KAUFMAN | DOLOWICH

"Preparing For Legal Scrutiny Of Data Retention Policies", Law 360, by Jack Kallus, Esq., and Labeed Choudhry, Esq., 5-10-2023

Two of the world's largest and most well-known corporations were recently involved in litigation where deficient data retention policies and procedures played a key role. On March 28, the U.S. District Court for the Northern District of California, in U.S. v. Google LLC, sanctioned Google for failing to preserve internal chat messages.

It had been Google's policy that internal chat messages were normally deleted after 24 hours and employees were allowed to make their own personal choices whether to preserve a chat or not. While Google created and implemented policies and procedures regarding preservation of employee communications through emails and other formats, those policies and procedures failed to adequately address the communication blind spot created by the company's internal chat program, even after a litigation hold was issued.

The court therefore found that "Google fell strikingly short" in how "it honored [its] evidence preservation duties" as it related to its internal chats, and that sanctions were warranted. Google will not only have to pay monetary sanctions for failing to preserve this information, but may also face further sanctions as that lawsuit progresses.

This result should not have been surprising to Google, as only a short 10 months before it was dealt this stinging rebuke, the same court in which the Google litigation is pending issued a similar ruling on a similar issue. On May 27, 2022, in Meta Platforms Inc. v. BrandTotal Ltd., the court ruled in favor of Meta Platforms — the parent company of Facebook and Instagram — that its opponent in a litigation should be sanctioned for failing to preserve data. Similar to what occurred in the Google litigation, the sanctioned party in this litigation had a system in place that automatically deleted some data after a certain time and failed to properly preserve that data in the face of litigation. The court ultimately concluded that Meta's opponents' failure to take the appropriate steps to preserve evidence was negligent and that failure warranted sanctions.

These recent cases should serve as a call to action for companies to ensure their data retention policies are updated and properly implemented to the degree of being able to withstand judicial scrutiny. As Google found out, simply having a retention policy is not enough if that policy is unreasonable in the face of litigation or is not constantly updated to reflect changes in technology or business practices.

Companies receive and generate a significant amount of data necessary to maintain their core business functions, but it is imperative their data retention policies also incorporate the capture of data for legal safeguarding of noncore business functions as well. However, the sheer volume of data generated by companies means that retaining all data for an indefinite period would quickly become prohibitively expensive, even for multibillion-dollar companies such as Google. Most companies must therefore routinely delete or destroy a significant portion of that data. The method by which that destruction or deletion takes place must also be contained in a retention policy.

Constantly Evolving Data Requires Constantly Evolving Retention Practices

A comprehensive and thorough drafting process is critical to the success of a retention policy. Each company must independently determine what documents and information must be preserved and for how long, as that determination is highly dependent on what industry or industries the company operates in and what laws it is subject to.

Different policies may also need to be tailored for internal documents and information that is only created and shared within the company depending on the department or arm of the company involved. Different policies may also apply to data that is either received from or transmitted to third parties, whether it be other businesses or consumers.

For example, the retention policy for internally facing departments such as human resources is likely to differ in scope to the retention policy of externally facing departments such as sales or marketing. Data related to employees' payroll and taxes serves a different purpose and should have different retention policies than data related customer accounts and invoices, which should have its own retention policies. Just as there cannot be a one-size-fits-all policy for all companies, it is unlikely that there would be a one-size-fits-all policy for all departments in any one company of reasonable size. Further, company size does not impact the evaluation of whether a retention policy is necessary. If a company generates data, it is vital that it has a data retention policy.

Retention policies must be specifically tailored.

Individualized policies are imperative to cover all the various hardware and software used by a company and its employees to conduct company business. For example, Amazon.com Inc. and FedEx Corporation have vast fleets of vehicles and equipment that is used by their employees daily and the retention policy must cover the data generated by those vehicles and equipment.

Furthermore, many employees, especially in smaller or midsized companies, continue to utilize their personal cellphones, laptops and vehicles for company business. In such cases, the retention policy must not only address data on company issued cellphones, vehicles, laptops or other electronic devices, but also company data on personal cellphones, laptops, vehicles and other personal electronic devices. The failure to do so may leave an unacceptable gap in the company's retention policy. While many companies continue to use email for both external and internal communications, many other companies increasingly use Slack, Microsoft Teams or other internal chat programs for internal communications.

Many companies also use chat functions to communicate with existing and prospective customers, an example being WhatsApp, an application that has become popular for international communications. As Google is in the middle of learning, a retention policy limited to the traditional methods of communication such as email will not be enough in the face of judicial scrutiny.

Proper implementation and enforcement of a retention policy is just as important as the adoption of a proper retention policy.

It is only through proper implementation and enforcement that a company can ensure that data is not destroyed or deleted based on the whims of an individual employee. This individualized ability to preserve or delete data played into why Google was ultimately sanctioned. There is no perfect uniform way to implement a retention policy. Some companies might need to form an entire department to handle the sheer volume of responsibilities imposed by a retention policy and may assign an assistant general counsel who manages an entire team of para-professionals while others may identify a specific person who is given the responsibility of routinely ensuring that company policies are consistently followed by all employees.

Retention policies cannot be static.

Policies must include protocols for when and how often the policy is to be reviewed — and if necessary — updated. The most effective retention policy is one that is continuously reevaluated to make sure that it continues to serve the company's best interest, remains in compliance with current laws and regulations, and property implements any necessary changes resulting from needed updates.

Retention policies must adapt to accommodate emerging technologies.

As technology continues to advance, the amount of data generated by companies and the volume of documents and information that companies must deal with will continue to grow. It is the advancement of technology that is largely responsible for companies generating data at a rate never seen in human history. The type of data that emerging technologies will generate will only add to the complexity of how that data must be stored or ultimately destroyed. In fact, emerging technologies and the devices incorporating those technologies will undoubtedly create digital footprints that are revolutionary. For example, AI programs are already presenting new and novel legal issues. Companies are now wrestling with how to identify what data it creates that needs collection and storage.

Other technologies that have been part of daily use for a significant number of years but are still in their infancy for industrial purposes — such as Fitbits, Apple Watches and other wearable devices — collect biometric data and use newer technologies like facial recognition technology that also must be considered. Proper retention of data generated by these emerging technologies must be done in a manner that is consistent with both good business practice and data privacy laws. At the same time, a company cannot ignore retention policies directed to traditional business records such as faxes, paper bills, invoices, wet signature contracts and even Post-it notes, which also require monitoring and updating.

Corporate counsel will undoubtedly have to toil to generate the appropriate policies and these policies will be undoubtedly tested by litigants and the courts. As such, it is vitally important to not just adopt and implement comprehensive retention policies, it is of the utmost importance to constantly review and update those policies.

Jack Kallus is a partner and Labeed Choudhry is an associate at Kaufman Dolowich & Voluck LLP.