The Legal Intelligencer
THE OLDEST LAW JOURNAL IN THE UNITED STATES 1843-2018
PHILADELPHIA, TUESDAY, FEBRUARY 20, 2018 VOL 257 • NO. 34 An ALM Publication

CORPORATE GOVERNANCE

Privacy by Deletion: Five Steps to Reducing Data Risk

BY ANTHONY DIANA AND JAKE FRAZIER

Special to the Legal

When it comes to data retention practices, most companies are stuck in limbo, balancing competing needs between providing easy access to data for business and regulatory purposes and safeguarding data against leakage and breaches. The landscape 10 to 15 years ago was one of gross over-retention, with many practicing a blanket "save everything" approach. That landscape has begun to shift, as the risks associated with data security and data privacy have become paramount for many companies. While money, resources and technology can be directed to "protecting" confidential information from data breaches and data intrusions, the daunting reality is that if a company is retaining sensitive information, including personal information of employees and customers, the most effective protection is to ensure that such sensitive information is deleted when it no longer needed, or is deleted or removed from areas within the organization that do not have adequate protections in place. In sum, data privacy and data security are just one aspect of an effective information governance program.

Regulators are bolstering their efforts around cybersecurity and data risk management, and

DIANA

FRAZIER

ANTHONY DIANA *is a litigation partner at Reed Smith in the firm's New York office in the records and e-discovery and IP, tech and data groups. He focuses his practice on commercial litigation, internal and regulatory investigations, electronic discovery and information governance, and data privacy and security.*

JAKE FRAZIER *is a senior managing director at FTI Consulting and heads the information governance, privacy and security practice within the technology segment. He helps legal, records, information technology and information security departments to identify, develop, evaluate and implement in-house electronic discovery and information governance processes, programs and solutions.*

> *"Starting in small, digestible chunks is one effective way to enable sound deletion practices. This may not clean up everything at once, but helps make progress toward new policies."*

many are actively engaged in cybersecurity supervision and enforcement, requiring companies to identify data risk, manage data flows and delete data. Numerous bodies have specific fines they can impose for data mishandling, particularly that which includes sensitive customer information. Regulators are closely examining whether companies that house this type of information are managing it correctly, including implementing security controls, managing where and how it is stored and promptly deleting data once it is no longer needed. The SEC has communicated that the severity of fines for data breaches will be partially based on whether the company was storing customer information that was no longer needed. One financial institution was fined $900,000 by FINRA for not doing enough to ensure data about customers' trades were handled properly and for failing to protect customer privacy. The SEC hit another financial institution with a $1M fine for alleged failure to adopt written policies reasonably designed to protect customer data, and allowing an employee to access and transfer data to a personal server, which was hacked by third parties. The FTC, CFPB and state regulators are expected to be increasingly more aggressive in policing companies on managing information.

These factors have become widespread and C-Suite executives, along with the board, have made information governance (often coached as cybersecurity) a priority. Legal, compliance, IT and records teams are recognizing the need for change and starting to ask: How do we address these risks? How do we even begin? How do we get budget and resources to adequately address these issues?

When viewed as a records management project, data remediation often won't generate a sense of urgency among senior management. While records management does play an important role in establishing privacy by deletion programs, framing this work as part of risk management efforts and broader cybersecurity is more likely to resonate with key business decision makers. It is also important to prioritize efforts rather than attempt to boil the ocean, so senior management can clearly understand the specific risks being addressed and what each phase of the project will cost. Increasing awareness around the impact of major data breaches, advancing cybersecurity threats and data privacy regulation like GDPR is setting the stage for legal and IT teams to have more success in getting these types of projects off the ground and successfully executed.

The following outlines five important steps organizations can take to remediate and defensibly delete data to improve privacy, security and mitigate other risks.

UNDERSTAND WHAT EXISTS

Data can be separated into a few categories: dark data, data of value, aged or redundant data and sensitive data. By mapping out these categories and beginning to understand the full scope of the overall universe, it becomes easier to determine what can be deleted, what needs to be migrated to an inexpensive storage platform and what needs additional security protections. Documents that have outlived their business value, or have hundreds of redundant copies must be identified and deleted. Sensitive data should be classified by type—i.e., important email communications, contracts, files containing personally identifiable information, etc.—and appropriately stored and safeguarded.

FIND BUDGET

It can be difficult to quantify risks when trying to secure budget

for a defensible disposal/remediation program. A recent Iron Mountain study reported that important electronically stored information (ESI) cannot be located and used when needed at 78 percent of organizations, which highlights the issue of why it is not safer to save everything. Present decision-makers with this type of validation alongside cost-to-value and risk-to-value gap analyses. Look for opportunities to pull budget for information governance from tangential programs—cybersecurity initiatives, transformation activities like mergers, acquisitions and divestitures, or decommissioning, upgrading or migrating IT systems. Often the need to manage or reduce the volume of information during these activities help meets the goals within those programs (and save costs).

BUILD POLICY IN LIGHT OF AMENDED FRCP

Legal is often an impediment to any corporate initiative to delete data due the risk of deleting data that should be on legal hold. However, Legal may be more receptive to such iniatiaves because the risk calculus has changed. The recent Federal Rules of Civil Procedure (FRCP) amendments protects against inadvertent deletion of legal hold data and deletion of electronic data as part of an overall disposal program (FRCP 26(b)(1), 37(e)) and also provides support for proportionality in preservation (Rule 37(e) advisory committee notes). These rules allow organizations to start deleting data, as long as it is done defensibly, and in good faith by standardized procedures. However, these changes do not protect against the failure to identify and produce responsive data, and severe sanctions can be imposed for failing to produce responsive data. Therefore, there is now more risk associated with not finding responsive data than with inadvertently deleting responsive data.

AUTOMATE DATA DISPOSAL

Finding the needle in the haystack, and either protecting that needle or producing that needle, will always be difficult, so legal teams should work to create environments with smaller haystacks. The longer data is retained beyond its required retention period, the higher the data security, data privacy and litigation risk. Therefore, systems and procedures should ideally be set up to ensure automatic deletion/destruction of all copies of records after they are no longer useful for business purposes or required for legal compliance. This can be difficult to implement, but routine, repeatable and defensible disposal by record type and information repository/application, based on risk defined by legal and regulatory stakeholders, is the most effective way to maintain policies and prevent over-retention.

ENSURE DEFENSIBLE DISPOSITION

Starting in small, digestible chunks is one effective way to enable sound deletion practices. This may not clean up everything at once, but helps make progress toward new policies. Ultimately, to ensure defensible disposal, teams need to establish retention policies based on what must be saved, have processes and technology to enforce those policies, support legal hold requirements and have the ability to audit processes for long-term compliance with deletion programs. •