

2021 Breach Notification Law Update: Connecticut and Texas Expand Requirements, Ransomware and Supply Chain Attacks Take Spotlight

Cyberattacks continue to make the news and affect our lives in increasingly more significant ways. However, after several years in which states have actively updated breach notification laws in reaction to significant data breaches, 2021, like 2020, has been relatively quiet. Just two states—Connecticut and Texas—have updated their general data breach notification laws, and only Connecticut's changes will have significant impacts on compliance. Connecticut and Utah also enacted novel "safe harbor" laws that provide reprieve from liability in certain data breach tort actions, but only if a company adopts specific recognized data security practices. (States have been [actively debating](#) privacy legislation this year—with [Colorado](#) and [Virginia](#) joining California in enacting omnibus privacy laws—but those laws generally do not impose any security requirements.)

Though state law updates have been relatively quiet, the recent spate of cyberattacks has ushered in a new era of federal attention to cybersecurity. In addition to updated breach reporting requirements, companies should take note of federal agency guidance on cybersecurity measures that should be implemented to prevent ransomware and other cyberattacks.

[Click here to view the full update.](#)

Authors



[Amelia M. Gerlicher](#)

Partner

AGerlicher@perkinscoie.com [206.359.3445](tel:206.359.3445)

Explore more in

[Privacy & Security](#)

Blog series

Perkins on Privacy

Perkins on Privacy keeps you informed about the latest developments in privacy and data security law. Our insights are provided by Perkins Coie's [Privacy & Security practice](#), recognized by Chambers as a leading firm in the field. [Subscribe ?](#)

[View the blog](#)