Articles + Publications | August 5, 2024

Spoliation: When the Duty to Preserve Data Outweighs the Obligation to Delete

Privacy & Cybersecurity Newsletter

WRITTEN BY

Lindsey E. Kress | Tara L. Trifon

RELATED OFFICES

Hartford

Implementing and enforcing appropriate legal holds is essential to preventing the destruction of data related to current or anticipated litigation and avoiding inadvertent spoliation claims. Depending on the nature of the lawsuit, this typically involves issuing systematic and individual custodial holds and ensuring that relevant data across multiple platforms is preserved. Companies must identify the scope of data that is subject to the legal hold and act quickly to suspend data retention procedures that could result in the destruction of relevant information. This is especially true for data with short retention periods, such as chat communications, which are typically not retained by companies beyond a 24- to 48-hour period.

Courts have issued spoliation sanctions against corporate parties that failed to preserve these communications as part of their legal hold process. Not only does a company risk spoliation sanctions in the event relevant data is not preserved, but the failure to preserve data can also drastically impair the company's ability to defend against claims in the lawsuit.

However, preserving too much data is not always the safer choice. Data can be expensive to store and costly to search. Preserving too much data in connection with a legal hold can drastically increase the cost of eDiscovery. Over-preservation may also conflict with data minimization requirements in certain jurisdictions. Companies should limit the retention of consumer personal information where possible, subject to their data preservation obligations.

Companies Must Be Proactive and Diligent to Avoid Spoliation Sanctions

Companies have a duty to preserve records and information potentially related to a pending or reasonably anticipated lawsuit. Spoliation of evidence occurs when a party has deliberately, negligently, or accidentally destroyed evidence relevant to a pending or reasonably anticipated lawsuit. Companies that fail to preserve relevant evidence can be subject to judicial spoliation sanctions – which can range from monetary fines to adverse jury instructions requiring jurors to find that the deleted information was harmful to the company's position.

Managing the legal hold process and avoiding spoliation sanctions has gotten more complicated in the age of eDiscovery and electronically stored information ("ESI") given the extent to which companies use different types of digital platforms to communicate and conduct business. Companies must ensure that all forms of relevant ESI are preserved by considering all sources of information and platforms that are likely to have information relevant to the litigated matter. This typically requires issuing both systematic and individual custodian hold notices, where applicable, and conducting quality control reviews to ensure that all relevant data is being preserved. This can be especially difficult for certain types of ESI that are not typically retained by companies, such as chat communications.

Last year, a federal district judge issued spoliation sanctions against a major technology company in multidistrict antitrust litigation pending in the United States District Court for the Northern District of California[1] as a result of the company's alleged failure to preserve company chat communications. While the company preserved relevant email data, it allegedly failed to suspend its 24-hour auto-delete policy for internal instant messaging communications and instead instructed employees to avoid discussing topics related to the lawsuit via chat and to turn on the "chat save function" if the conversation strayed into a topic related to the litigation. The court found these measures were insufficient given that the company had the ability to suspend its auto-delete policy and issued monetary spoliation sanctions against the company. The court further warned that additional non-monetary sanctions may issue once additional discovery reveals what information was lost.

Another company was sanctioned in a case pending in the Northern District of Ohio for failure to preserve its internal chat communications.[2] In that case, the company changed its Slack messaging retention setting from "indefinite" to a seven-day retention period after it was on notice of anticipated trademark infringement litigation, which allegedly resulted in several thousand potentially relevant messages being deleted. The company argued that it changed its policy to "minimize potential liability for the theft and disclosure of its customer's [sic] confidential information" under the California Consumer Privacy Act ("CCPA") and the International Standard of Operation Compliance ("ISO") – not to gain an advantage in the litigation. The court found that neither the CCPA nor the ISO required destruction of the Slack messaging data and the fact that the company changed its policy shortly after litigation was reasonably foreseeable suggested the destruction was intentional. As a result, the court issued spoliation sanctions in the form of a mandatory adverse-inference instruction requiring the jury to presume the lost information was unfavorable to the company.

Failing to Preserve Relevant Data Can Impair the Company's Ability to Defend Against Claims

Not only can destroying relevant evidence result in spoliation sanctions, but it can also impair a party's ability to defend against (or prosecute) the claims in the litigation. It is not just harmful information that can be lost when data is destroyed. The failure to preserve relevant data can result in the destruction of information that is helpful to the party's position in the lawsuit.

Companies must ensure that the scope of their legal holds are sufficiently tailored to litigated matters – especially in class action lawsuits. Failing to preserve relevant class data can be catastrophic to a defendant's ability to defend against class claims and defeat certification. Where possible, companies should ensure that legal holds in class action lawsuits apply to the defined class and not just the named plaintiff – even pre-certification.

Preserving Too Much Data Presents Different Risks

While companies may face spoliation sanctions if they do not preserve information relevant to litigated matters, they also run the risk of violating data minimization requirements if they unnecessarily preserve nonpublic personal information of consumers. When it comes to personal information of consumers, companies must balance the duty to preserve with the obligation to delete.

For companies operating in the EU, this means ensuring that protected consumer information that may be subject to a legal hold complies with the data minimization requirements of the General Data Protection Regulation ("GDPR") – including confirming that the personal information being stored is "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed."

Several state privacy laws also impose a data minimization requirement, including California, Colorado, Delaware, Indiana, Iowa, Kentucky, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Tennessee, Texas, and Virginia. These states all require companies to ensure that the collection, use, retention, and sharing of consumer personal information is necessary and proportionate to the purpose for which the information is collected and stored. Companies subject to data minimization requirements must ensure that their legal holds are sufficiently tailored to avoid unnecessary retention of consumer personal information.

Apart from data minimization requirements, excessive electronic data is expensive to maintain and costly to search. Preserving too much data can drastically increase the cost of eDiscovery. Ensuring that the legal hold is narrowly and appropriately tailored to suit the needs of the litigation can not only help ensure compliance with data minimization requirements, but it can also reduce litigation costs. And once the lawsuit has concluded and the legal hold is no longer required, it is essential that companies release the legal hold and ensure that information or evidence that was subject to the legal hold is returned to its normal retention policies.

Conclusion

Storing excessive electronic data can be costly and may violate relevant data privacy laws where such data includes unnecessary consumer personal information. However, when litigation is pending or reasonably anticipated, companies are obligated to preserve all potentially relevant information across systems immediately. This requires issuing a legal hold that sufficiently considers the scope of the claims in the lawsuit, the type of relevant data that may exist, what platforms relevant data may be stored on, data retention policies for different types of data, and custodial control. However, companies should avoid preserving unnecessary data outside of normal retention periods, especially where consumer personal information is present.

—

[1] *In Re Google Playstore Antitrust Litigation*, 664 F.Supp.3d 981 (N.D. Cal. Mar. 28, 2023).

[2] *Drips Holdings, LLC v. Teledrip, LLC,* Case No. 5:19-CV-2789, 2022 WL 4545233, at *1 (N.D. Ohio Sept. 29, 2022).

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber