

SIDLEY AUSTIN LLP

SIDLEY

BEIJING BRUSSELS CHICAGO DALLAS FRANKFURT GENEVA HONG KONG LONDON LOS ANGELES NEW YORK PALO ALTO SAN FRANCISCO SHANGHAI SINGAPORE SYDNEY TOKYO WASHINGTON, D.C.



Government Dimensions of Cloud Computing

Alan Charles Raul
March 12, 2010

Federal Communications Commission (FCC)

- “Is the FCC positioning itself to become the Federal Cloud Commission?” - Adam Thierer, PFF
- FCC solicited comments on cloud regulation for National Broadband Plan – portability of data, transparency & privacy
- FTC and others commented the FCC should examine cloud privacy
- FCC will release the plan on March 17

Federal Trade Commission (FTC)

- FTC is investigating privacy and security implications of cloud computing
 - 2009 FTC filing with the FCC states:
“The ability of cloud computing services to collect and centrally store increasing amounts of consumer data, combined with the ease with which such centrally stored data may be shared with others, create a risk that larger amounts of data may be used by entities not originally intended or understood by consumers”
 - FTC indicated to the FCC that it was pursuing an investigation on cloud computing services
- “Storage of data on remote computers may raise privacy and security concerns for consumers.”
 - David Vladeck, FTC's Consumer Protection Bureau

FTC Privacy Roundtables

- January 2010 privacy roundtable focused on evolving technologies, including cloud computing
- EPIC comments
 - User's privacy and confidentiality risks vary significantly with the terms of service and privacy policy established by cloud provider
 - Questions user's ability to:
 - assess the provider's security
 - audit security for compliance
 - determine whether level of security meets statutory/regulatory requirements
 - Transfer of information to cloud may facilitate government access without notice

Complaint to FTC Re: Google's Cloud Computing

- FTC considering EPIC petition regarding Google's provision of cloud computing services
 - March 2009 EPIC complaint asserts privacy and security risks
 - Complaint cited breaches:
 - Google disclosed user-generated documents saved on its Google Docs Cloud Computing Service to unauthorized users
 - Security flaws in Google's Gmail service allowed theft of usernames and passwords for the 'Google Accounts' centralized log-in service
 - EPIC alleged:
 - Google misrepresented the security of users' information
 - Google's inadequate security is an unfair and deceptive business practice

Personal Health Information

- HIPAA/HITECH
 - HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other personal health information
 - HITECH “breach notification” regulations require health care providers and other HIPAA covered entities to promptly notify affected individuals (and possibly the HHS Secretary and the media) of a breach
 - HITECH now applies certain HIPAA and HITECH security and privacy requirements to business associates (BA)
- Covered Entities must enter BA agreement with cloud provider to store records containing PHI
 - HIPAA/HITECH security and breach notifications obligations apply in cloud

BA Agreements for Cloud Providers

- HIPAA's requirements could conflict with cloud provider's standard terms of service
- Customized BA agreements may be necessary or appropriate
- HIPAA prohibits entities from transmitting PHI over open networks or downloading it to public or remote computers without encryption

HIPAA Security Rule

- Security Rule requires covered entities to establish detailed administrative, physical and technical safeguards to protect electronic PHI
 - Implement access controls
 - Encrypt data
 - Set up audit controls for electronic PHI
 - For example, detailed activity logs to see who had access, what data was accessed, what IP addresses entered the site
 - Data back-up procedures
 - Must maintain exact copies of electronic PHI
 - Disaster recovery mechanisms
 - For example, Amazon's EC2 offers Availability Zones, which are distinct locations engineered to be insulated from failure in other zones

HITECH: FTC Breach Notification for PHR Vendors

- “PHR” is electronic record of identifiable health information on an individual drawn from multiple sources and managed, shared, and controlled by or primarily for the individual
- “Vendors of personal health records and PHR related entities shall notify third party service providers of their status as vendors of personal health records or PHR related entities...”
 - Will be necessary to notify cloud computing service providers that vendor’s data includes PHRs
- PHR vendors must notify the FTC and each affected individual of a breach of their identifiable health information
- FTC presumes that unauthorized "acquisition" occurs upon unauthorized access to unsecured PHRs, subject to rebuttal proof that there was not, or could not reasonably have been, any unauthorized acquisition

Federal Government Use of Cloud Computing

- Unique data privacy and security issues raised by federal government's increasingly widespread use of cloud computing
 - Will government's cloud providers assume quasi-law enforcement roles?
 - Will GSA vendors have immunity for privacy or security breaches?
 - Will vendors have to process and store U.S. government data only in the U.S. to enhance security and avoid potential conflicts with foreign or international law?

Federal Information Security Management Act

- Federal Information Security Management Act of 2002 (FISMA)
 - Requires each federal agency to develop, document, and implement agency-wide program to provide information security
- Cloud providers Microsoft and Google are seeking FISMA compliance accreditation from the National Institute of Standards and Technology (NIST)

Office of Management and Budget (OMB)

- OMB and the CIO council are working on policies to make cloud computing easier for agencies
 - Centralizing security certifications so vendors don't have to repeat lengthy and costly security checks
- WH CIO Vivek Kundra (Sept. 15, 2009):
 - “Apps.gov is an online storefront for federal agencies to quickly browse and purchase cloud-based IT services, for productivity, collaboration, and efficiency. Cloud computing is the next generation of IT in which data and applications will be housed centrally and accessible anywhere and anytime by a various devices (this is opposed to the current model where applications and most data is housed on individual devices). By consolidating available services, Apps.gov is a one-stop source for cloud services – an innovation that not only can change how IT operates, but also save taxpayer dollars in the process.”

Financial Institutions

- Requires due diligence and contractual control over cloud provider
- Assure safeguards maintain compliance with
 - Gramm-Leach-Bliley Act
 - Fair Credit Reporting Act (FCRA)
 - State Information Security Laws

State Information Security Laws

- Massachusetts issued regulations (effective March 1, 2010) requiring any person who holds personal information about Massachusetts residents to develop and implement a comprehensive written information security program to protect the data
- Other state laws (and EU, of course) mandate affirmative data security requirements and controls over service providers

Cloud Computing and the Fourth Amendment

- Relationship of cloud to 4th Amendment expectation of privacy?
 - *Smith v. Maryland*, 442 U.S. 735 (1979) (no privacy expectation for records of phone numbers dialed)
 - *US v. Miller*, 425 U.S. 435 (1976) (no privacy expectation for bank records including checks/deposit slips)
 - *Warshak* panel opinion (reversed en banc) questioned reasonableness of assuming lost expectation of privacy for data turned over to service providers
- Or is cloud computing a modern version of a safe deposit box, storage locker or personal computer hard drive?
 - If so, cloud users could argue their data is subject to Fourth Amendment and protected against warrantless searches

Warshak en Banc on Privacy Policies

- “. . . variety of internet-service agreements and the differing expectations of privacy that come with them. An agreement might say that a service provider will “not . . . read or disclose subscribers’ e-mail to anyone except authorized users.” . . . might say that a service provider “will not intentionally monitor or disclose any private email message” but that it “reserve[s] the right” to do so in some cases. . . . might say that a service provider “may or may not pre-screen Content, but . . . shall have the right (but not the obligation) in [its] sole discretion to pre-screen, refuse or move any Content that is available via the Service”—as indeed Warshak’s Yahoo! account did. . . . might say that e-mails will be provided to the government on request—as indeed the same Yahoo! account did. . . . might say that other individuals, besides the recipient of the e-mail, will have access to it and will be entitled to use the information in it. . . . might say that the user has no expectation of privacy in any of her communications.”

Electronic Communications Privacy Act (“ECPA”)

- Remote Computing Service (RCS) is “provision to the public of computer storage or processing services by means of an electronic communication system”
- Electronic Communication Service (ECS) is “any service which provides users the ability to send or receive wire or electronic communications”
 - Access to ECS generally requires warrant (unless stored at a provider for >180 days, in which case treated as RCS)
 - Easier access to RCS: subpoena with notice to user or a court order
- Cloud providers may also be able to voluntarily turn over content:
 - **Rights or Property of Carrier.** As necessarily incident to the rendition of the service or protection of the provider’s rights/property
 - **Exigent Circumstance.** If provider believes in good faith that emergency involving danger of death or serious physical injury requires disclosure without delay
 - **Child Pornography.** To the quasi-governmental National Center for Missing and Exploited Children

PATRIOT ACT AND NSLs

- NSL: letter request for information held by third party issued in connection with authorized counterterrorism or counter-intelligence investigation (no notice)
 - NSLs allow access to records from internet service providers, phone companies, banks, credit card companies and other financial entities
- Section 215 of PATRIOT Act: authorizes access to business records relevant to counter-intelligence or counter-terrorism with FISA court order (no notice)

Cloud Data In Civil Litigation

- In U.S. civil litigation, a party may be required to produce all relevant, non-privileged data in its “possession, custody or control.” [FRCP 34\(a\)](#).
 - Includes data stored with cloud provider to which party/witness has contractual or common law right of access
 - Discovery request directed to party could apply to cloud data, regardless of where cloud provider's servers are located

Microsoft Cloud Computing Initiative

- Microsoft's "Cloud Computing Advancement Act":
 - Modernize ECPA to make clear that Fourth Amendment protections apply to the cloud
 - Boost CFAA penalties and jurisdiction
 - Reconcile conflict of law issues by seeking a multilateral framework by treaty or similar international instrument

The Cloud and Cybersecurity

- Cyber-attacks against Google were a "wake-up call" about the vulnerabilities that could cripple the US economy (Dennis Blair, U.S. Director of National Intelligence)
- White House Cybersecurity Coordinator Howard Schmidt:
 - “Cloud computing makes a lot of sense, but we need to make sure that the policies...the legal framework is in place”
 - “The spotlight will shift to authentication, encryption, service level agreements and legal requirements”
 - Schmidt has been working on requirements for secure cloud computing architectures

Contact Information

Alan Charles Raul

Sidley Austin LLP

1501 K Street, NW

Washington, DC 20005

araul@sidley.com

(202) 736-8477

www.sidley.com/cyberlaw

Sidley Austin LLP, a Delaware limited liability partnership, operates in affiliation with other partnerships, including Sidley Austin LLP, an Illinois limited liability partnership, Sidley Austin (UK) LLP, a Delaware limited liability partnership (through which the London office operates), and Sidley Austin, a New York general partnership (through which the Hong Kong office operates). The affiliated partnerships are referred to herein collectively as Sidley Austin, Sidley or the firm.

This presentation has been prepared by Sidley Austin LLP as of September 11, 2007, for informational purposes only and does not constitute legal advice. This information is not intended to create, and receipt of it does not constitute, a lawyer-client relationship. Readers should not act upon this without seeking advice from professional advisers.