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

The ever-increasing amount of data being generated by companies has led to the retention of large volumes of unneeded information. Given the costs and risks associated with saving too much information, it is more important than ever for companies to adopt a defensible disposition plan that allows for the systematic disposal of data that is not subject to business, legal or regulatory retention obligations.

MONICA McCARROLL
OF COUNSEL
REDGRAVE LLP

Monica focuses her practice on providing advice and counsel on e-discovery, information governance and cybersecurity issues. She also has extensive experience working as a trial attorney specializing in complex civil litigation, and has tried cases in both federal and state courts.

DIANA FASCHING
SENIOR ADVISOR
REDGRAVE LLP

Diana works with clients' legal, business and information technology teams to identify issues and recommend solutions relating to the lifecycle of information and the integration of emerging technologies. Her experience includes conducting records management and discovery readiness gap analyses, and contributing to the development of legacy data disposition plans.

BENJAMIN JOFFE
ATTORNEY
REDGRAVE LLP

Ben has worked on various matters relating to e-discovery and defensible data disposition. His experience includes assisting in drafting an e-discovery competency and knowledge management plan, preparing defensible disposition strategies, and developing and implementing e-discovery procedures and best practices.

The volume of data companies are creating and storing is growing at an astronomical rate. Whether it is the fear of deleting evidence that may be relevant to future litigation, concerns about complying with increasing government regulations, a lack of resources to devote to managing data or general employee apathy, many companies are keeping too much information. Much of this information has little intrinsic value to the companies or their stakeholders, but could prove to have great worth to hackers, adversaries, competitors, regulators or the general public. It is critical for companies to address this issue by implementing a plan to defensibly dispose of data 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. In addition to storage costs and the costs and risks of potentially reviewing excess data in connection with litigation, the occurrence of a data breach can severely damage a company's reputation and bottom line.

STORAGE COSTS

The costs of storing enormous volumes of data are significant. Among other things, companies may need to pay for storage systems, software, bandwidth and personnel to manage the data. However, a recent study found that 69% of an organization's retained data serves no business, legal or regulatory purpose (*Compliance, Governance & Oversight Council, Information Lifecycle Governance Leader Reference Guide, 2d ed., at 5 (2014)*, available at *cgoc.com*). This means that much of the storage costs incurred by companies are unnecessary and could be avoided with proper data management.

LITIGATION COSTS

Data over-retention also can lead to substantial litigation-related costs, particularly during the e-discovery process. Keeping massive amounts of unnecessary information makes it more onerous and expensive to process, collect and review data for production, as well as to identify and preserve documents subject to a litigation hold. Additionally, saving unneeded data that is not subject to retention requirements raises the risk that unfavorable evidence that should have been deleted may surface during litigation.

Search Litigation Hold Toolkit for a collection of resources to help counsel preserve documents and implement a litigation hold when a company anticipates or becomes a party to litigation.

DATA BREACH COSTS

The headline-grabbing hack of Sony Pictures Entertainment late last year was just the latest in a long line of massive and costly data breaches. A data breach can cost a company millions of dollars, and those costs are expected to rise at an alarming rate. For example, in 2009, a data breach cost Heartland Payment Systems an estimated $140 million, whereas the 2014 Sony hack is expected to cost the company nearly $1 billion.

Some of the costs associated with a data breach are easy to quantify, such as the penalties the majority of states impose under state law relating to the disclosure of personally identifiable information. Although there is no overarching federal law that applies to data breaches, certain key industries regulate or strongly recommend that personally identifiable information remain 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) and the Health Information Technology for Economic and Clinical Health (HITECH) Act.

Intangible costs associated with data breaches 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 about the 2013 Target Corporation breach, its approval rating among consumers plummeted.
- Months after the 2014 Sony breach, the company is still reeling from the disclosure of e-mails between executives that are not just embarrassing, but relationship-damaging.
- Almost two years after Edward Snowden's 2013 security breach, the National Security Agency and other information-gathering organizations throughout the world remain engaged in ongoing damage control.

Often, damages to reputation and relationships are proportional to the size of the data breach. Since a breach may be inevitable, companies should seek to reduce the associated risks.

Search Key Issues in Consumer Data Breach Litigation and Expert Q&A on Standing in Data Breach Class Actions or see page 20 in this issue for information on data breach class actions.

IMPLEMENTING A DEFENSIBLE DISPOSITION PLAN

Defensible disposition refers to the systematic deletion of data in a reasonable, good faith manner, taking into account a company's business, legal and regulatory retention obligations. In other words, a defensible disposition plan involves a process for making disposition decisions that can withstand a legal challenge.

A defensible disposition plan falls within a company's overall information governance program for managing company data. By adopting strong information governance policies and procedures that include not only effective methods for retaining and handling data, but also for disposing of it when it serves no legitimate purpose, companies can control the volume of information they ultimately must pay for and manage.

The fear of deleting important information combined with the overwhelming amount of data can make undertaking a defensible disposition plan seem daunting. However, by addressing several key issues at the start, a company can effectively implement a plan that will hold up in court.

GET SUPPORT

At the outset, the company should find and engage people who are willing to dispose of company data defensibly, and gradually build momentum through word of mouth and early successes. Short-term successes can be used to gain executive support, as well as to obtain enterprise funding to help minimize bottlenecks that otherwise would inevitably arise because of issues regarding who will budget and pay for the defensible disposition efforts.

DEVELOP A PROTOCOL

An effective defensible disposition protocol involves the following steps:

- Identifying the data subject to disposition.
- Assessing the data to determine whether a retention obligation applies.
- Deciding whether to retain or dispose of the data and taking the appropriate action.
- Repeating the defensible disposition process across a company's data on an ongoing basis.

As a preliminary matter, companies must come up with a plan for identifying the data available for potential disposition. They should start with low-hanging fruit, that is, data that has the potential for quick and easy cleanup. Examples include:

- Unstructured data such as e-mails, which often have little business value once they are read, sent or acted on.
- Legacy systems that still exist even though data was migrated to successor systems.
- Large legacy tape storage closets.

Companies should also consider whether there are any areas that are at a breaking point or require quick action, such as orphan servers and databases lingering in at-capacity data centers or data centers that are being dismantled due to a consolidation, a merger or an acquisition.

Once a company has identified the data that may be eligible for deletion, it must conduct an investigation to assess whether the targeted data can and should be retained or disposed. The foundation of this analysis is the company's data retention and preservation obligations. In particular, counsel must consider whether there is:

- A business reason to retain the data.
- A legal or regulatory reason to retain the data.
- An ongoing or a threatened litigation that mandates preservation of the data.

If the assessment reveals that there is no basis for keeping certain data, then it should be disposed of promptly and properly. Conversely, if the data is required to be retained for some period of time, for example, 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.

Search Document Retention Policy for a model records and information management policy that describes how a company expects employees to manage company data, with explanatory notes and drafting tips.

USE TOOLS AND TECHNOLOGIES

Rather than trying to conduct a manual, item-by-item review of the data, companies can use tools and technologies to complement defensible disposition plans and aid in disposition decisions. For example, companies may consider employing tools and technologies that:

- Identify "junk" data, which clearly are not company records and have no business value (such as e-mails regarding personal Amazon.com purchases or office Fantasy Football pools). Examples include advanced analytics or technology-assisted review.
- Allow companies to sample and gain insight into the contents of backup tapes without requiring the purchase and implementation of a restore environment. Examples include tape indexing or analysis engines.

Search Predictive Coding: It's Here to Stay and The Advantages of Early Data Assessment for more on the tools and technologies that can be used to identify and cull data.

DO NOT FORGET THIRD PARTIES

To implement a truly effective defensible disposition plan, a company must extend the plan to third parties, including vendors. For example, third parties that store or manage a company's data should be subject to the same disposition protocol so that all of the company's data subject to disposal is deleted according to the plan. Consistency is critical when defending the disposition of data in litigation.

Additionally, data breaches involving a company's vendor or other third party may be costly. Indeed, the SEC identified vendors and other third parties as a potential soft spot for unintentional data disclosure issues (see *SEC Office of Compliance Inspections & Examinations: Nat'l Exam Program Risk Alert, OCIE Cybersecurity Initiative (Apr. 15, 2014)*, available at *sec.gov*). Accordingly, a company should understand and verify how any third party that has access to its data will defensibly dispose of that data at the appropriate time.

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

- Perform risk assessments on their outside vendors.
- Require their outside vendors and other third parties that handle their data to have the same type of, if not more comprehensive, policies in place.
- Conduct an inventory of those third parties that handle customer and employee data.