Cyberspace Lawyer
January-February, 2010

CLOUD COMPUTING: WHOSE LAW GOVERNS THE CLOUD? (PART III)

Barry Reingold, Ryan Mrazik, Miriam D'JaenFN[FNa1]

Introduction

This article is the last of a three-part series looking at cloud computing from market and legal perspectives. Part I, published in the June 2009 issue of *Cyberspace Lawyer*, examined the technological and business capabilities of cloud computing and the associated privacy and data security concerns. Part II, published in the September 2009 issue of *Cyberspace Lawyer*, highlighted recent industry and policy developments.

This Part focuses on key jurisdictional issues that will shape the future of cloud computing: Whose law governs cloud services, especially if there is a security breach? And who has possession, custody or control over data in the cloud that is sought in litigation? Finally how will courts resolve conflicts of law between overlapping jurisdictional claims over conduct by cloud service providers?

Who Has Jurisdiction?

The Internet, almost by definition, implicates the laws of multiple jurisdictions. Which jurisdiction's laws will apply to information stored in a cloud, particularly in a situation involving a data breach, may turn on the type of user, the location of the user's computer, the location of the cloud provider's server(s), or some combination of these variables.

In the United States, some federal privacy, data protection, and computer fraud statutes, including the Children's Online Privacy Protection Act (“COPPA”), the Gramm-Leach-Bliley Act (“GLBA”), and the Computer Fraud and Abuse Act (“CFAA”), assert jurisdiction when (a) American consumers are targeted for harm through (b) computing services used in interstate or international commerce.FN[FN1] As such, these and other laws that assert jurisdiction based on the location of a resident will protect personal information, even as it is transferred from in-country computers to offshore cloud computing services.

Also in the United States, state data breach notification and data protection laws typically assert jurisdiction over (1) data protection practices that injure state residents, regardless of the location of the actual data, and (2) entities that do business in the state.FN[FN2] These state statutes vary widely on coverage (what types of data collection), terms (how restrictive) and remedies for breach (civil, criminal, with or without a private right of action).FN[FN3] Regardless, the models for asserting jurisdiction in these statutes-over the personal information of state residents and over entities doing business in the particular state-could subject cloud service providers and their clients to breach notification and data security requirements in multiple locations with conflicting laws.

The situation in the European Union is also complex. In 1995, the EU passed a comprehensive data privacy directive (the "Directive") that provides a framework for data protection laws across Europe and requires member states to enact their own national data protection laws.FN[FN4] The Directive also requires member state to establish local Data Protection Authorities ("DPAs"), which are government agencies dedicated to privacy and the administration of data protection laws. Some DPAs are more proactive than others, and Spain is generally regarded as the toughest EU data enforcement state.

The Directive applies both within the EU and extraterritorially; it specifically prohibits cross-border data transfers from EU member states to countries with "inadequate" data protection laws - one of which is the United States.FN[FN5] Not surprisingly, the Directive has had a profound impact on multinational companies that collect data from EU data subjects.FN[FN6] The ability to enforce it, however, remains questionable, particularly for data collectors with no physical presence in the EU.

How would this multi-jurisdictional framework apply in practice? In a hypothetical example, assume a US-based health insurance company contracts for claims processing software and storage with an EU-based cloud computing service, with server farms in the UK and France. This is an "infrastructure as a service" ("IaaS") contract. Under the contract, the claims information originates from policyholders located in all 50 states. A few policyholders are citizens of EU member states who are working temporarily in the US. Policyholders submit the data to the insurance company's servers in New York City, which then organize and relay it to the cloud provider's servers in the EU. After processing, the data is returned to the insurance company, with a copy stored on the cloud providers' servers.

Assume the contract gives the cloud service provider unlimited discretion to decide which components of its system are made available to process and store the insurance company's data. On this point, the contract expressly authorizes the cloud provider to switch processing and storage from one of its servers to another in response to changing system capacity demands, and "to undertake all steps reasonably needed to ensure the proper functioning of its system." The contract is silent, however, as to whether in periods of excess demand, the cloud provider may contract with third parties to lease extra capacity.

The contract includes the parties' reciprocal representations that their services will comply with "all applicable data security and privacy laws and regulations." The contract also requires the cloud provider to indemnify the insurance company for damages arising from the provider's "negligent acts or omissions." The contract does not require the cloud provider to buy any specific amount of insurance coverage, or to get a performance bond.

Six months after the service begins, the cloud provider has an unexpected aggregate spike in demand. It decides to contract with a small EU data management firm with a server farm in Spain temporarily to offload some of the cloud provider's data, including that of the insurance company. One week later, a disgruntled former employee of the Spanish firm hacks into the database, pulls the claims information, and posts it on the Internet. Not surprisingly, much of it consists of sensitive personal information about the policyholders, whose names aren't omitted or otherwise masked. Data security enforcement authorities in the US (both federal and state level), the UK, and Spain open investigations. Policyholders whose information has been disclosed are considering a class action in the United States against the insurance company.

Which firms are potentially liable under which laws? Who has or should have jurisdiction? And how could the insurance company better have protected itself?

In the US, health-related data in the possession of the insurance company is governed by the Health Insurance Portability and Accountability Act ("HIPAA") and laws of the states in which the policy holders reside. FN[FN7] As discussed above, jurisdiction under these statutes typically turns on the location of the injured consumers or the location of the business entity, rather than the location of the facilities through which the breach occurred. Thus, the US-based policyholders would likely have remedies available against the US-based insurance company, even though the breach occurred while their data was located in Spain. And they would likely have these remedies even if their insurance policies included as a standard term of service the insurer's disclaimer of liability for data loss or misuse because such disclaimers may not trump statutorily-provided rights.

More troublesome is the fact the breach took place while the data was in neither the insurance company's nor the cloud provider's control. Had the breach happened while the data was in the cloud provider's control, the insurance company might be liable to policyholders on the theory the cloud provider was the insurance company's agent. But the breach happened while the data was in the control of the Spanish firm, with whom the insurance company had no contract - indeed, of which it had no knowledge.

That fact alone might arguably bar recovery by the policyholders against the insurance company. But could the policyholders argue the insurance company was negligent in not addressing in its cloud services contract the possibility the cloud provider would outsource some services to another party? Note the indemnity between the cloud provider and the insurance company would not bar policyholders' claims or a United States government enforcement action against the insurance company. It would simply shift to the cloud provider financial responsibility for damages and penalties assuming the insurance company can show the cloud provider was negligent.

The situation in the EU is more complicated. Because the Directive protects the personal information of citizens of member states alone, it applies only to the few policyholders who are EU citizens. There is also some question about which party would be subject to liability as the "data controller" - that is, party who controls the "the purpose and means" of data processing. Under the Directive, both the insurance company and the cloud provider may be considered "co-controllers," and, equally liable. As a practical matter, however, because it is physically present in the EU, the cloud provider is more susceptible to enforcement of a judgment against it for non-compliance with data protection laws. Penalties vary by member state; therefore, the cloud provider could face a range of civil and criminal penalties depending on where the policyholders reside.

This scenario highlights the importance of drafting detailed data control, risk allocation, and indemnity provisions in cloud service contracts. These agreements, when negotiated by sophisticated commercial enterprises, should include data security provisions and clear allocations of financial risk in the event of a breach. The contract in our hypothetical lacked such provisions. With respect to indemnity claims against the cloud services provider, the insurance company would be in a stronger position if the contract had barred the provider from contracting with third parties without the insurance company's consent, or had expressly required the provider to guarantee the performance of any third-party providers and indemnify the insurance company against any performance-related loss. Also, the insurance company should not have agreed to condition its indemnity rights on proof of the cloud provider's negligence.

Who Has Possession, Custody or Control of Data in the Cloud?

In civil litigation in the United States, a party (or subpoenaed non-party witness) may be required to produce all relevant, non-privileged data in its "possession, custody or control." FN[FN8] This includes data stored with a cloud provider to which the party or witness has a contractual or common law right of access. Because the party or witness has this right, a discovery request or subpoena directed to the party or witness should result in production of the information, regardless of where the cloud provider's servers are located.

But what if, for whatever reason, the party or witness refuses to request the information from the cloud service provider, or to turn it over if copies are already in the party's or witness's possession? May a civil litigant subpoena the information directly from the cloud provider?

In the context of civil litigation, a third-party cloud service provider has no obligation to turn over user information or content and will likely not do so absent proof of consent of the user or a court order.FN[FN9] Where a party or witness, however, will not consent to the disclosure, the court may order the party or witness to consent to the disclosure. The service provider can then make the disclosure pursuant to that consent, as authorized by statute.FN[FN10]

For example, the Stored Communications Act, 18 U.S.C. §§2701-2712 ("SCA"), which prohibits voluntary disclosures of user data by providers of electronic communications services or remote computing services, contains explicit exceptions for voluntary disclosures through consent. The court in *Flagg v. City of Detroit*, 252 F.R.D. 336 (E.D. Mich. 2008), applied these exceptions, and *Flagg* is often cited when parties are seeking court orders requiring third-parties to disclose user-generated electronic data.

What Happens When Laws Conflict?

As discussed in this article, a single breach could result in violations of US federal and state laws, EU law, and the laws of other foreign countries, and conduct that violates the laws of multiple jurisdictions could be penalized under each of these types of laws. What happens then?

A defendant's exposure to the laws of multiple jurisdictions does not itself create a conflict, but a conflict can nevertheless exist where a foreign law mandates (or bars) specific acts in one jurisdiction and compliance with that law is impossible without violating another jurisdiction's laws. To use the French "blocking statute" as an example of how laws may conflict, a United States court may order discovery from a U.S.-based firm with offices in France, and such disclosure, if made, would violate the French blocking statute.FN[FN11]

In such cases, whether one nation's law trumps the other's may turn largely on the practical ability of judicial authorities in the respective countries to enforce their laws. Where a cloud service provider has physical assets in a jurisdiction, that jurisdiction's judicial or administrative authorities will have a much better opportunity to enforce their jurisdiction's laws against the provider. Where a cloud service provider does not have such a physical presence, enforcement will be more difficult; even so, however, where there is a will to enforce local laws, aggressive prosecutors will find a way to assert authority. The possibility of such national conflicts suggests that international agreements on the enforcement of data laws may be inevitable.

FNa1. *Barry Reingold is a partner in the Privacy & Security Law practice of Perkins Coie LLP. Ryan Mrazik and Miriam D'Jaen are associates in the practice, and were the firm's 2009 Perkins Coie Internet Fellows.*

FN1. *See, e.g.*, 15 U.S.C. § 6501(2) (defining COPPA's jurisdiction over any website that operates in an interstate or international manner); 15 U.S.C. § 6801(a) and (b) (identifying financial institutions' obligations to protect the privacy and security of the personal information of their customers); 18 U.S.C. § 1030(e)(2)(B) (defining a "protected computer" as one used in interstate or foreign communications).

FN2. *See, e.g.*, Alaska stat. § 45.48.010 (asserting jurisdiction over any company that stories personal information of an Alaska resident); Ariz. Rev. state. § 44-7501 (asserting jurisdiction over any entity that does business in Arizona); Cal. Civ. Code. § 1798.82 (asserting jurisdiction over any entity doing business in California); Idaho Code § 28-51-104 (asserting jurisdiction over any entity that owns or licenses personal data of an Iowa resident).

FN3. State statutes vary regarding what types of data constitute personal information. Most states include an individual's first name or first initial and last name in combination with any one or more of the following data elements: Social Security number, driver's license or state ID number, or account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. however, some states also define the following as personal information: medical information, health insurance information, laboratory results, passport number, account passwords or personal ID numbers or other access codes, unique biometric data, DNA profile, electronic registration or voter registration number, Individual Taxpayer ID number, Tribal ID card, date of birth, mother's maiden name, employee ID number, and digitized or electronic signature. The terms and penalties also vary widely.

FN4. EU Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of such Data, 1995 O.J. (L 281) 31.

FN5. *Id.* at Chapter IV, Article 25(1).

FN6. The Directive presents a huge challenge for US-based businesses. Therefore, to facilitate EU-to-US data transfers, the US Department of Commerce and the EU Commission developed a voluntary, self-certification "Safe harbor" framework, which is enforced by the US Federal Trade Commission. Entities that self-certify may collect, store, process, and disclose personal data about EU data subject, provided they adhere to the safe harbor principles, which include such elements as notice, choice, access, and enforcement. Alternatively, a non-EY entity can rely upon binding/model contract clauses or binding corporate rules to legally transmit personal data outside of Europe. *Id.* at ch. IV, art. 26.

FN7. The HIPAA privacy rule regulates the use of certain patient information held by covered entities, including health insurers. 45 C.F.R. 164.501 (stating that HIPAA regulations apply to entities that engage in "health care operations," including health insurance companies). State laws, where not "contrary" to HIPAA, are not preempted. 45 C.F.R. § 160.202. This is a basic explanation of HIPAA; the statutory details are much more complex.

FN8. *See e.g.*, Fed. R. Civ. P. 34(a).

FN9. *See* 18 U.S.C. § 2702 (describing situations where a service provider may turn over user records or information; these situations do not include civil litigation where a party or witness has not consented to the disclosure).

FN10. *Id.* at § 2702(b)(3), (c)(2) (authorizing disclosure of customer records and information pursuant to user consent).

FN11. *See, e.g.*, Martinet, Laurent and Akyurek, Ozan, "The Perils of Taking Discovery of France," The Practical Litigator (Sept. 2009) *available at* http:// www.jonesday.com/files/Publication/a52851fa-

6c10-4467-afcb-0894b8ae6e73/Presentation/ PublicationAttachment/206bf819-b8c9-41c8-bbe3-0dd390b8ed0e/TheP ractical0 Litigator -T heP erils0 Of0 Taking DiscoveryT oF rance (LM- ÖA) - s eptem.pdf. The authors discuss the perils of U.S. courts ordering discover from U.S. firms based in France, including the possibility of criminal sanctions under the French blocking statute.

15 No. 1 Cyberspace Law. 1

END OF DOCUMENT