PRIVACY POLICY UPDATES AND CONSIDERATIONS

Startup Blog Alert
September 21, 2016

A privacy policy explains how your company gathers, uses, discloses, and manages personally-identifiable information and other sensitive data (PII). In today's digital world, almost every company manages PII electronically. Digital PII is valuable and easy to collect. Maybe too easy. Lawmakers and customers are growing concerned with reports of PII misuse and theft. As such, a well-tailored privacy policy will reassure customers and satisfy increasingly watchful regulators. A policy may even be required by law. Therefore, it's important to review your company's privacy policy with an eye for detail.

Unsurprisingly, a good privacy policy requires more than changing the company name in an online template. This post lists some basic factors that you should consider during a privacy policy review.

Legal Requirements and Regulations

The Federal Trade Commission (FTC)

Currently, the United States does not have an overarching federal privacy law. However, the FTC has lead a regulatory charge for consumer privacy. Although the FTC does not suggest a specific privacy policy format, they do suggest close attention to the following tenets:

- notice, awareness, and transparency;
- choice and consent;
- access, participation, and correction; and
- data integrity and security.

Building on these principles, the FTC has prepared three documents that you should review before updating your privacy policy.

1. Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers;
2. Mobile Privacy Disclosures: Building Trust and Transparency; and
3. Internet of Things: Privacy and Security in a Connected World.

Attorneys

Gary Schober

Practices & Industries

Startups & Emerging Companies

Each of these documents provides useful tips and suggestions for companies that handle PII.

State Laws

Some states require you to follow certain rules if you collect PII from their residents. For example, California, Delaware, and Connecticut have privacy protection laws. See:

- The California Office of Privacy Protection Guidelines and CalOPPA.
- The Delaware Online Privacy Protection Act.
- Connecticut General Statutes, Section 42-471.

Each state has its own laws. You should prioritize compliance in states where you expect to do significant business.

Industry Specific Rules

Certain industries are subject to additional laws or regulations. Here's a short list:

- Financial Institutions and Information: The Gramm Leach Bliley Act and related state law and regulations.
- Healthcare and Health Information: The Health Insurance Portability and Accountability Act of 1996 (HIPAA).
- Children: The Children's Online Privacy Protection Act of 1998 (COPPA).
- Students: The Family Educational Rights and Privacy Act (FERPA) and relevant state student privacy laws.
- Online Behavioral Advertising: Network Advertising Initiative Code of Conduct.

International Laws

Collecting PII from international customers may trigger obligations from foreign jurisdictions. For example, transferring PII out of EU member states can be technically easy, but legally complex. The EU data privacy rules are strictly enforced. If you're interacting with EU member states, consider EU/US data transfer issues and review the EU data protection and notice requirements.

Drafting the Privacy Policy

Simply meeting legal and regulatory requirements does not make a strong privacy policy. An overbroad privacy policy may create negative reactions and public relations problems. A narrow privacy policy may preclude future revenue models and create costly data protection obligations. A good privacy policy is flexible, meets customer expectations, and satisfies your legal requirements.

The trick is to keep it simple. Use plain language. Avoid long lists of exceptions to the policy's use restrictions. And make sure the privacy policy is tailored for your specific needs. Every good privacy policy may contain the following details:

- the types of PII you collect, how you collect the PII, and how you plan on using or sharing that PII;
- who controls any PII collected by you or on your behalf;

- how long you keep the PII;
- if there is any PII that receives special care;
- what happens to PII during a merger, or sale of assets;
- contact information for questions, comments, and concerns; and
- when you will transfer PII to third parties.

Also, consider how you want to deliver the privacy policy to your customers—perhaps through email or by an online notice. You should reserve the right revise the policy at any time. If you revise your privacy policy, keep a copy of past versions. Most importantly, beta test the policy with customers that provide PII and employees that collect or use PII.

Following the Privacy Policy

Now that you have a privacy policy, you need to follow it. Don't retain or store PII except as outlined in the privacy policy. Review the privacy policy with your employees so they act consistently.

Schedule periodic reviews of your privacy policy to make sure that it remains consistent with your business practices and continues to comply with the law. The FTC has taken action against companies that handle PII in ways that contradict their stated privacy policy. Although actions have been mostly limited to cases involving PII breaches, the FTC (and other regulators) have made it clear that they intend to take a more aggressive approach in the future.

A privacy policy needs to be more than just an afterthought. These policies are becoming increasingly critical in enforcement actions, mediations, and lawsuits. A strong privacy policy can protect your business and reduce complaints from your customers.