Bloomberg Law Reports® Technology Law

Seeing in the Clouds: Understanding Why You Need to Know Where Your Data Lives

Jonathan Redgrave, Redgrave LLP, and James Sherer

In recent years, more corporate resources and data storage have moved to "cloud computing." While determining the location of the cloud computing services and data was initially thought to be difficult, if not impossible, conventional wisdom has changed expectations, and industry and government experts now expect a much clearer picture of where their information resides, and where it has traveled. These expectations modify attorneys' responsibilities for tracking this information, understanding cross-border implications, and can impact potential discovery responses. In short, the globalization of data services brings into play the real-life consequences of data crossing borders and potentially being subject to the laws of each affected country.

It took decades before UPS offered external tracking access to its customers. As of 1995, UPS recorded only 100,000 online tracking requests for the entire month of December (the busiest month).[1] Now, package tracking is understood as a given in a business environment built on just-in-time manufacturing, competing deadlines, and constant comparisons to the near-instantaneous nature of e-mail and on-demand data delivery.

Package tracking was a major step forward for industry and individuals, but its importance demonstrates an inherent difference between a physical shipment and an electronic communication: package tracking is important because there is someone waiting, for more than a second, on the other end. The path an Amazon-shipped book or Cairo-manufactured widget takes can be traced across a map, representing real hand-offs in airport hangars and trucking hubs. But e-mail and data delivery can take quite different routes — and between some data's creation and receipt, it was thought that the data might never be "'located' in a specific place"[2] at all.

Surprisingly, early discussions of new resources, such as cloud computing, seemed to remove the ambiguity of *where* and *how* the data actually travels by the very nature of the cloud's complexity. This was due in large part to the way these services operate when maintaining client data. Because the primary driver for resource allocation was speed, not necessarily location, providers of cloud services often relied "on content-data networks that store commonly retrieved data in Internet points of presence ("POPs") around the world."[3] Resource allocation might shift instantaneously, and specific locations for data were sometimes unclear even for the service provider.

Commentators such as Christopher Kuner have couched much of the debate over international data privacy and the legality of data transfer as a discussion of jurisdiction, often focusing on the "place of storage or processing of personal data."[4] But the above ambiguity served, in some instances, to resolve the issue of jurisdiction into a more

---

simple consideration of where the information originated, and where it ends. Defining "where it goes" within the cloud was postulated as an impossible conjecture.

E-mail and data, in transit or in storage within the cloud, might not have had a specific locale to assist a corporate query for a missing document or piece of evidence. But even with an understanding of this ambiguity, attorneys understood there was no "true" protection afforded under this regime. If questioned, it also provided little defensible protection against government-asserted cross-border data transfer infractions. Modern legal scholars well-versed in information technology are adamant that "[c]ross border harms that occur via the Internet are not any different than those outside the Net. Both demand a response from governmental authorities . . . ."[5] This created a new tension for the in-house or outside counsel collecting "cloud" information for a considered deal or evolving lawsuit — and the continued need to consider not two, but three fundamental factors: where the information originates, *where it goes* within the cloud, and where it goes at the end of the journey.

Despite this tension, this concern remained something of a novelty in actual practice until recently. In an August, 2010 report, the US Government's Chief Information Officers Council ("CIOC") worked to refine the proper use of cloud computing providers by federal agencies. In that report, the CIOC did focus on this concern — where the data *is* before it *ends up* — and admonished agencies that a possible outcome of using a cloud computing provider is that the "Federal government cannot access the data to perform necessary audits. The data has been moved to a different country and a different server and the government suffers a loss in reputation and trust."[6]

The CIOC understood the global nature of "cloud storage" and defined it as "widely dispersed servers or databases located domestically or even overseas."[7] Based on prior discussions within the industry, the CIOC's emphasis on the possible ambiguity of a transient location for data was certainly not misplaced. However, as this technology has matured, cloud computing experts now agree that cloud storage is *not* impossible to locate, and challenge the idea that cloud computing equals anonymous, amorphous storage "somewhere" in the world. In a recent interview, the Cloud Security Alliance's Jim Reavis clarified what he believed to be a fundamental confusion about cloud computing resources, stating that customers of those services "may have this [belief of] real anonymity of the geography of where your information is stored, where with traditional outsourcing you have the knowledge of — in fact we can pick a specific co-location facility, and a lot of that may not be available in cloud . . . that's really one of the biggest things that we see out there [that is] just a misunderstanding."[8]

The CIOC agreed, and in that August 2010 report, stated that government agencies, when conducting a Privacy Threshold Analysis ("PTA") before engaging a cloud storage provider, should determine "where the server on which the data will be stored is physically located."[9] In the same breath, however, the CIOC immediately acknowledged that providers of these services "may not typically disclose where their data centers are physically located."[10] The CIOC then specifically referred its readers to Tom Vanderbilt's New York Times article *Data Center Overload* for a more fundamental understanding of what Vanderbilt tellingly describes as a "vast, dispersed network of interdependent data systems [that] has lately come to be referred to by an appropriately atmospheric—and vaporous—metaphor: the cloud."[11] Vanderbilt is not the only commentator discussing the operation of data storage within the cloud; Robert Gellman also acknowledges that "[i]nformation in the cloud may have more than one legal location at the same time, with differing legal consequences."[12]

The new reality is simple: it may not be easy to determine if your enterprise or client uses cloud computing resources and, if so, where those

resources (and your specific) data might be located. But, experts say it can be done, and the US Government's privacy committee says it should be done. And, while deeper analysis adds costs and may require expert assistance, not all outcomes are necessarily bad for a corporation or client. Offshoring of data within a cloud might subject valuable business information to additional data privacy and/or litigation protections. For example, Gellman recognizes that data given to a cloud provider in France "would acquire rights of notice, access, correction, etc. under French Law,"[13] and other, specific country rules may make locations attractive for a company's proprietary data mining techniques, similar to the protections Swiss banking laws once provided. Gellman also stresses that a "provider who promises to maintain user data in a specific jurisdiction (e.g., the United States) may reduce some of the location risks that a user may face."[14]

The converse to any additional benefits that come with easy international data operation is the consideration of data movement when performing due diligence in multi-national business transactions, or when engaged in cross-border data transfers during litigation discovery. Gellman highlights the concern that a cloud provider faced with a government or civil subpoena "would not have the same motivation as the user to resist a subpoena or other demand."[15] Other concerns include the State in which the data is held, as a specific data location may have "minimal security safeguards in place that technically satisfy the local requirements (although they may fall far short of security requirements in jurisdictions with more rigorous standards)."[16]

From the legal perspective, The Sedona Conference, a 501(c)(3) research and think tank organization,[17] sponsored a conference in September in Washington, D.C. concerning cross-border e-discovery and data privacy issues. The conference, featuring participants from around the world, tackled the complexities presented by the globalization of business (including cloud computing models) from the standpoint of country-specific data privacy concerns among other issues. The explication of issues at the conference reflected the relative infancy of regulation of the cloud but a growing awareness of the need for rules that can help corporations understand and comply with data privacy obligations. Data protection authorities and third party organizations, such as The Sedona Conference's Working Group 6, are working on guidance documents that will likely be issued in the next 6-12 months.[18]

In sum, the cloud's inherent, irreducible complexity does not excuse an organization from understanding where its data is processed and resides and whether those arrangements implicate privacy and data transfer laws. The responsibility to understand where data is stored in the cloud affects large and small entities that are now taking advantage of the efficiencies offered in the cloud. Notably, entities should closely examine whether the location of the data at any point gives rise to rights for those persons as to which the data at issue relates and how those rights are impacted by the transfer of data to and within the cloud.

As a practical matter, careful attention to originating service contracts with cloud computing providers, with promises of data-location specificity by the vendor as well as specific representations and warranties regarding data protection and privacy, can provide a powerful tool for organizations to better manage risk, and possibly implement additional protections. Similarly, multinational organizations (and purely domestic companies that have taken advantage of international data operations) need to think through their approach to legal discovery (from preservation through collection to production) as it applies to data that are within their legal control but hosted in the cloud.

Jonathan Redgrave is a Partner at Redgrave LLP in Washington, D.C. James Sherer was most recently in-house counsel with The Dow Chemical Company. He is currently travelling the world, sampling the

tastes and data protection regulations of countries in multiple continents. The views expressed in this article are those of the authors do not reflect the views of Redgrave LLP or others.

---

[1] *UPS Reaches Online Tracking Milestone*, BUSINESS WIRE, Dec 20, 2000, *available at*http://findarticles.com/p/articles/mi_m0EIN/is_2000_Dec_20/ai_68281602/ (last visited Nov. 1, 2010).

[2] Kuner, C., *Internet Jurisdiction and Data Protection Law: An International Legal Analysis*, 47 (2010), *available at*http://www.privacyconference2010.org/upload/Conflict%20Kuner_article.pdf (last visited Nov. 1, 2010).

[3] Vanderbilt, T., *Data Center Overload*, N.Y. TIMES, June 8, 2009, *available at* http://www.nytimes.com/2009/06/14/magazine/14search-t.html?pagewanted=all (last visited Nov. 1, 2010)

[4] Kuner, *supra* note 2 at 47.

[5] Goldsmith, J. & Wu, T., *Who Controls the Internet?* (Oxford University Press 2008).

[6] Chief Information Officers Council, The Privacy Committee, Web 2.0/Cloud Computing Subcommittee, *Privacy Recommendations for the Use of Cloud Computing by Federal Departments and Agencies*, August, 2010 (p. 3) *available at* http://www.cio.gov/documents_details.cfm/uid/8FA78033-5056-8F64-364A9E774146990A/structure/Information%20Technology/category/IT%20Security-Privacy (last visited Nov. 1, 2010).

[7] *Id.* at 8, n. 9.

[8] Field, T., *Cloud Computing Leaders & Laggards: Interview with Jim Reavis of the Cloud Security Alliance* Information Security Media Group (August 18, 2010) *available at* http://www.bankinfosecurity.com/articles.php?art_id=2851 (last visited Nov. 1, 2010).

[9] Privacy Committee, *supra* note 6 at 7.

[10] *Id.*at 7, n. 5.

[11] *See* Vanderbilt, *supra* note 3.

[12] Gelman, R., *Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing*; World Privacy Forum, February 23, 2009, at 7. *available at* http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf (last visited Nov. 1, 2010).

[13] *Id*. at 19.

[14] *Id.* at 18.

[15] *Id.* at 14.

[16] Wugmeister, M. *et al.*, *Global Solution for Cross-Border Data Transfers: Making the Case for Corporate Privacy Rules*, 38 GEO J. INT'L LAW 449; (2007) *available at* http://www.mofo.com/docs/pdf/0801CrossBorder.PDF (last visited Nov. 1, 2010).

[17] The Sedona Conference, www.thesedonaconference.org (last visited Nov. 1, 2010).

[18] The Sedona Working group will be publishing a monograph setting forth principles to address cross-border discovery issues much like the original Sedona Principles that were originally published in draft form in 2003.