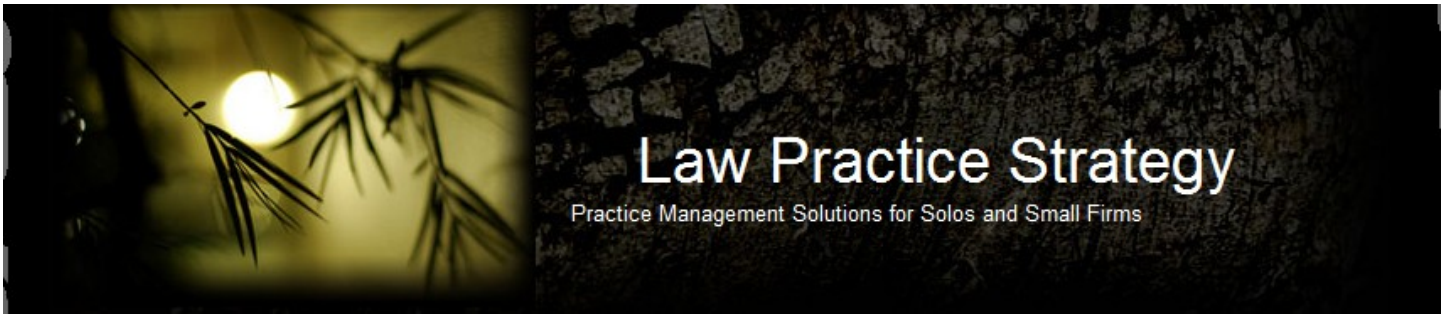

Oh, Data, Where Art Thou? Security, Politics & the Bottom Line

NOTE: This article originally appeared in LJN's Legal Tech Newsletter, an ALM Media publication (www.ljnonline.com/alm?lt)

The ability to convert capital expenditures to operating expenses, tax considerations and other cost-savings benefits are sending businesses to the cloud with glee, the legal profession lagging behind but getting the hint. But as the evolution of security measures becomes more imperative, tales of international disagreement regarding security regulation make the location of your vendor's servers a question of paramount importance in selecting your cloud provider. For lawyers, this question of location is compounded by jurisdictional considerations.

Location, Location, Location

When you place data in the cloud, you lose control of it. How it is handled by the vendors you've entrusted it to depends on two things: their security protocol and the regulations and laws of the physical location of your vendor's servers. For example, Google has servers worldwide, and frequently employs cross-border data transfers. However, the terms of its security policies include a provision whereby the location of your data will not (or cannot) be revealed.

Google's policy is the extreme and not representative of standard cloud vendor policy. But this issue is particularly problematic for legal data, as potential litigants are required to preserve evidence through a legal hold when they know, or should have known, that litigation is pending. Vendors must be able to comply with ediscovery rules and implement them timely for both the main and back-up servers storing the data. A conflict arises because the EU directive's rules on ediscovery are not consistent with those of the US. SOX compliance creates a similar conflict, giving rise to the potential for refusal of a foreign nation to release data required by our laws.

Location is a concern also with respect to the laws and regulations of a specific jurisdiction, as data may become subject to the regulations of the jurisdiction where it is stored. As a policy matter, the EU/UK are big on comprehensive regulation, although there are meaningful differences among EU countries with respect to their national laws and regulations that implement the EU Directive. For example, Germany and France have far more restrictive controls than the UK, so companies may choose data storage location depending on the level of security controls they prefer.

In a blog post entitled Cloud Security: Google won't like the Enterprise View, neither will Facebook, Dennis Howlett reports that overall, European end-users continue to be significantly concerned with security, and the location of their data is a very sensitive issue. They believe it is time to hold cloud vendors to increased responsibilities for security and privacy, and are concerned that low-cost providers are less willing to negotiate their terms of service/vendor agreement. He points to the potential effect of storing data in the US due to the Patriot Act's broad government oversight as another over-riding concern.

Danny Johnson, Marketing Analyst for NetDocuments, agrees: "UK firms are definitely more concerned when it comes to data stored in the US due to the Patriot Act." Moreover, the US has no comprehensive regulation with respect to data privacy and security, and takes an as-needed approach to regulate various industries within the business community. Europeans feel it is not uncommon for US commentators to profess that there really is no privacy anyway, and that European attitudes hold back progress and interfere with the flow of business. Ben Schorr, CEO at Roland, Schorr & Tower, puts it this way:

"US companies are allowed to do things they'd never get away with in the EU. . .

The US pays lip service to privacy, but actual enforcement is weak or non-existent at the government level. And at the corporate level, privacy concerns tend to go out the window if there is a savings in the operational budget to be had. More often than not profits trump privacy."

Security Regulatory Schemes

The EU has comprehensive security regulation called the EU Data Protection Directive. Each member state implements the Directive via its own regulation, creating yet another layer of variation among nations. Most notably, one of the critical terms of the Directive is that it prohibits the transfer of personal information from the EU to any country that does not provide adequate levels of data protection, which includes the US.

In contrast, the US has approached security regulation and standards from a piecemeal perspective, instituting regulation as specific concerns arise. Existing regulations include:

- The Sarbanes-Oxley Act – requires public companies to comply with email retention, data security and oversight requirements
- Payment Card Industry Data Security Standard (PCI-DSS) – requires enhancement of payment account data security
- Health Insurance Portability and Accountability Act (HIPAA) – regulates use and disclosure of health information
- Federal Information Security Management Act (FISMA) – requires federal agencies to develop and implement information security programs related to their own operations
- COPPA – regulates online data collection of children under 13
- The Gramm-Leach-Bliley Act – regulates disclosure of non-public information by financial institutions

Individual US states have also instituted regulations and standards that must be considered in choosing data location. In a recent webinar presented by Sandra Jaskie and Jonathan Armstrong of Duane Morris, LLP, the presenters noted that Massachusetts and Nebraska passed legislation requiring encryption of personal information and imposing responsibilities on vendors related to notice of data breach. Massachusetts also requires development of a security and privacy plan for all personal data that is either in storage or transmission on any (read mobile) device, and imposes stiff penalties for non-compliance.

In an attempt to bridge these different privacy approaches and provide a streamlined means for U.S. organizations to comply with the Directive, the U.S. Department of Commerce and the European Commission developed a "Safe Harbor" certification process. The process enables individual US vendors to self-certify compliance with the EU directive, thereby eliminating the data transfer restriction. There is also a US-Swiss Safe Harbor framework, since Switzerland is non-member state.

For US vendors whose servers reside in the US and who do not target European markets, Safe Harbor certification is not a goal. But for document storage vendors whose systems also provide for online collaboration, certification is necessary due to the high rate of international collaboration among businesses and law firms.

InfosecIsland.com's blog entitled "Cloud Computing Data Protection World Map" includes a link to a great visual, coded to show worldwide security protection levels.

The Future of International Security Regulation

The economic viability of conducting business, including the business of law, online is the significant driver in this scenario. If the continued economic instability of global financial markets has taught us anything, it is that cost-efficiency will be of enduring prominence. Because cost-efficiency is the trademark of cloud computing and virtualization, there is no doubt that international cooperation will improve. In fact, it is already moving in that direction.

Duane Morris recently reported that:

- The UK's Information Commissioner's Office (ICO) issued its new Code of Practice on handling personal information online.
- A new EU directive is likely within the next two years.
- There are moves at harmonization, both within Europe and with the US, with EU data-privacy regulators holding a meeting with the FTC.

Project Counsel discussed several sources of potential for global security regulation:

- the European Commission and the US have opened negotiations on the creation of a data protection agreement to govern data transfers between the EU and the US
- In Washington, Viviane Reding, Commissioner for Justice, Fundamental Rights and Citizenship, made clear her agenda to begin negotiations with the US on an umbrella data protection agreement
- The European Parliament gave approval to the latest framework within which US authorities can gain access to Europeans' banking details to aid counter-terrorism intelligence

Due Diligence Questions to Ask Potential Vendors

Traditionally, developers and vendors have tried to put security obligations on the shoulder of end-users. But it is now time to put them to the test of security compliance and transparency.

Here is a list of concerns that should be addressed via a written vendor questionnaire:

- Where are the servers located? If more than 1 location, which server will store your data?
- Where are the servers that will back-up your data?
- What are the jurisdiction's regulatory requirements?

- Do they engage in cross-border data transfers? If so, when and where? Will you be notified? Is there a compliance plan for cross-border transfers?
- Do they employ Tier 4, 256-bit encryption, bank-level security?
- Are these security measures in place both while the data is in transition and in storage?
- Have their operations ever been audited (if so, obtain a copy of the report)
- Do they own their servers, or lease them from a third party?
- If they do not own them, what are the terms of the third-party agreement (obtain a copy)
- Will your data be stored on a dedicated server, or on a multi-tenancy server (i.e., with others' data)
- If multi-tenant, how is your data separated from others?
- How is the server building physically secured?
- Who has access to the stored data?
- What kind of training is provided their employees?

- Have they ever had a security breach?
- What is their customer notification policy upon breach?
- What is their response policy upon breach?
- What is their disaster recovery/business continuity plan?
- Are they Safe-Harbor certified?

Create a template questionnaire that will give you a clear basis for evaluation of their policies and services. Your vendor contract and Service Level Agreement must contain the terms that have been agreed to once your due diligence has been completed. The best way to insure this is to attach a copy of the completed vendor questionnaire to your final contract.

There is definitely a learning curve associated with the virtual practice of law. It is an additional area of law practice on which you must stay current, and CLE courses on this topic are emerging quickly. If this seems onerous, think of it this way: the corporate world is doing business in the cloud. Consumers are conducting business online. All of this is occurring in ever-increasing numbers, the cost-effectiveness is staggering and tech-savvy consumers are in control. In other words, the horse is out of the barn.

If you and your firm are going to stay competitive, there is nowhere else to turn. You can try to hold out until retirement in your brick-and-mortar practice, hoping for the best. Or you can embrace your future in the cloud, certain that your practice will thrive as digital natives become the generation in need of your services.