertising, covered a relatively narrow industry—companies engaged in the practice of online behavioral advertising (OBA).\(^{31}\)

Another significant aspect of PIPEDA is that it requires consent for the collection, use, and disclosure of what many would consider to be publicly available information, such as information contained in public records or posted on a website.

(A) SPECIFIC ONLINE BEHAVIORAL ADVERTISING GUIDANCE

In 2009, the FTC issued a set of principles designed to provide industry with guidelines that could be applied to self-regulatory efforts. The principles were not binding rules, but rather a framework to encourage industry to develop its own self-regulatory codes.\(^{32}\) The 2009 OBA Report included four principles that the FTC asserted should guide the development of any self-regulatory regimes covering online behavioral advertising. Formally the four principles (Self-Regulatory Principles) are only advisory as they lack the force of law; however, the FTC will treat them as a baseline for evaluating self-regulatory efforts. Although they have been further refined by the FTC’s subsequent

31. The Principles were contained in a staff report, issued in 2009. See FED. TRADE COMM’N SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING (2009), [hereinafter OBA REPORT] available at http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf. “Online behavioral advertising” is defined in the OBA Report as “the tracking of a consumer’s online activities over time . . . in order to deliver advertising targeted to the individual consumer’s preferences.” Although the report and principles focus on OBA, the report notes that the principles largely follow the FTC’s prior approaches in related areas involving unfair or deceptive trade practices applied to privacy policies and security protections. See, e.g., id. at 40 (“It is fundamental FTC law and policy that companies must deliver on promises they make to consumers about how their information is collected, used, and shared.”); id. at 5 (reviewing FTC enforcement actions against deceptive privacy claims and improper disclosure of consumer data).

32. However, the principles do incorporate policy choices about what self-regulatory codes should contain, how they should operate, and what practices might warrant possible enforcement actions or encourage the Commission to reconsider a more regulatory approach.
issuance of a new privacy framework, these principles remain valid in
guiding companies’ activities when practicing OBA. The four principles
are summarized below:

<table>
<thead>
<tr>
<th>Principle</th>
<th>Guidance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transparency and Consumer Control</td>
<td>Websites that collect consumer data for OBA should disclose any collection and explain whether consumers have a choice as to whether the information is collected and used. Disclosures should be clear and accessible to consumers.</td>
</tr>
<tr>
<td>Data Security and Retention</td>
<td>Consumer data should be accorded “reasonable” security, tailored to the sensitivity of the collected data, the nature of the business for which it is collected, the types of risks the company faces, and what reasonable protections are available. Further, consumer data should only be retained as long as necessary to fulfill a legitimate business or law enforcement need.</td>
</tr>
<tr>
<td>Opt-In Consent for Sensitive Data Collection</td>
<td>If the consumer data being collected is “sensitive,” the consumer should affirmatively and expressly agree to any data collection before it occurs. The FTC did not fully define “sensitive” data, deferring to industry and policy-making stakeholders. Nevertheless, the FTC indicated that it considered financial information, health information, information about children, information about precise geographic location (geo-location</td>
</tr>
</tbody>
</table>
Affirmative, Express Consent for Retroactive Changes

If a company seeks to change its privacy policy and retroactively apply the new policy to data collected *prior to* the policy change, a company should obtain the affirmative, express consent of the consumer before implementing any such change.

### 1. Department of Health and Human Services

Under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Department of Health and Human Services (HHS) is authorized to promulgate rules to protect the privacy and security of personal health information. The HIPAA Privacy and Security Rules, which were finalized in 2003, are enforced by HHS and the State Attorneys General.

### 2. FTC Privacy Reports

The FTC Privacy Reports signal the FTC’s evolving attitudes towards self-regulatory regimes by identifying three core principles: simplified choice, greater transparency, and privacy by design. While both *Privacy Reports* lack the force of law, they were issued to influence and guide policymakers, including those in Congress, and may signal the Commission’s future enforcement priorities.

While maintaining flexibility to accommodate the development of new technologies and practices, the reports provide a series of best practices to guide industry in its approach to privacy and data security practices. Notably, these best practices are intended to apply not only to “online” companies that engage in behavioral advertising, but also more generally to any company that might “collect, maintain, share, or otherwise use consumer data that can be reasonably linked to a specific
consumer, computer or device.” These best practices seek to encourage businesses to:

- incorporate data security and privacy protections into systems and practices proactively as they are being designed (privacy by design);
- improve notice, disclosure, and consent procedures to streamline, shorten, and improve their relevance and usability for consumers; and
- recommend the further implementation and refinement of Do Not Track systems that easily allow consumers to opt-out of data collection, use, or sharing.

Privacy by Design. The Final Report supports Privacy by Design, a principle encouraging companies to build in privacy during the initial stages of any product and/or service design. The concept includes both active privacy protections, such as implementing reasonable data security measures and retention practices, and more passive methods, such as minimizing unnecessary data collection. Furthermore, Privacy by Design implies companies should update their data management procedures as their products and practices change.

(3) Greater Transparency

The FTC also urged companies to increase the transparency of their data practices. Privacy policies should be clearer, shorter and more standardized, to enable consumers to better understand and compare them. Furthermore, companies should provide consumers reasonable access to the data they maintain. If companies wish to use the data they have collected in a manner materially different, the company must provide prominent disclosures of that fact, and obtain affirmative

33. PRIVACY REPORT, supra note 18, at v.
consumer consent prior to the new use. The Commission also called for greater consumer education about commercial data practices.

c. Enforcement

When the FTC does bring an enforcement action, its remedies are not restricted to any single alleged violation of a specific law or regulation. The Commission routinely pursues orders that extend beyond the scope of the precise violation alleged in order to “fence in” the conduct, as long as that conduct is “reasonably related” to the violation. For example, in 2006, the Fourth Circuit Court of Appeals upheld an FTC order against Telebrands. The FTC filed an administrative complaint against Telebrands for its advertisements of an alleged weight-reducing belt. The administrative law judge held that Telebrands made false and misleading claims in violation of the FTC Act. The Commission’s order required not only substantiation for claims related to weight-reducing belts, but also for “any food, drug, dietary supplement, device, or other product, service or program” offered by Telebrands. The court stated:

The FTC considers three factors in determining whether order coverage bears a reasonable relationship to the violation it is intended to remedy (1) the seriousness and deliberateness of the violation, (2) the ease with which the violative claim may be stated in connection with other products, and (3) whether the respondent has engaged in prior violations. In reviewing FTC orders for the existence of a reasonable relationship between the remedy and the violation, courts have relied on these same factors. The court also stated that this analysis “operates on a sliding scale—any one factor’s importance varies depending on the extent to which the others are found.”

The FTC’s enforcement jurisdiction under Section 5 of the FTC Act currently is subject to a significant litigation challenge. On January 26,

35. Jacob Siegel Co. v. FTC, 327 U.S. 608 (1946).
36. Telebrands Corp. v. FTC, 457 F.3d 354 (4th Cir. 2006).
37. Id., at 358 (citations omitted).
38. Id.,
2012, the FTC filed suit against Wyndham Worldwide Corp. ("Wyndham") and three of its subsidiaries, alleging that Wyndham engaged in "unfair practices" by making misleading representations on its websites regarding the company’s safeguarding of customer information. The FTC also alleged that Wyndham failed to maintain reasonable data security practices, leading to three separate data breaches. In response, Wyndham challenged the FTC's authority to regulate private companies' data security under Section 5 of the FTC Act. Wyndham argued, among other things, that before bringing an enforcement action under Section 5, the FTC must publish "rules, regulations, or other guidelines" regarding data security standards, and that it had not done so here.

C. General Trends in State Law

To date, forty-six states, the District of Columbia, Puerto Rico, and the U.S. Virgin Islands have enacted specific legislation that addresses the notification process an organization must follow upon the discovery of a data breach. Alabama, Kentucky, South Dakota, and New Mexico are the only states that have not enacted security breach legislation.