Drafting Privacy Policies

by Elizabeth C. Rogers, Greenberg Traurig, LLP

Elizabeth C. Rogers is a shareholder in Greenberg Traurig's Cybersecurity, Privacy and Crisis Management practice group.

While there is no universal legal requirement that every company have a published privacy policy, consumers have become increasingly sensitized to the data collection practices of companies with which they do business. Often, they expect to be able to examine a company's privacy policy to learn how their data will be handled, which could impact their decision to do business with that company. Consequently, if your client collects consumer data via the Internet or otherwise (e.g., by accepting credit card payments, operating a website, or having an online marketing presence), it should create a privacy policy that it can maintain and which contains universally recognized privacy principles.

This practice note discusses the key issues that a practitioner should consider when drafting or reviewing a client's privacy policy, including:

- The types of personal information collected by the client
- Relevant legal and regulatory requirements
- What information to include in the policy
- The importance of adhering to the policy in practice

Privacy Policy Basics

A privacy policy is an external-facing statement that specifies a company's practices regarding the collection, use, and sharing of customer or consumer data (in most cases, such companies own or operate websites, mobile applications, social media platforms, or the like, though any company may have a privacy policy). It is distinct from a company's overall enterprise-wide program for processing personally identifiable information (PII) or any other information regulated by law.

A privacy policy should be viewed as a binding, enforceable agreement. While breach of contract claims based on privacy policy violations have been largely unsuccessful (either because the policies were not contractual in nature or the plaintiffs failed to adequately allege the requisite harm), the Federal Trade Commission (FTC) regularly brings enforcement actions against companies that misrepresent their privacy practices (in privacy policies or otherwise). For more on FTC enforcement, see Importance of Adhering to the Policy below.

It is therefore crucial to not only have a well-crafted policy that addresses any legal or regulatory requirements, but also to ensure that the organization adheres to the policy in practice.

What Personal Information Is Collected?

Because privacy policies need to be tailored to an organization's industry and business processes, as a first step in drafting or reviewing a privacy policy, you must identify the kinds of personal information that your client is, or will be, collecting from customers or consumers. Such information is commonly referred to as personally identifiable information (PII).

While there is no universal definition of PII, it is generally considered "any information that can be used to distinguish or trace an individual's identity" or "any other information that is linked or linkable to an individual." See National Institute of Standards and Technology, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, NIST Special Publication 800-122 (2010).

For instance, the following types of PII may be obtained in a commercial transaction:

- Name
- Address

- Telephone number
- Email address
- Credit card information
- Banking account information

Derivative data may also be collected or generated from commercial transactions, such as purchase history, customer preferences, and geo-locational data.

Companies in the healthcare or life sciences industries (e.g., health care providers, pharmacies, medical device manufacturers) and their downstream contractors and service providers may capture medical information related to age, health, prescription medication, or insurance or medical claim related data. Such information is commonly referred to as personal health information (PHI) and is a type of PII.

Other types of PII may include educational or employment information, personal identification numbers (e.g., social security numbers or driver's license numbers), date and place of birth, and biometric records (e.g., photographs, fingerprints, x-rays).

Legal & Regulatory Considerations

An appropriate privacy policy must not only address the kinds of data that are being processed, but also should consider the legal and regulatory requirements concerning the collection and use of that data.

Unlike other nations, there is no comprehensive, uniform data privacy law in the United States. Instead, various federal and/or state laws regulate data privacy, generally by industry sector. Thus, the requirements of a privacy policy are often dictated by the laws governing the dominant industry to which a company belongs, as well as the state(s) where the company does business and where relevant consumers reside.

Notable Federal Privacy Laws

Notable federal privacy laws (by industry sector) include the following:

- **Health sector** – the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH Act)
- **Financial sector** – the Gramm-Leach-Bliley Act (GLBA) and the Fair Credit Reporting Act (FCRA)
- **Educational sector** – the Family Educational Rights and Privacy Act (FERPA) and the Protection of Pupil Rights Amendment (PPRA)
- **Telecommunications and marketing sector** – Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM), the Telecommunications Act of 1996, the Cable Communications Policy Act of 1984, and the Video Privacy Protection Act of 1988 (VPPA)

For a more detailed discussion on the GLBA and CAN-SPAM, see Complying with the Privacy Requirements of the Gramm-Leach-Bliley Act (GLBA) and Complying with the CAN-SPAM Act.

In addition, regardless of the industry, websites and online services that target children must comply with the Children's Online Privacy Protection Act (COPPA). COPPA applies to "an operator of a website or online service directed to children" and to "any operator that has actual knowledge that it is collecting personal information from a child." 15 U.S.C. § 6502(a)(1). A child is any person under the age of 13.

Privacy policies for websites or online services covered by COPPA must be posted online and must include the following:

- The information that is collected from children (including whether the website or online service enables children to make personal information publicly available), how the operator uses such information, and the operator's disclosure practices for such information
- The names, addresses, telephone numbers, and email addresses of all operators who collect or maintain children's personal information through the website or online service
- A statement that a parent can review or have deleted a child's personal information, and refuse to permit further collection or use of such information, along with the procedures for doing so

16 C.F.R. § 312.4(d). For a more detailed discussion on COPPA, see COPPA Compliance.

Notable State Privacy Laws

You should also be familiar with the privacy laws of the states in which your client does business and where relevant consumers reside, both for privacy notice and for data breach remediation purposes. For a more detailed discussion on data breaches, see Planning for & Managing a Data Breach, Preparing a Breach Notification Letter, and State Statutory Laws Regarding Data Breaches.

California, for instance, has been at the forefront of state privacy legislation. The California Online Privacy Protection Act (Cal-OPPA) applies to any business that collects PII about California residents through websites, mobile applications, or online services. As such, Cal-OPPA has a broad reach and extends to most companies that conduct business online or engage in other online activities.

Cal-OPPA requires an operator of a commercial website or online service (which includes mobile apps) to do the following:

- Conspicuously post a privacy policy on its website (or in the case of an online service, make the policy available)
- Include various disclosures in the policy (such as what information is collected and with whom it is shared, how the business responds to web browser "Do Not Track" signals, and whether any third parties may collect PII on the business's website or online service)
- Adhere to the policy

See Cal. Bus. & Prof. Code § 22575.

An operator violates Cal-OPPA if it fails to post a privacy policy within 30 days after being notified of noncompliance, or if it otherwise fails to comply with Cal-OPPA or with the terms of its posted privacy policy either knowingly and willfully, or negligently and materially. See Cal. Bus. & Prof. Code §§ 22575(a), 22576. Failure to comply with Cal-OPPA may lead to an enforcement action by the California Attorney General (under the California Unfair Competition Law) and fines of up to $2,500 per violation. See Cal. Bus. & Prof. Code § 17206(a).

Other notable California data privacy laws include:

- **Privacy Rights for California Minors in the Digital World.** Allows minors to request the removal of content or information posted online and restricts the online advertising of certain products and services to minors (see Cal. Bus. & Prof. Code §§ 22580 – 22582).
- **Student Online Personal Information Protection Act (SOPIPA).** Protects the use of student data by operators of websites, mobile applications, or online services that have actual knowledge that the site, service, or application is primarily used for K-12 school purposes and was designed and marketed for such purposes (see Cal. Bus. & Prof. Code §§ 22584 – 2285).

Other states may have similar laws to those in California (see, e.g., the Delaware Online Privacy and Protection Act (DOPPA), 6 Del. Code Ann. § 1201C – § 1206C) or laws that address other aspects of privacy, such as biometric data (see, e.g., Illinois's Biometric Information Privacy Act, 740 ILCS 14/1 – 740 ILCS 14/99).

It is therefore critical to research the privacy laws of all states in which your client does business, as well as the federal laws and regulations that govern data privacy in your client's industry sector, to ensure that the privacy policy complies with any applicable requirements. If your client does business in countries other than the United States, your client will also need to comply with those countries' laws.

Information to Include in a Privacy Policy

In drafting a privacy policy, you may need to balance the completeness of the information conveyed in the policy with conciseness, so that the result is approachable and is more likely to be read and understood. Jargon and legalese should be kept to a minimum, and hyperlinks to definitions or terms of art (e.g., "cookies" or "data controller") should be included.

The policy should contain at least the following information:

- What personal data is collected
- How the data is collected (e.g., is the data collected directly from the consumer or from third party sources?)
- How the data will be used and protected (e.g., are there reasonable security safeguards in place?)
- Whether the data will be shared with any affiliates or unrelated third parties for marketing (or other) purposes

- The consumer's rights and choices (e.g., any right to access the data and make corrections; rights and/or choices regarding data collection, use, and sharing)
- Any opt-out or opt-in procedures
- How cookies are used (cookies are small text files that a website transfers to a consumer's hard drive or web browser and that are used to track user preferences, often for analytics and marketing purposes)
- The organization's contact information (e.g., an email or postal address)
- The effective date of the policy

Other information may be required depending on the states or countries where your client does business, the laws and regulations governing your client's industry sector, and whether your client's website targets children under the age of 13, as discussed above under Legal & Regulatory Considerations.

The policy should be flexible enough so that it will not need frequent changes. To this end, you should consider how the organization collects and uses data, not only presently, but in the future. For example, a company may not currently share information with affiliates for marketing purposes, but may decide to do so at some later time. To account for this possibility, the privacy policy should state that information which a customer provides in connection with completing a transaction may be shared for marketing purposes with affiliated entities and unrelated third parties. Other potentially foreseeable collection and use should also be stated in the policy, which will help keep the document flexible and relevant.

"Layered" Policies

For websites or mobile apps especially, you should consider recommending a "layered" privacy policy to your client. The first layer would be a short-form version of the policy that consumers may immediately and easily view (even on a smart phone screen) and that highlights the most important and necessary privacy disclosures. The short version may, for instance, describe the kinds of data being captured, the permitted uses and disclosures of the data, the consumer's rights and choices, contact information, and a link to the long-form, more comprehensive version of the policy (i.e. the second layer). You might also consider including FAQ sheets as part of the second or even third layer.

Disclosing the Policy

A privacy policy should be posted in a prominent location (such as the homepage of your client's website). Any link to the policy should be clear and conspicuous. This may be achieved, for instance, by using larger text in the link than the surrounding text, by using contrasting symbols or colors, or by using the word "privacy" in the link.

In some situations, annual privacy notices must be mailed or hand-delivered to consumers to comply with relevant laws such as the Gramm-Leach-Bliley Act (GLBA). See, e.g., Regulation P (12 C.F.R. § 1016.9), adopted by the Consumer Financial Protection Bureau (CFPB) pursuant to the GLBA.

Note, however, that a recent amendment to the GLBA provides an exception to the annual privacy notice requirement if a financial institution:

- Only shares nonpublic personal information (NPI) as permitted by the GLBA
- Has not changed its policies and practices with regard to disclosing NPI since the most recent disclosure sent to consumers

See Section 75001 of the Fixing America's Surface Transportation Act (the FAST Act), *114 P.L. 94* (effective Dec. 4, 2015).

Reviewing and Updating the Policy

A business should review its privacy policy on a regular basis, and promptly update or revise the policy to reflect any material changes in how it uses or shares PII (though, ideally, the policy would be flexible enough to encompass such changes, as discussed above). It might also consider having a process in place for notifying consumers of any material changes.

Importance of Adhering to the Policy

It is important to advise your client that once it decides to create and publish a privacy policy, it needs to comply with the policy in practice. The Federal Trade Commission Act (FTCA) prohibits unfair and deceptive trade practices, and the FTC has taken the position that the use or dissemination of personal information in a manner different from what is indicated in a posted privacy policy is a deceptive trade practice under the FTCA, 15 U.S.C. § 45.

The FTC has brought numerous enforcement actions relating to privacy policies (or other consumer-facing statements) that resulted in consent decrees, including the imposition of fines and audit obligations (which in some cases may last for 20 years). Common reasons for enforcement actions include:

- Broken promises
- Retroactive privacy policy changes
- Deceptive data collection or use
- Inadequate data security
- Inadequate disclosure of the amount of data gathering

Notable enforcement actions in these areas are discussed in further detail below.

Broken Promises

In *In re Nomi Technologies, Inc.*, respondent had used mobile device tracking technology to track consumers' movements within retail stores (specifically, it sold the technology to retailers and, as such, had no direct contact with the consumers whose information was being tracked). Respondent's privacy policy stated that consumers could opt-out of such tracking either online or in stores using the technology, and that consumers would be informed when the tracking was taking place. However, respondent did not require its retailer clients to notify consumers that they were being tracked.

The FTC alleged that the privacy disclosures in respondent's policy were deceptive and violated Section 5 of the FTC Act because respondent did not, in fact, provide in-store opt-out mechanisms or notify consumers of the tracking. The FTC noted that retailers that contracted with respondent were not obligated to post notices of the tracking program in their stores and that respondent's website did not list all of the retailers using its technology. Thus, the fact that consumers could opt-out via respondent's website did not overcome the failure to provide in-store opt-out mechanisms. See In re Nomi Techs., Inc., 2015 FTC LEXIS 101 (F.T.C. Apr. 23, 2015).

Retroactive Privacy Policy Changes

In *In re Gateway Learning Corp.*, respondent's online privacy policy stated that it would not sell, rent, or loan customer personal information to third parties without consent. However, respondent began renting personal information to third parties without informing customers or obtaining consent, and subsequently revised its policy to state that it would provide customer information to "reputable companies" from time to time. Finding that the retroactive change to the privacy policy was material and constituted an unfair practice, the FTC barred respondent from making future retroactive material changes to its policy without first obtaining consumer consent. See In re Gateway Learning Corp., 138 F.T.C. 443 (F.T.C. 2004).

Deceptive Data Collection or Use

In *In re PaymentsMD, LLC*, the FTC alleged that a medical billing provider and its former CEO used the sign-up process for an online billing portal—where consumers could view their billing history—to deceptively obtain consumers' consent to collect highly detailed medical information from pharmacies, medical laboratories, and insurance companies. As part of the settlement, the FTC banned respondents from deceiving consumers about how they collect and use information, including how the information may be shared with or collected from a third party. See In re PaymentsMD, LLC, Complaint and Decision and Order (F.T.C. 2015).

Inadequate Data Security

In *In Re Oracle Corp.*, respondent Oracle Corp. had acquired Java Standard Edition (Java SE) software from Sun Microsystems in 2010. Oracle was aware that older versions of Java SE were insecure and offered updates to consumers. Oracle warranted, as part of the update process, that both the updates and the consumer's system would be "safe and secure" with the "latest . . . security updates." However, the update only removed the most recent version of Java SE and not any of the earlier insecure versions. The FTC alleged that Oracle's failure to disclose the limitations of the update process was deceptive in light of its statements regarding security. See In re Oracle Corp., 2015 FTC LEXIS 292 (F.T.C. 2015).

Inadequate Disclosure of the Amount of Data Gathering

In *In re Compete, Inc.*, respondent, a web analytics company, collected data about consumers through two products: a Toolbar and a Consumer Input Panel. Respondent represented that its products would collect and transmit information about the websites consumers visited, but failed to disclose the extent of personal information that was collected and transmitted. Such information included consumers' Social Security numbers, credit card and bank account numbers, and security codes and expiration dates. The FTC alleged that respondent's failure to disclose the extent of data gathering violated Section 5 of the FTC Act. See In re Compete, Inc., 2013 FTC LEXIS 14 (F.T.C. 2013).

Checklist – Drafting Privacy Policies

As discussed above, if your client collects consumer data, it should have a privacy policy in place and adhere to that policy in practice. The privacy policy should be viewed as an agreement between the client and its customers or consumers. This checklist will serve as a quick guide of things to look for when reviewing and/or drafting a privacy policy.

1. Identify the personal information that is collected, how it is collected, and how it is and will be used and protected by the client.
2. Think long term. You should not only consider the client's current data collection and use practices, but also any potentially foreseeable collection and use.
3. Consider any relevant federal and state laws and regulations that have specific requirements regarding how consumer data must be handled. Also consider the legal regimes of other countries if your client does business outside the United States.
4. The privacy policy should be complete, concise, and flexible to account for potential changes in company policy without needing revisions.
5. Explain or define any legal or technical terms.
6. Explain how cookies are used.
7. Explain whether, and how, consumer information will be shared with any affiliates or unrelated third parties.
8. Disclose the consumer's rights and choices (e.g., any right to access the data and make corrections; rights and/or choices regarding data collection, use, and sharing).
9. Identify how consumers may contact the company to file a complaint or for other purposes.
10. Include guidelines on how the client may change its privacy policy (e.g., by providing notice on its website).
11. Include information on how consumers can opt in or out of privacy-related practices (e.g., not receive marketing materials) or change/cancel their email notices.
12. State the effective date of the policy.
13. Disclose the policy as required by applicable laws and regulations. Online policies should be posted in a prominent location (e.g., the homepage of your client's website), and any links to the policy should be clear and conspicuous.
14. Update or revise the policy to reflect any material changes in how your client collects or uses personal information.
15. Confirm that the client understands and is able to comply with its own stated policy in practice.