

Privacy & Cybersecurity Newsletter

Locke Lord's Privacy & Cybersecurity Newsletter provides topical snapshots of recent developments in the fast-changing world of privacy, data protection and cyber risk management. For further information on any of the subjects covered in the newsletter, please contact one of the members of our privacy and cybersecurity team.

In This Issue

State Developments

U.S. State Privacy Laws: California, Colorado, Connecticut, Delaware, Indiana, Iowa, ?Montana, Oregon, Tennessee, Texas, Utah, Virginia

In 2023, new consumer privacy laws will be effective in California, Colorado, Connecticut, Utah, Virginia. Other laws from the states of Delaware, Indiana, Iowa, Montana, Tennessee, Oregon, and Texas were signed this year and will become effective by 2026. [read more](#)

New Amendments to NY DFS Cybersecurity Regulation: Big Changes for Big Companies, and Other Implications

Effective November 1, 2023, the New York Department of Financial Services issued its second amended Cybersecurity Regulation (the "Regulation," [23 NYCRR Part 500](#)). The amendment follows extensive [public comments](#), some of which were reflected in the Regulation. Compliance is required by April 29, 2024 (180 days after the effective date), subject to the transition dates. [read more](#)

EU, U.K. Developments

New Mechanism for Cross-Border Data Transfer: The EU-U.S. Data Privacy Framework

On June 10, 2023 the European Commission (the "Commission") [issued an adequacy decision](#) on the new EU-U.S. Data Privacy Framework (the "DPF"). The decision restored free transfer of data between the EU and U.S. after three years of uncertainty following the [Schrems I](#) and [Schrems II](#) decisions, which overturned the preceding [Safe Harbor Framework](#) of 2000 and [2016 Privacy Shield](#). [read more](#)

U.S.-U.K. Data Transfer Developments

The U.K. Data Bridge extension to the EU-U.S. Data Privacy Framework ("DPF") was formally green-lighted by the U.K. Government on 12 October 2023. [read more](#)

Incident Response

Challenging Recent Developments for Incident Response

The United States is on track to see a record number of data breaches in 2023 and state regulators are paying attention. The swift action required by victim companies includes containment and elimination of the threat, and

quick and thorough analysis to determine required notifications to state and Federal agencies, affected individuals, and other third parties. Notice requirements vary by jurisdiction, as does the level of regulatory oversight. The need for companies to strengthen their incident response plans is highlighted by the recent increase in the volume, severity and complexity of incidents, and changes in the legal, regulatory and litigation environment. Good preparation will reduce the time and increase the effectiveness of breach response and help mitigate the related cost and potential exposure. [read more](#)

Litigation

More Safe Harbor Protections for Navigating Cyber and Privacy Litigation

Cybersecurity and data privacy risks continue to loom large with potentially significant consequences. Litigation, often filed soon after incidents, adds to the possible repercussions. In our previous [article](#), we discussed a trio of states providing affirmative defenses or “safe harbors” that companies can take advantage of to minimize litigation exposure resulting from a data breach. Three other states have recently followed, with Oklahoma, Iowa, and Tennessee recently passing their own “safe harbor” laws. [read more](#)

Beware Common Website Technology Tools That Can Lead to Wiretap Claims

Knowing how consumers behave while on a website can provide businesses with valuable information. Frequently businesses employ “session replay” tools to analyze what users do on their website. “Session replay” is software embedded in a website that allows companies to improve the effectiveness of a website. Use of this technology has been challenged in a number of class action lawsuits filed over the past few years. Another group of lawsuits allege that some companies are unlawfully embedding code in their chat features that allows a third-party service provider to create and retain a real time transcript of chats with consumers. [read more](#)

Visit Locke Lord’s [Privacy & Cybersecurity Resource Center](#) for topical, practical snapshots of recent developments in the fast-changing world of privacy, data protection and cyber risk management.

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber