19 States Have Passed Privacy Laws: Law Firms Tighten Cybersecurity

by Sharon D. Nelson, Esq., John W. Simek, and Michael C. Maschke

Privacy Laws Increase Law Firm Risks

It's been a long while since law firms got used to data breach laws and the required notifications – all 50 states have such laws. Privacy laws, which are a relatively new development, are fast becoming another concern for law firms. "Battening down the hatches" has taken on a new impetus as state after state has passed a privacy law, enhancing the dangerous financial risk accompanying a data breach or failure to abide by the privacy law requirements, which govern the collection, use and disclosure of personal data and establish standards for the handling of sensitive personal data.

Here's a list of the states with privacy laws, noting the effective date for those states where the law is not yet in force.

- California
- Colorado
- Connecticut
- Delaware (effective January 1, 2025)
- Indiana (effective January 1, 2026)
- Iowa (effective January 1, 2025)
- Kentucky (effective January 1, 2026)
- Maryland (effective July 1, 2025)
- Minnesota (effective July 1, 2025)
- Montana (effective October 1, 2024)
- Nebraska (effective January 1, 2025)
- New Hampshire (effective January 1, 2025)
- New Jersey (effective January 1, 2025)
- Oregon
- Rhode Island (effective January 1, 2026)
- Tennessee (effective July 1, 2025)
- Texas
- Utah

- Virginia

As you will note, only seven states have privacy laws which were effective by July of 2024. But there is a wave of states whose laws will be effective in the next two years – and many additional states are poised to pass privacy laws soon.

What Brought About the Onslaught of Privacy Laws?

Just when law firms had come to grips with data breach laws in all 50 states and the territories, lawmakers determined that privacy laws were needed. Everyone and their brother seeks to hoover up our private information and they are willing to pay for it.

The interconnections of the internet make it easy to harvest data – and protection is all but non-existent. Our data is no longer our data. It is stolen, monetized and used for endless nefarious purposes. The outcry of consumers and businesses whose data has been misused led to state legislators bent on taking action. The more fraud, identify theft and other misdeeds took place, the more legislators were pressed by constituents to "bring down the hammer." Not only was privacy legislation needed, but so were fines designed to mandate stronger protection for individuals and companies.

How are Law Firms Impacted by the Wave of Privacy Laws?

There is good news of course, for any law firm that practices privacy law. Privacy law has taken off as a practice area, sometimes alongside data breach law.

But there is an impact on law firms which do not adequately protect the personal information of clients. One recent and concerning example is the number of lawyers that have given client data over to artificial intelligence systems. Not properly protecting data, including the use of adequate cybersecurity measures, could violate client privacy.

Use of shoddy or obsolete cybersecurity could also violate privacy laws, with severe potential penalties to follow.

Will Law Firms Feel the Heat of New Cyberinsurance Requirements?

We think it is very likely that cyberinsurance companies, already known for increasingly strict cybersecurity demands, will want to make sure that they are not

on the hook for paying privacy law fines. Getting coverage from cyberinsurers has become an increasing headache for law firms. It has been our observation that law firms generally pay more and get less coverage. Some things may be explicitly excluded from coverage. For instance, if you do not mandate minimum data protections required by state privacy laws, you may not be covered.

As data privacy laws proliferate, the impact of those laws is certainly likely to increase – and, thus far, we've not seen a rush to comply with those laws!

Final Words

Privacy in today's interconnected world is illusory. Can state laws play any significant role in restoring privacy? Doubtful, to say the least. But the new laws are probably a worthy call to arms for law firms which have stringent ethical rules and must meet the demands of cyberinsurance companies.

Sharon D. Nelson *is a practicing attorney and the president of Sensei Enterprises, Inc. She is a past president of the Virginia State Bar, the Fairfax Bar Association and the Fairfax Law Foundation. She is a co-author of 18 books published by the ABA.* snelson@senseient.com

John W. Simek *is vice president of Sensei Enterprises, Inc. He is a Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH) and a nationally known expert in the area of digital forensics. He and Sharon provide legal technology, cybersecurity and digital forensics services from their Fairfax, Virginia firm.* jsimek@senseient.com

Michael C. Maschke *is the Chief Executive Officer at Sensei Enterprises, Inc. Mr. Maschke is an EnCase Certified Examiner (EnCE), a Certified Computer Examiner (CCE #744), an AccessData Certified Examiner (ACE), a Certified Ethical Hacker (CEH), and a Certified Information Systems Security Professional (CISSP). He is a frequent speaker on IT, cybersecurity and digital forensics and he has co-authored 14 books published by the American Bar Association. He can be reached at* mmaschke@senseient.com*.*