Avoid Legal Traps When Drafting a Privacy Policy

Michelle Tyde and Brooke McGuffey

Daily Report

October 26, 2016

In the United States, there is no single federal law that requires a company to have a privacy policy. Some laws mandate it under certain circumstances, including the following:

- **The Children's Online Privacy Protection Act** (COPPA) requires commercial websites and online services (including mobile apps) that knowingly collect information about, or target children under age 13, to post a clear and comprehensive online privacy policy;
- **The Gramm-Leach-Bliley Ac**t requires institutions "significantly engaged" in financial activities to give "clear, conspicuous, and accurate statements" of their information-sharing practices;
- **The Health Insurance Portability and Accountability A**ct (HIPAA) requires companies engaged in health care services to give written notice of its privacy practices; and
- **California law** (Calif. Bus. & Prof. Code §§ 22575-22578) requires an operator of a commercial website or online service (including mobile apps) that collects personally identifiable information (PII) about California residents to post a Privacy Policy on its website.

Even if a privacy policy is not required by law, the Federal Trade Commission (FTC), the nation's chief privacy and data security enforcement agency, encourages businesses to give consumers written notice of the company's privacy practices when collecting and using PII, including how the company collects, uses and discloses PII. In recent years, the FTC has increasingly brought actions against companies that failed to follow their own stated privacy policies as an unfair and deceptive trade practice. Thus, it is crucial to draft a privacy policy carefully; poor drafting can create traps for the unwary and open a company up to liability.

It is a common mistake to focus on privacy protection when drafting a policy. For example, statements such as "your privacy is important to us" or "we respect your privacy" or "protecting your information is our #1 priority" are not legally required and can form the basis of consumer class actions and/or FTC enforcement actions. Rather, the focal point should be giving consumers' notice of your company's privacy practices (i.e., what information it collects from consumers, how it uses and shares such information, and a consumer's choice with respect to such practices). Keep the following tips in mind when drafting and/or revising your company's privacy policy to avoid similar traps.

Accurately reflect the company's actual privacy practices. The policy must state what a company does, and the company must do what the policy states. Misalignment of the policy's statements with the company's actual practices is one of the most common and significant missteps that leads to liability.

One size does not fit all as each company's practices differ. Thus, you cannot simply use a form or draft a privacy policy without conducting due diligence as to:

- The types of information collected and ways in which it is collected;
- How the company uses such information;
- How the company protects collected information;
- Whether the company shares collected information with others, and if so, what is shared and with whom;
- The company's retention practices; and

- Any controls or choices that the customer has with respect to such collection and use. Consult with multiple stakeholders across your company when conducting such diligence (e.g., IT, marketing, different business units, etc.).

Consider future business plans and potential changes. It is important to strike a balance between providing detailed information about current practices and providing flexibility for future changes, which can be difficult to achieve. Consider both positive changes and negative ones. For example, the policy should expressly contemplate how the consumer's information will be handled in the event of a sale or a merger, as well as in bankruptcy.

Be clear and concise so that the average consumer can understand the company's practices. Use short sentences, active voice, and bullet points to organize the information logically. If a consumer cannot understand the policy, it increases the risk of an unfair or deceptive trade practice claim.

Avoid boilerplate and legalese. The policy is not intended to be a contract but rather a statement of the company's privacy practices.

Choose your words carefully. For example, tracking technologies such as persistent identifiers and IP addresses make it easier to personally identify a consumer. Keep in mind that the FTC has expanded the definition of PII to include any information that can reasonably be used to identify an individual, so companies should carefully identify their practices regarding new tracking technologies. Additionally, do not include statements that are not legally required, such as discussing your company's security measures in detail (e.g., "we use the best encryption software in the industry"), which can form the basis for a breach of warranty claim or a negligence action.

Do not make promises that you cannot keep. For example, no one can guarantee security; thus, avoid statements such as "your personal information is protected from unauthorized access," "your financial information is completely secure." Also, avoid absolute statements such as "we will never disclose your information to a third party."

Disclose both collection practices that are apparent and the use of tracking technologies. This includes personal information actually provided by the consumer, as well as the use of any tracking technologies that collect information automatically including cookies, IP address, web beacons and geolocation information.

Include disclosures required by state law. For example, both California and Delaware require statements on "Do Not Track."

Review and revise your company's policy regularly. Do this as needed to reflect changes in business practices, evolving technology and compliance with applicable laws and regulations.

Specify how you will implement changes to the policy and give notice thereof. The FTC requires companies to give consumers notice of material changes in the policy and obtain affirmative express consent prior to making certain material retroactive changes to their privacy practices. Companies should differentiate between these two concepts and not design a one-size fits all approach to notification of changes.

While the tips in this article will assist drafters in avoiding some of the traps for the unwary, you should consult with an experienced privacy attorney for guidance when drafting a new privacy policy or considering changes to an existing one.

Michelle Tyde, counsel at Kilpatrick Townsend & Stockton, focuses her practice on intellectual property/technology transactions and privacy and data security matters. She is a certified Information Privacy Professional (CIPP/US) by the International Association of Privacy Professionals. Brooke McGuffey, associate at Kilpatrick Townsend & Stockton, focuses her practice on information technology, data security and privacy, and technology transactions. She is a certified Information Privacy Professional (CIPP/US) by the International Association of Privacy Professionals.