HUDSON COOK

Why You Need a Website Privacy Policy

November 30, 2022 | Erik Kosa and Jennifer L. Sarvadi

Privacy is a growing area of regulation in the United States, and not just for large institutions like national banks. If you do business in the United States, it is becoming increasingly likely that you are covered by a law that requires you to have a website privacy policy and has specific requirements about what you say to consumers about their privacy. These laws also give consumers certain rights to tell you what you may or must do with their data. You may be required to inform visitors to your website about what information you collect about them, how you use it, how you share it, and how you protect it.

Regulators view your website privacy policy as a promise to consumers about your data collection and sharing practices, and they will hold you to the promises you make. But figuring out what information is covered by these laws so you can make an accurate privacy policy can be complicated, requiring you to dig more deeply into the kinds of data you collect on consumers than you may have expected.

States have been leading the way in imposing privacy requirements on businesses that have traditionally not had to worry about them. In 2018, arguably the most significant privacy development ever in the United States occurred with the passage of the California Consumer Privacy Act (CCPA), which applies to broad swaths of the nation's largest economy. The CCPA applies to any entity doing business in California that meets one of the following thresholds:

- It has annual gross revenues in excess of $25 million;
- It annually buys, receives for its commercial purposes, sells, or shares for commercial purposes personal information relating to 50,000 or more consumers, households, or devices;
- It derives 50% or more of its annual revenue from selling personal information.

Other states are catching up with California. In 2023, Colorado, Connecticut, Virginia, and Utah all have similar laws coming into effect:

- The Virginia Consumer Data Protection Act, Va. Code Ann. §§ 59.1-571 *et seq.*, will be effective January 1, 2023.
- The Colorado Privacy Act, Colo. Rev. Stat. §§ 6-1-1301 *et seq.*, will be effective July 1, 2023.
- The Connecticut Data Privacy Act, Conn. Gen. Stat. Ann. § P.A. 22-15 *et seq.*, will be effective July 1, 2023.
- The Utah Consumer Privacy Act, Utah Code Ann. §§ 13-61-101 *et seq.*, will be effective

December 31, 2023.

These laws generally give consumers broad rights, including, among other things, the right to receive notice about and access to certain information about them, the right to request that a business delete some that information, and the right to opt out of the sale of certain information. But parsing which rights apply to which data is not simple. For example, data covered by the Gramm-Leach Bliley Act or Fair Credit Reporting Act may be exempt, requiring you to think carefully about the kinds of data you collect before deciding what you will promise consumers in your privacy policy. And these new consumer rights require businesses not just to get their website privacy policy disclosures right, but also to stand up an internal process for making sure the company is following its own policy. In addition to thoroughly analyzing the data the business collects, businesses engaging service providers may also need to ensure their agreements with these entities contain appropriate restrictions on the use of data. And don't forget the states with narrower disclosure requirements specific to website privacy policies, including California, Nevada, and Delaware.

In sum, the changing legal landscape requires a new way of thinking about how your business is run. Are you doing business in a state with a privacy law that applies to you? Are you collecting—either directly or via a third party—personal information on consumers? What categories of data? Do your third-party service providers have requirements in their terms of use that affect how you handle data and disclosures about that data? How will you go about making sure you get the answers to these questions right?

Moreover, once the privacy program is implemented, you are not done. A website privacy policy is not a "set it and forget it" tool. It must remain a living document that is reviewed regularly and evolves with both your business practices and the law. For example, the CCPA's requirements are changing in 2023 as a result of the new California Privacy Rights Act, adding additional requirements for businesses subject to the law and standing up a new enforcement agency, the California Privacy Protection Agency, which is going to engage in additional CCPA rulemaking. The new state laws in Colorado, Connecticut, Virginia, and Utah will also soon have accompanying regulations which are still taking shape. And states are also passing laws regulating more targeted information, like biometric information privacy, that businesses have not had to contemplate before.

If that's not enough, at the federal level, the Federal Trade Commission, the Consumer Financial Protection Bureau, and even Congress are now eager to get in on the fun. The FTC and CFPB and contemplating rulemakings on privacy, and with the negotiations around the American Data Privacy and Protection Act, Congress appears to be getting closer to a consensus on what future comprehensive privacy legislation may look like. The specifics have yet to take shape, but we expect that soon these rulemaking and legislative efforts will significantly change the legal landscape of privacy, again. And as the various regulators' enforcement actions under these new laws develop, we are going to learn yet more about how regulators view your responsibilities.

If you are covered by a privacy law, you will need a process for reviewing your compliance program with competent counsel to ensure both that your business is in a good position to comply with these new laws and keep up with any changes to the law or your business practices, so they are properly reflected in your privacy policy.

HUDSON
COOK

Hudson Cook, LLP is a national law firm representing the financial services industry in compliance, privacy, litigation, regulatory and enforcement matters.

7037 Ridge Road, Suite 300, Hanover, Maryland 21076
410.684.3200

hudsoncook.com