Managing Corporate Data in the Era of Mobile Tech and the Internet of Things

By Jeff Kerr

Our golden age of digital convenience is shadowed by vast amounts of unmanaged and unorganized data. According to the website Backblaze, the price to store a gigabyte of data has dropped from $500,000 in 1980 to less than $0.03 today. And as businesses and consumers invest in new devices and applications, we're generating more data than ever. It is now generated by both people (e.g., someone writing an email) and machines (e.g., location tracking, database logging and automatic step counting). There's almost always more data than we know, and even experts find it difficult, if not impossible, to collect all of the data belonging to a person or a business.

The increase in the amount and complexity of data has serious legal implications for American businesses in the areas of data security, e-discovery and recordkeeping. Without good data management (aka "information governance"), enterprise data can become a liability. Data that is not managed properly is more vulnerable to data breaches, as well as more difficult to locate and produce if it is needed in e-discovery. Indeed, during litigation, widely distributed and poorly inventoried data has a direct relation to e-discovery cost because of the time that must be spent collecting it.

Beyond cost, overlooked sources can create problems of their own. To tame the chaos and minimize the risk of growing data, businesses need to be aggressive in designing and implementing data management policies. These policies should be informed by regulatory requirements and rules related to the preservation of evidence, and they should generally be drafted with the assistance of counsel. They also need to be accepted at all levels of the organization. If you have a rule that employees may use only employer-approved (or issued) devices for business purposes, that rule should apply to the CEO, too.

UNDERSTANDING ENTERPRISE DATA

The impact of mobile computing and cloud-based applications on the challenge of information governance can hardly be overstated. Cloud computing means that data is more and more decentralized. Rather than having a central set of on-premises servers, businesses — sometimes unwittingly — rely more and more on both public and private cloud infrastructures. Most new software products used by businesses are accessed through websites, with data stored on cloud infrastructure; the software is leased by the software provider and owned by major vendors, such as Amazon and Rackspace.

At the other end of the spectrum, many employees take work home with them and use laptop computers, smartphones and tablets to do their work. At any time, a business's data could be spread across thousands of devices. Keeping tabs on this data, managing it and finding it can be an enormous challenge. Nonetheless, cloud computing and mobile devices are popular because they drive productivity and are often superior to other alternatives. It is unlikely that banishing them from your business will be a workable solution.

AVOIDING DATA PROLIFERATION

David Cole, a partner who practices in data security, privacy and e-discovery law with Freeman Mathis & Gary LLP, suggests that to mitigate the risks associated with data inundation, businesses keep only the data they need and for only as long as they need it. Even so, challenges remain, including the large number of devices involved and the varieties of operating systems, platforms

and applications. A simple first step is to keep an inventory of the company's electronic assets. This can be facilitated by IT, which should register and configure each device.

Cole notes that a key source of trouble is having multiple repositories for corporate data, some of which (such as employee-owned smartphones) may not even be in the custody and control of the corporation. "The simplest solution is to not allow the storage of company data on mobile devices," he says. "You can do it by policy, but that can be hard to enforce. You can also disallow it, not by policy, but by design of your data infrastructure."

At a minimum, Cole says, "a business should have a clear policy of not allowing corporate data on employee-owned devices, and the policy should be enforced." To control where data is stored, one option he recommends is so-called "thin" or "zero" client deployment of employer computer systems. With this model, he says, "employees use devices with little to no local storage, and those devices simply connect to a remote server that hosts the operating system, applications and data."

Accordingly, when an employee saves a file, the file is saved not to a hard drive connected to the computer at the employee's desk, but to a server that the business can access and control. This system can be easier to administer and more secure than setups that spread data across numerous hard drives.

Cole also recommends that businesses provide employees with "approved, corporate-controlled applications for work communications, and then allow only employees to use those applications." This prevents the kinds of problems that will arise when employees, wanting to rely less on email, turn to an internal chat application without consulting IT or management. This can result in relevant communications needed for e-discovery being spread across numerous devices and applications.

When the company creates or designates corporate-controlled applications for all work communications, they become centralized and easily accessible. This also allows the business to ensure that its chosen vendor complies with data security and e-discovery requirements, and makes clear that unauthorized software violates policy.

MANAGING DATA IN LITIGATION

When there's actual litigation, the stakes become even higher. It's essential at the beginning of a case, Cole says, that preservation notices be issued to all individuals who may have data relevant to the case, and that the notice be written in plain English, with the expectation that it will end up in the hands of the opposing party.

Indeed, Cole recommends that preservation notices be issued not only by legal counsel, but also by management to employees, with the expectation that they will be discoverable. A primary purpose of a well-crafted preservation notice is to ward off claims of careless or intentional destruction of evidence.

Inside counsel must also monitor compliance with preservation measures. If there's any reason to believe that a particular employee may be inclined to ignore the notice or attempt to destroy data (a reasonable assumption when the data would be damaging to the employee personally), counsel may opt to have a computer forensics specialist preserve the data without notifying the employee.

THE ROLE OF SOFTWARE

The variety of software is one of the causes of data chaos, but it can also help mitigate the problem. In advance of litigation, businesses should choose software with an eye to needs that will arise during litigation. For example, ask vendors during the purchasing process how data can be locked down in the event of a legal hold, and how it can be collected during e-discovery. Many vendors will not have a ready answer, but a larger organization may be able to push vendors to address these issues in their applications.

Some vendors are reading the handwriting on the wall. Google Vault, for example, adds archiving and e-discovery features to the company's business email, storage and calendaring products. With pressure from purchasers, more vendors will build documented e-discovery and records retention features into their products.

There are many tools to assist businesses during litigation, with data collection, de-duplication, search, review and production. Some of these tools are marketed primarily to e-discovery vendors, who then charge steep fees to their clients. Others offer a more economical self-service model. Deciding on the right tools for the project is possible only if the project has been properly scoped. Will there be 15 gigabytes of data, or 15 terabytes?

If it's the former, you may get along without industrial strength tools and teams of experts; but if it's the latter, you will need powerful technology. Remember, however, that possessing 15 terabytes of data does not mean your e-discovery project will embrace all of it. Some, if not most, could be unrelated to claims and defenses or could be duplicative.

One litigation tool that inside counsel should consider is software for managing a matter's most important documents and communicating the importance of those documents to outside counsel. Several vendors offer tools for constructing chronologies that link key documents to the facts of a case. These tools can be invaluable for coordinating case strategy with outside counsel.

In sum, the proliferation of data creates challenges, and failing to manage data creates risk. Businesses need to actively manage the data they create and retain, and their plans and procedures need to be informed by legal requirements. Counsel who understand both the legal side and the technical side of this issue are best positioned to help a business meet these challenges. ■

Jeff Kerr is CEO and co-founder of the legal and case management software company CaseFleet.

jeff@casefleet.com