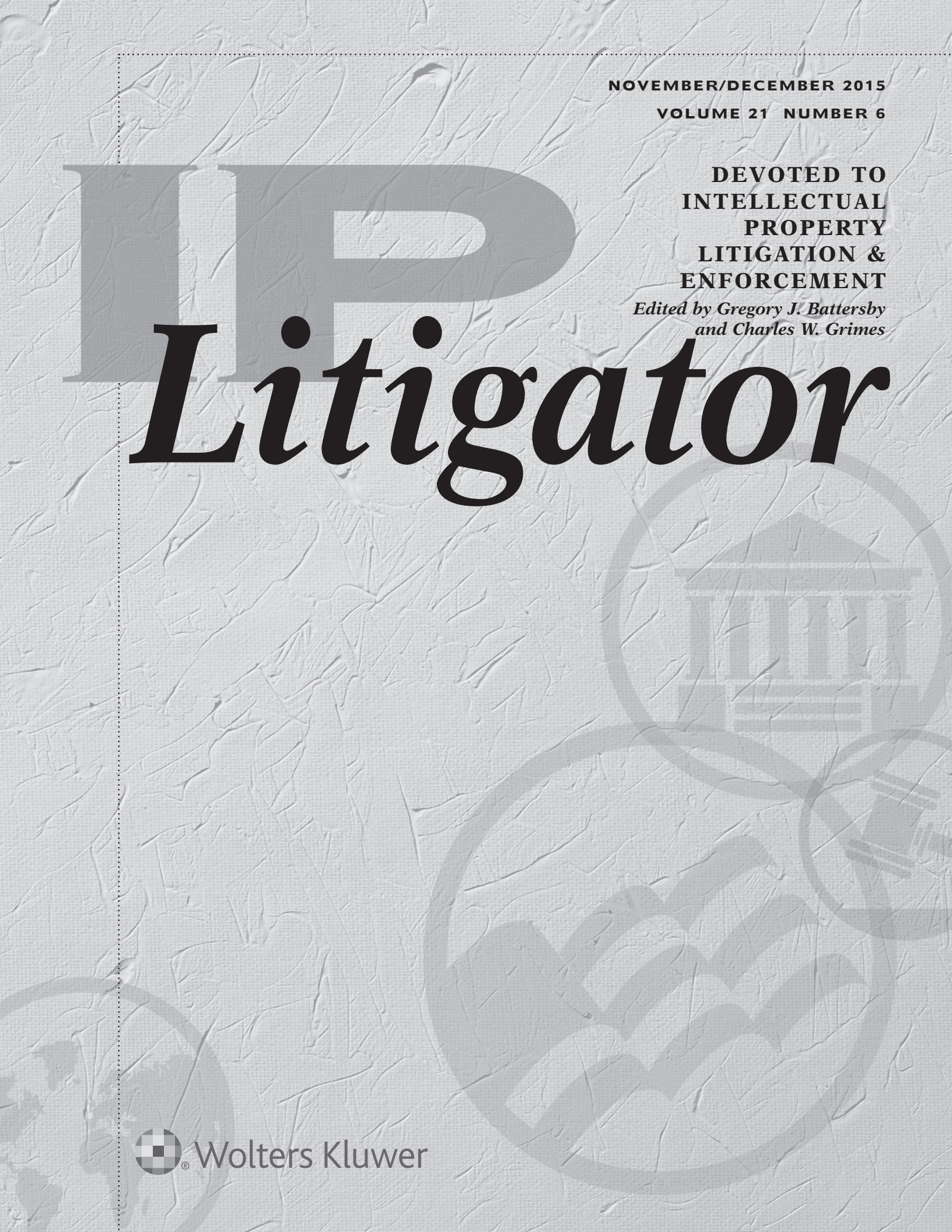
NOVEMBER/DECEMBER 2015
VOLUME 21 NUMBER 6

IP Litigator

DEVOTED TO INTELLECTUAL PROPERTY LITIGATION & ENFORCEMENT

Edited by Gregory J. Battersby and Charles W. Grimes



Wolters Kluwer

Discovery

Kim Leffert and Michael Bornhorst

Ensuring that Cloud-Based Information Is Properly Stored and Accessible

Consider the following scenario: A large corporation has received notice of a purported contractual breach of a nationwide distribution agreement. The facts central to this dispute will be reflected in emails, documents, and other forms of electronically stored information (ESI) generated across offices. The corporation previously had retained a third-party vendor to provide a cloud-based solution to manage and maintain its ESI. As a result of that, the corporation's general counsel expects that much of the data relevant to this dispute is stored "in the cloud" rather than in any office.

Cloud Computing Storage of ESI

Cloud computing consists of computing resources—hardware and software—that are made available for use over the Internet by a service provider, typically on a subscription basis. More and more, companies are using cloud computing to reduce IT-related costs and to make data more readily available throughout the company. To stay current with the latest technology, minimize their own support costs and attract the widest customer base possible, cloud service providers often build their platforms on standardized products that offer little or no customization. As a result, frequently there is limited flexibility with regard to how ESI can be retrieved from a cloud service provider once that data has been uploaded.

Cloud-Based Discovery Need Not Be Stormy

Although "the cloud" has changed the way corporations (and individuals) maintain ESI, it has not changed a corporation's obligation to preserve, collect, and produce ESI in the event of litigation. Nevertheless, given that data stored in the cloud typically is maintained off-site by a third-party vendor, satisfying these obligations can be a challenge. This challenge is then frequently exacerbated by the lack of uniform standards by which cloud computing service providers address electronic discovery considerations and the fact that these service providers are sometimes unfamiliar with electronic discovery practice altogether.

Nonetheless, a company can effectively manage e-discovery obligations while maintaining its data on the cloud. Planning and communication are the keys to success. More specifically, when a company has reason to believe that its preservation or discovery obligations have been triggered, it should, among other things:

- **Determine on which cloud(s) the data is stored.** It is not uncommon for companies to rely on multiple cloud service providers to store company data. For instance, one service provider may host the company's software applications and the related data while another hosts the company's email platform. Thus, a good first step is to consult with the company's IT department with the goal of creating a comprehensive list of the company's cloud service providers and the types of data they store.
- **Determine how relevant ESI within the cloud can be identified.** After determining where the company's data is stored, the next step is to identify what ESI should be extracted from the cloud. Applying targeted keyword searches to a company's ESI can narrow the scope and cost of a company's document collection, review, and production. However, performing keyword searches in the cloud can be a challenge. Some cloud service providers give users direct access to the stored data, while others may only permit access through a proprietary user interface that offers limited interaction with the data. While some providers can apply powerful forensic applications to the data they store, others maintain data in a way that limits or prohibits keyword searching. Consider working with your cloud service provider(s) to identify the various options available to assist with the identification of relevant ESI stored within the cloud.
- **Determine how the ESI will be retrieved from the cloud.** Once the relevant ESI has been identified, it must be extracted. Cloud computing service providers vary in their ability to export data. On one end of the spectrum are providers that allow their users to rapidly download data in bulk. On the other are those providers that are only able to export files one at a time. Where the company's cloud provider falls within this spectrum may determine whether discovery deadlines can be met. What is more, there are cloud service providers that only can export files using certain formats (such as PDF) even if the file was not

originally created in that format. It may be necessary to consider a work-around if the company's e-discovery obligations require that files be produced in their native format. For these reasons, companies need to consult with their cloud service providers to understand how they can, and cannot, export responsive ESI, preferably before committing to discovery deadlines and obligations.

- **Determine whether the ESI's metadata has become "cloudy."** Sometimes, compliance with e-discovery obligations requires that ESI be collected and produced in a manner that preserves the integrity of its metadata. Doing so is not always straightforward when retrieving data from the cloud. Some cloud computing service providers separate files from their metadata when storing data. If this is the case, retrieving a file and its metadata requires two separate downloads: first the file, then its metadata. In addition, some providers store or export data in a manner that may not accurately preserve the dates associated with the file, such as replacing a file's creation date with the date that file was imported/uploaded or exported/downloaded. If the preservation of metadata is important in your e-discovery plan, be sure to learn whether your company's cloud service provider stores data in a manner that impacts a file's metadata.
- **Determine if the cloud should be put on hold.** Parties that anticipate litigation typically must take steps to ensure the preservation of documents reasonably related to the subject of the litigation. This is commonly referred to as a "litigation hold." Meeting this obligation can be complicated when the relevant data is stored in the cloud. Data retention and destruction policies vary widely between service providers. Thus, when relevant ESI may be stored in the cloud, companies should consider making their cloud service providers aware of any litigation hold. Further, it may be necessary to reach out to your cloud service providers to determine whether any additional steps may be needed to preserve the data they store.

Conclusion

Currently, there is no uniform standard or approach that all cloud service providers use to support e-discovery. Every service provider is different. As a result, by engaging in a proactive dialogue with the third-party service providers maintaining the company's data in the cloud, a corporation can seek to ensure that it meets its discovery obligations while still enjoying the benefits provided by cloud computing.

Kim Leffert is a counsel at Mayer Brown in Chicago, IL and a member of the Litigation & Dispute Resolution practice. One of the founding members of the firm's Electronic Discovery & Information Governance group, a significant and growing part of Ms. Leffert's work involves electronic discovery issues.

Michael Bornhorst is a senior associate at Mayer Brown in Chicago, IL and a member of the Litigation & Dispute Resolution practice and Electronic Discovery & Information Governance group.