THOMSON REUTERS
PRACTICAL LAW™

Act Now or Pay Later: The Case for Defensible Disposition of Data

by Diana M. Fasching, Monica McCarroll, Charles R. Ragan, and Benjamin M. Redgrave, Redgrave LLP, with Tara Emory and Michael Kearney, Redgrave Strategic Data Solutions LLC

Status: **Law stated as of 12 Dec 2022** | Jurisdiction: **United States**

This document is published by Practical Law and can be found at: **us.practicallaw.tr.com/6-606-0848**
Request a free trial and demonstration at: **us.practicallaw.tr.com/practical-law**

This Article examines key considerations in developing a defensible disposition plan that allows for the systematic disposal of data that is not subject to business, legal, or regulatory retention obligations.

The volume of data that companies create and store continues to grow exponentially as data volumes double every year. The proliferation of mobile-based applications and collaboration platforms, such as those developed for increased remote work, has exacerbated this trend. For a variety of reasons, including corporate inertia, economizing budgets, and a belief by some that retaining large amounts of data can enhance sales, companies are keeping much more information than is prudent.

At the most fundamental level, information management professionals have long preached that only 15 percent of data created has value for more than a brief period. Of course, certain laws and regulations require the retention of certain information, depending on an organization's business and geographic footprint. Other laws and regulations (particularly those governing personal privacy) require data minimization and provide for private rights of action and fines for non-compliance.

Further, when an organization retains more data than necessary, it must use more servers and databases to hold all of it. These additional data sources become potential targets for hackers and other malicious actors, exposing more information if a data breach occurs. Therefore, extraneous data increases both the likelihood of a cybersecurity incident and the costs and penalties associated with the incident or breach.

Some companies used to retain data out of fear that a court may find wrong or sanctionable the act of deleting evidence that **may** be deemed relevant to future litigation. Counsel should recognize that the 2019 *Sedona Conference Commentary on Legal Holds, Second Edition: The Trigger & The Process* (20 Sedona Conf. J. 341, 348 & n. 27 at 356) emphasizes that the 2015 amendments to federal civil procedural rules narrowed the scope of discoverable information. They clarified that discoverable information is that which is relevant to the claims or defenses and proportional to the needs of the case and no longer extends to information that is reasonably calculated to lead to the discovery of admissible evidence. This change in scope should reduce the reflexive tendency to retain data for purely speculative concerns about future federal court litigation and discovery requests. (See Legal Update, Overview of December 2015 Amendments to the Federal Rules of Civil Procedure.)

For all of these reasons, it is critical that companies recognize the risks associated with over-retention and implement policies and plans that balance those risks against the value of retaining information to dispose of unnecessary data defensibly as part of a comprehensive information governance program.

The High Costs of Data Over-Retention

Holding on to unneeded or valueless data can be both expensive and risky. While unit costs of data storage have recently decreased substantially, in many cases those savings are more than offset by the increasing volume of data being generated, such that total current storage costs may have increased. The International Data Corporation estimates that the worldwide volume of unstructured data is likely to grow from 33 zettabytes in 2018 to 175 zettabytes by 2025, an annual growth rate of 61 percent (see Data Storage Costs: Three Key Steps to Better Manage Spend, Ahsan Siddiqui, September 8, 2022). A recent survey found that data storage was

among the top-five drivers for information governance projects (Global Information Governance Survey, 2022 InfoGov World Media).

Even if total storage costs are not rising for a certain enterprise, it is indisputable that retaining unnecessary hard copy documents and data means that those materials are available for future litigation or investigations. The costs and risks associated with discovery arising from future litigation or investigations may be substantial. Aside from discovery costs, a company may also incur costs for failing to protect customers' personally identifiable information (PII or personal data) or failing to dispose of it in a secure and timely manner, or both.

Litigation and Investigation Costs

Data over-retention can also lead to substantial costs, such as from litigation or investigations, whether internal or governmental, particularly during discovery. Companies that keep large volumes of information that have little or no value to the underlying business must preserve any data that is relevant to the claims and defenses of litigation once the company reasonably anticipates litigation. (See Practice Note, Implementing a Litigation Hold.) Similar retention obligations apply to investigations. A company with large volumes of data that otherwise should have been disposed faces the onerous and expensive task of identifying, collecting, processing, and reviewing that data for production. Saving unneeded data that is not subject to retention requirements also raises the risk that unfavorable evidence that could and should have been deleted before any duty to preserve attached may later surface during the litigation or investigation.

For a collection of resources to help counsel preserve data and implement a litigation hold when a company anticipates or becomes a party to litigation, see Litigation Hold Toolkit.

Compliance Costs

Traditionally, the regulation of personal data in the US has been limited to a mix of state and federal laws addressing specific issues, such as health information, financial information, and information about students and children. In other words, there is no comprehensive US privacy regulation. That situation has begun to change significantly. In 2018, US companies with business in the European Union became subject to the General Data Protection Regulation (GDPR), violations of which can result in substantial penalties. For example, in September 2022, Ireland fined Instagram (owned by US-based Meta, formerly Facebook) €405 million after finding that the social media platform had mishandled teenagers' personal information.

More recently, several states have enacted comprehensive, but varying, legislation governing personal data. These states include California, Virginia, Colorado, Utah, and Connecticut, and additional states are expected to follow.

Over-retention of personal data in violation of the myriad rules and regulations governing the handling of personal data or related to data compromised during a security incident or breach can lead to substantial fines and penalties. In 2022, for example, several US companies were assessed significant fines, including:

- $600,000 against EyeMed related to a data breach.
- $1.5 million for violations of the Children's Online Privacy Protection Act (15 USC § 6501 to 6505) by two California companies.
- $1.5 million against an online custom merchandising platform related to a data breach.

(See Article, Data Minimization and Avoiding the Over-Retention of Personal Information.)

In October 2022, a federal jury in Chicago returned a verdict against a company that collected fingerprints from truck drivers in violation of the Illinois Biometric Information Privacy Act (740 Ill. Comp. Stat. 14/5), which regulates the possession and use of personally identifiable biometric information. The jury's verdict in this class action resulted in a $228 million judgment (or $5,000 per class member) against BNSF Railway, one of North America's largest freight railroad operators. (See Legal Update, Jury Awards $228 Million Judgment in First Illinois Biometrics Law Trial.)

Additionally, certain laws and regulations govern how an organization should secure personal data and the measures it should follow in disposing sensitive information safely. Violating these laws can be extremely expensive. For example, due to a lack of adequate security for its customer data from encryption and insufficient supervision of a contractor retained to dispose of hard drives and backup tapes containing that data, Morgan Stanley Smith Barney recently settled with the SEC for $35 million (see SEC Press Release, Morgan Stanley Smith Barney to Pay $35 Million for Extensive Failures to Safeguard Personal Information of Millions of Customers).

New York State's law, the Stop Hacks and Improve Electronic Data Security Act (SHIELD), requires

companies that own or license the personally identifiable information of New York residents to implement and maintain reasonable safeguards to protect the security, confidentiality, and integrity of this type of data, including but not limited to its disposal ((N.Y. Gen. Bus. Law § 899-aa(2)). (See Legal Update, New York Amends Data Breach Notification, Information Security, and Identity Theft Prevention Obligations.)

When a company defensibly disposes of unnecessary information and properly categorizes it subject to statutory or regulatory obligations, it becomes much easier to comply with the increasing obligations posed by state and federal rules and regulations and reduce the costs associated with failures to comply.

Data Breach Costs

An average data breach, one that puts at risk between 2,200 and 102,000 records, costs a company millions of dollars. According to IBM's annual Cost of Data Breach Report for 2022, the global average cost for a data breach now sits at $4.35 million, a 13 percent climb since 2020.

Many of the costs associated with a data breach are easy to quantify, such as the penalties most states impose relating to the disclosure of personal data, and the substantial costs associated with class action lawsuits that individuals file. For example, the class action litigation against Target resulting from the data breach during the 2013 holiday season concluded in late 2018 with the appellate approval of a settlement (*In re Target Corp. Customer Data Sec. Breach Litig.*, 892 F.3d 968 (8th Cir. 2018) (rehearing and rehearing en banc denied (Aug 14, 2018))). Sometimes litigation costs arising from a data breach may include defending directors and officers named in derivative actions for breach of fiduciary duty and waste of corporate assets.

While there continues to be no overarching federal law applicable to data breaches, certain key industries regulate or strongly recommend that personal data remain protected and confidential. For example, healthcare organizations that improperly disclose personal health information are subject to stiff penalties mandated under the:

- Health Insurance Portability and Accountability Act of 1996 (HIPAA).
- Health Information Technology for Economic and Clinical Health (HITECH) Act.

Intangible costs associated with data breaches, including reputational damage, may not be as easy to measure, but are no less real. Data breaches can cause significant harm to a company's reputation and relationships, as illustrated by the following examples:

- After news broke in 2018 about the Facebook Cambridge Analytica scandal, a Ponemon Institute survey found that trust in Facebook dropped precipitously from 79 percent in 2017 to just 27 percent a week after the first news report.
- According to a 2019 survey from Security.org, more than 1 in 5 Americans are unwilling to give their information to a company exposed to hacking.
- Two years after the 2017 Equifax Data Breach, studies by the RepTrak Company suggested that Equifax's reputation had suffered significantly.

The damage to a company's reputation and relationships often is proportional to the size of the data breach. Because a breach may be inevitable, companies should seek to mitigate its risks by defensibly disposing of unneeded data.

For more information on data breach class actions, see Practice Note, Key Issues in Consumer Data Breach Litigation.

Implementing a Defensible Disposition Plan

Defensible disposition refers to the systematic deletion of data in a reasonable and good faith manner, recognizing a company's business, legal, and regulatory retention obligations, as well as its privacy obligations to dispose of data when no longer necessary for its intended purpose. A defensible disposition plan involves a process for assessing the value of a company's information along with the risks and obligations associated with retaining it and making disposition decisions that can withstand legal challenges.

A defensible disposition plan falls within a company's overall information governance program for managing company data. It should draw on individuals and departments with diverse experience and qualifications, such as privacy and compliance. By adopting strong information governance policies and procedures that include effective methods for retaining and handling data, and for disposing of it appropriately when it serves no legitimate purpose, companies can control the volume of information they ultimately must pay for and manage and mitigate the risks associated with retaining unneeded information.

The fear of deleting important information combined with the sheer volume of data generated by most organizations

can seem daunting when embarking on a defensible disposition plan. Addressing several key issues at the start allows a company to effectively implement a plan that can withstand scrutiny from courts and regulators. Without that effort, a company can ensure that it has greater and unpredictable future costs.

There are additional potential benefits to implementing a defensible disposition plan. The dramatic increases in data volumes have produced larger haystacks of unneeded information, making it more difficult and time-consuming for employees to locate the needles of valuable and desired information. To the extent employees are individually tasked with managing their information, that type of searching distracts from their primary employment duties and responsibilities and may contribute to negative sentiments. Therefore, a defensible disposition plan can improve efficiencies and employee morale.

Get Support

A defensible disposition plan that is part of an overall information governance program should ideally receive support from the organization's directors at the highest levels, specifically those responsible for identifying and managing risk (see New ISO Information Governance Standard Can Help Fuel Organization Initiatives, Redgrave LLP Alert, October 2022). Counsel should recognize that not all unneeded information can be disposed of at one time. The plan should instead proceed in phases.

At the outset, the company should identify:

- Individuals knowledgeable about current data repositories.
- The information those repositories contain.
- The regulations and laws to which that data may be subject.
- People willing to execute decisions to dispose of company data defensibly, once the analysis is completed.

Leadership for the project should also leverage other initiatives (such as data categorization for privacy purposes) that may be underway within the company. With the team in place, the plan can evolve and gradually build momentum from word of mouth, early successes, and growth over time. Companies can use short-term successes to gain continuing executive support and obtain enterprise funding to help minimize bottlenecks that may arise concerning who budgets and pays for the defensible disposition efforts.

Develop a Protocol

An effective defensible disposition protocol involves the following steps:

- Defining the company's information objectives and risk tolerance.
- Identifying data or repositories potentially subject to disposition.
- Determining whether a retention obligation or other compliance obligation (such as confidentiality or privacy) applies to the data.
- Deciding whether to retain or dispose of the data.
- Reviewing the data targeted for disposition with appropriate diligence to evaluate whether it is subject to a business, regulatory, or other legal duty to retain, including a litigation preservation obligation.
- Segregate as necessary any data that falls under a litigation hold obligation, for continued preservation.
- Executing the planned disposition:
  - in a timely fashion to avoid the possibility of a preservation duty arising in the interim;
  - consistently with any other obligations surrounding the data (that is, if the data is confidential, ensuring that disposition is securely handled and there is no risk of exposing the data using the disposition process); and
  - confirming that the plan was executed as intended.
- Periodically reassessing the disposition plan, improving processes, and re-prioritizing objectives based on lessons learned.
- Repeating the defensible disposition process across a company's data on an ongoing basis.

When identifying the data available for potential disposition, a company should start with data that has the potential for quick and easy cleanup. Examples include:

- Unstructured data, such as e-mails not belonging to legal hold custodians, which often have little business value once they are read, sent, or acted on.
- Legacy systems that remain even after data was migrated to successor systems.
- Physical storage spaces for legacy media, such as tapes and compact discs.

Companies should also consider whether there are servers that have not been accessed for a long period and appear to have been orphaned or any applications

that are nearing capacity or a breaking point and require quick action. A few examples of these include databases lingering in at-capacity data centers or data centers that are being dismantled due to a consolidation, merger, or acquisition.

Once a company has identified the data that may be eligible for deletion, it must assess whether the targeted data can and should be retained or disposed. This analysis should focus on the company's data retention and preservation obligations. In particular, the project leadership team should consider whether there is one or more of the following:

- A business reason to retain the data.
- A legal or regulatory reason to retain the data.
- An ongoing or reasonably anticipated litigation or investigation that mandates preservation of the data.

If the assessment reveals that there is no basis for retaining the data, then it should be disposed of promptly and properly. Conversely, if certain targeted data must be retained for some period of time, such as until a litigation is resolved, the company should ensure that it has a process in place for disposing of that data once the retention criterion no longer applies.

For a model records and information management policy that describes how a company expects employees to manage company data, see Standard Document, Document Retention Policy.

Use Tools and Technologies

Companies should leverage technology to complement defensible disposition plans and help with disposition decisions. Companies should first evaluate the current IT ecosystem to determine the capabilities of existing applications to identify, organize, and defensibly delete data. Onboarding other technologies may present opportunities to implement a defensible disposition plan. Different solutions may be necessary for the disposition of historical data stores versus dispositions inherent in ongoing data lifecycle management, but there may be overlap. Companies should consider overall needs from a technology implementation strategy perspective before selecting existing or new tools to assist with a disposition plan.

Examples of how different applications or tools may help with disposition include:

- Legal hold management tools help track the status of legal holds and may assist in identifying and preserving data subject to a legal hold. These tools also can help identify data that may become eligible for disposition when a legal hold is released, while ensuring the defensibility of disposition efforts.
- Email platforms, cloud storage applications, and collaboration platforms often contain modules that enforce ongoing disposition of files, primarily based on file location and date. These modules offer customizable settings so that, for example, documents stored in a particular folder are automatically deleted once they reach a certain age when they are not otherwise subject to a preservation obligation, such as a legal hold.
- Advanced search applications can be leveraged to tailor searches targeting files that are no longer needed. These tools often create an index that include data locations, metadata (such as file type and last date accessed), and text. Companies may also be able to use these tools to search and index data stored on backup tapes without fully restoring the environment. The ability to sample and review results within the tool can be particularly helpful when designing a defensible data deletion process.
- Artificial intelligence search tools can be used to assist with grouping documents that can help separate intermingled files to fit within the company's record retention schedule taxonomy as part of its overall information governance program. These tools may do so using unsupervised learning, which clusters similar documents, allowing the user to act on all similar documents as a group. Other technologies may include supervised learning, which may contain or allow building of machine learning models that can efficiently classify documents into the desired taxonomy. Then, files within their retention periods or otherwise subject to preservation obligations may be retained, while older files can be eligible for disposition.
- Other artificial intelligence tools can help identify or extract specific content that may prioritize files for disposition. Examples include tools that may help find files containing personal data, while others may help determine which contracts have expired.

For more on the tools and technologies that can be used to identify and cull data, see Practice Notes, Long Live Predictive Coding and The Advantages of Early Data Assessment.

Do Not Forget Third Parties

Data retained by a third party can generate all the same costs as data retained by the company itself, including

litigation costs, compliance costs, and data breach costs. To implement a truly effective defensible disposition plan, a company must extend the plan to third parties, including vendors and other service providers that store and manage the company's data, to ensure that all of the company's data subject to disposal is deleted according to the plan. This requirement should be added to any contracts or service level agreements with third parties that are storing or managing a company's data, including, without limitation, third parties providing professional services, such as lawyers and accountants. Counsel should be aware, however, that certain privacy regulations may preclude a defense that the company had no reason to believe a third party was misusing its data or in violation of the regulation, or both, when the contract includes these provisions, but they are never enforced or audited. (See, for example, Section 7051(e) of the proposed California Privacy Protection Agency regulations under the California Privacy Rights Act (effective as of January 1, 2023)).

One example that illustrates how a third party's action or inaction regarding a company's data can generate all the same costs involves Laboratory Corporation of America Holdings (commonly known as LabCorp). They had contracted with a vendor (American Medical Collection Agency (AMCA)) to collect past due accounts. The vendor suffered a data breach in 2019, resulting in the personal data exposure of more than 10 million patients. Twenty-three putative class actions were filed against LabCorp (in addition to suits filed against other healthcare providers who had used AMCA), all of which were consolidated in a multidistrict proceeding in the District of New Jersey.

In 2020, a shareholder of LabCorp also brought a derivative suit in Delaware state court against the company's directors and executive officers, alleging that they had violated their fiduciary duties by allowing the company to provide personal healthcare and financial information to a vendor that had inadequate security to protect the patient information and deficient cybersecurity and data breach detection. The derivative action has been stayed pending resolution of the MDL proceeding in New Jersey (see Labcorp's August 2021 10Q SEC filing, pages 17-18). In an extensive unpublished opinion, the New Jersey MDL court ruled in late 2021 that claims against LabCorp could proceed on theories of negligence and negligence per se, as well as a claim under the Massachusetts Consumer Protection Act (see *In re Am. Med. Collection Agency, Inc. Customer Data Sec. Breach Litig.*, 2021 WL 5937742 at *37 (D.N.J. Dec. 16, 2021)).

Including vendors and other service providers in a company's defensible disposition plan

is particularly important in light of the 2022 IBM study's conclusions:

- 45 percent of breaches occurred in the cloud.
- 43 percent of the surveyed companies either were in the early stages or had not started applying security practices to safeguard cloud environments.
- 19 percent of breaches occurred because of a compromise at a business partner.

Data breaches involving a company's vendor or other third parties may be even more costly than if the breach occurred with data maintained on-premises due to state and federal breach notification laws that generally put the responsibility to notify individuals of a data breach on the owner of the data, which is typically the company, not the third party (see Tech Transactions & Data Privacy 2022 Report: Third-Party Data Incidents: Preparing and Responding as the Volume of Incidents Rise, February 10, 2022).

To combat the risk of a third-party data breach, companies should:

- Properly vet outside vendors and service providers before engaging them to ensure that they have implemented the administrative, technical, and physical safeguards necessary to protect any data they are entrusted with, including, without limitation, third parties providing professional services, such as lawyers and accountants.
- Perform periodic risk assessments on their outside vendors and service providers to confirm that the safeguards vetted at the start of the relationship remain in place or have been improved.
- Require outside vendors and other third parties that handle their data to have the same type of, if not more comprehensive, data disposition policies in place.
- Conduct an inventory of those third parties that handle customer data, employee data, or any data type particularly attractive to hackers and other bad actors.
- Ensure contracts and service-level agreements include data disposition and certification requirements.