5-1-2011

Cloud Computing - Legal Issues in the U.S. & International Implication

Maki DePalo
Georgia State University College of Law

Georgia State University | COLLEGE OF LAW

Research Guides

Cloud Computing - Legal Issues in the U.S. & International Implication

Guide Information

Last Updated: Jan 24, 2012
Guide URL: http://libguides.law.gsu.edu/cloudcomputing
RSS: Subscribe to Updates via RSS

Guide Index

Home

Scope

Cloud Computing - Growing Trend

Gartner, the world's leading information technology research and advisory company, predicts "the [cloud services] industry is poised for strong growth through 2014, when worldwide cloud services revenue is projected to reach $148.8 billion." Cloud Computing extends the concept of utility computing and is often characterized by its value propositions such as "on-demand self-service" and "broad network access." As Cloud Computing becomes a new business model, not just a new technology, it brings a new legal challenge as well as accentuating the need of due diligence regarding traditional legal issues associated with technology and outsourcing.

There are legal issues and risks both for Cloud Service Providers and for Cloud Service Users. This research guide places primary focus on the Cloud Service Business Users. Further, this research guide is only a starting point for a law student or an attorney to research legal issues. The guide also expands on issues with privacy protection and trans-border data transfer.

Overview

Cloud Computing Defined

National Institute of Standards and Technology (NIST) issued the Definition of Cloud Computing marked as V15 on October, 2009. NIST defines Cloud Computing as "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

NIST further dissects Cloud Computing from three different perspectives: essential characteristics, service models, and deployment models.

Essential Characteristics

- On-Demand Self-Service
- Broad Network Access
- Resource Pooling
- Rapid Elasticity
- Measured Service

Service Models

- Cloud Software as a Service (SaaS)
- Cloud Platform as a Service (Paas)
- Cloud Infrastructure as a Service (IaaS)

Deployment Models

- Private Cloud
- Community Cloud
- Public Cloud
- Hybrid Cloud

These classifications are important because different legal challenges may arise depending on the specific type of Cloud Computing services. For example, a large business entity that procures service under the Private Cloud model may find the legal issues similar to traditional IT outsourcing engagements. On the other hand, small and medium size businesses (SMB) may find the Private Cloud model not attractive as their volume of business may not warrant the cost associated with the use of Private Cloud.

However, the use of Public Cloud may present a series of legal issues to SMB because most cloud service providers offer the services only in general terms with few meaningful commitments on a "take it or leave it" fashion. Further, when risk factors such as business disruption and regulatory noncompliance are considered, a business case may become unsustainable if it is merely focused on cost savings.

In fact, James Staten, analyst of Forrester Research, predicts the trend in 2011 which includes failed attempts to effectively use the Private Cloud model and growth of the Community Cloud driven by security and compliance.

Legal Risks and Issues associated with Cloud Computing

Connecticut Law Tribune published an article "Cloud Computing: Why Forecast Should Matter To You" in October, 2010. The articles, such as the above, summarize some critical issues associated with Cloud Computing.

- Jurisdictional Issues
- Data Security
- Privacy & Data Protection Laws
- Contract of Adhesion
- Costs and Pricing Model
- Maintenance and Support
- Availability and Reliability
- Disaster Recovery
- Exit Strategy
- Intellectual Property, Licensing

In February, 2011, Connecticut Law Tribune also published an article "E-Discovery: Cloud Computing Complicates E-Discovery Issues" to expand on how Cloud Computing brings up significant challenges as to how and where Electronically Stored Information (ESI) resides.

- Electronically Stored Information (ESI)
- E-Discovery

Further, lawyers must understand the ethical obligations when practicing in the Cloud world considering the ABA's opinion.

- Ethical Obligation

Outline of this Library Guide

Primary Sources tab

- U.S. Constitution
- U.S. Codes that may govern the use of Cloud Computing services
- Administrative laws
- State-law implication
- U.S. Case laws that dealt with the Cloud Computing related issues

Secondary Sources tab

- U.S. Resources
  - The secondary sources that discuss applicable U.S. legal issues
  - Blogs and other resources
- International Resources
  - The secondary sources that discuss International legal issues with focus on privacy and data protection laws
  - Information about relevant International organizations

News and Media tab

- Reference legal news articles
- Reference business & technology news articles
- RSS Feeds

About the Author

Maki DePalo is a second year student at Georgia State University College of Law. She is expected to graduate in May, 2012.

Disclaimer

Please note this guide should not be considered as legal advice or as a legal opinion on any specific facts or circumstances. If you need further assistance in researching this topic or have specific legal questions, please contact a reference librarian in the Georgia State University College of Law library or consult an attorney.

Back to Top

Primary Sources

U.S. Constitution

The Fourth Amendment of the United States Constitution provides:

> "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."
>
> - U.S. CONST. AMEND. IV.

U.S. Codes

Acts with General Scope

The U.S. Codes that set forth general standards over personal information.

- The Privacy Act of 1974
  - 5 U.S.C. § 552a.
  - The Privacy Act provides for records maintained on individuals and imposes conditions on disclosure.

- The Electronic Communications Privacy Act of 1986 (ECPA)
  - 18 U.S.C. §§ 2510-2522, 2701-2712.
  - The ECPA sets out the provisions for access, use, disclosure, interception and privacy protections of electronic communications. The law was enacted in 1986 and covers various wire and electronic communications. However, with emerging technologies in data storage available in Cloud Computing, it is not clear whether or not the ECPA applies to certain circumstances.

- The Stored Communications Act of 1986 (SCA)
  - 18 U.S.C. §§ 2701-2712.
  - The SCA, Title II of the ECPA, sets forth a system of statutory privacy rights for customers and subscribers of computer network service providers. Under the SCA, two (2) types of providers are regulated: Electronic Communication Services (ECA) and Remote Computing Services (RCS). Similar to the ECPA, the applicability of the SCA in certain circumstances is not always clear.

Acts with More Specific Scope

Specific statutes that may impose unique restrictions on personal information include, but are not limited to, the following:

- The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
  - Pub.L.104-191
  - Under the authority of the HIPAA, the HIPAA privacy rule provides a comprehensive scheme to regulate the use and disclosure of personally identifiable health information. The regulations require covered entities to enter into a business associate agreement before the covered entity may transfer the protected health information to a third party service provider.

- The Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH)
  - Pub.L. 111–5
  - The HITECH Act is part of the American Recovery and Reinvestment Act of 2009. The HITECH Act encourages healthcare providers to adopt electronic medical records while protecting the privacy of health information and promoting security in a qualified electronic health record. The Act is designed to "assist health care providers to adopt, implement, and effectively use certified EHR [electronic health records] technology that allows for the electronic exchange and use of health information."

- The Fair Credit Reporting Act of 1970 (FCRA)
  - 15 U.S.C. § 1681b.
  - The FCRA imposes the restriction on the use of credit reports by limiting the use only to permissible purposes expressed in the provision.

- The Gramm-Leach-Bliley Act of 1999 (GLBA)
  - 15 U.S.C. § 6802.
  - The Act is also known as the Financial Services Modernization Act of 1999. The GLBA imposes the Privacy and Safeguards Rules to restrict financial institutions from disclosing consumer's non-public personal information to non-affiliated third parties.

- The Federal Information Security Management Act of 2002 (FISMA)
  - Pub.L. 107–347
  - The FISMA purports to provide a comprehensive framework for ensuring the effectiveness of information security, recognize the highly networked nature of the current Federal computing environment and provide effective government wide management and oversight of the related information security risks, provide for development and maintenance of minimum controls required to protect Federal information and information systems, provide a mechanism for improved oversight of Federal agency information security programs, acknowledge that commercially developed information security products offer advanced, dynamic, robust, and effective information security solutions, reflecting market solutions for the protection of critical information infrastructures important to the national defense and economic security of the nation that are designed, built, and operated by the private sector, and recognize that the selection of specific technical hardware and software information security solutions should be left to individual agencies from among commercially developed products.

- The Cable Communications Policy Act of 1984
  - 47 U.S.C. § 551.
  - The Act imposes protection for subscribers by requiring notice, restricting collection and disclosure of personally identifiable information, and requiring destruction of such information.

- The Video Privacy Protection Act of 1988 (VPPA)

- 18 U.S.C. § 2710.
- The Act prohibits wrongful disclosure of video tape rental or sale record and imposes liability for knowing disclosure of personally identifiable information.

Case Law

Personal Jurisdiction

Forward Foods LLC v. Next Proteins, Inc., 873 N.Y.S.2d 511 (N.Y. Sup. 2008).

A virtual data room set up in New York to conduct electronic document review along with meetings, email, and phone calls provided a basis to show sufficient contacts with New York to grant personal jurisdiction in New York when the subject matter of the meetings and documents was consistent with the litigated issue.

Fischbarg v. Doucet, 880 N.E.2d 22 (N.Y. Sup. 2007).

The court found the exercise of personal jurisdiction over residents of California was proper when these defendants retained a New York attorney to represent the corporation in an action brought in Oregon because defendants' retention and subsequent communications through telephone, mail, e-mail and facsimile with plaintiff in New York established a continuing attorney-client relationship in New York and thereby constitute the transaction of business.

Privacy

State v. Bellar, 217 P.3d 1094 (Or. App. 2009), review denied, 231 P.3d 795 (Or. 2010).

Although this case does not involve cloud computing directly, the dissent noted that people have an expectation of privacy for data stored in the cloud and expressed: "Nor are a person's privacy rights in electronically stored personal information lost because that data is retained in a medium owned by another. Again, in a practical sense, our social norms are evolving away from the storage of personal data on computer hard drives to retention of that information in the “cloud,” on servers owned by Internet service providers... I suspect that most citizens would regard that data as no less confidential or private because it was stored on a server owned by someone else.”

Theofel v. Farey-Jones, 359 F.3d 1066 (9th Cir. 2004).

The Ninth Circuit elaborated on the Storage Communications Act (SCA) and what "backup protection" means. The Court held that the Defendant violated the SCA when it offered a "free sample" of 399 messages stored "for the purpose of backup protection" under 18 U.S.C. Section 2510(17)(B). The Court further found that disclosure of email messages by the plaintiff's ISP pursuant to the defendant's overly broad subpoena did not constitute an “authorized” disclosure under the Stored Communications Act.

Jennings v. Jennings, 697 S.E.2d 671 (S.C. Ct. App. 2010), reh'g denied (Aug. 27, 2010).

Husband brought action against wife, wife's daughter-in-law, and private investigator hired by wife for violations of Stored Communications Act (SCA) stemming from accessing of husband's e-mails to his girlfriend by wife's daughter-in-law. The Court agreed with the Ninth Circuit and found e-mails were stored by “electronic communication service” (ECS) and “for purposes of backup protection,” within meaning of SCA.

Immunomedics, Inc. v. Doe, 775 A.2d 773 (N.J. App. Div. 2001).

Biopharmaceutical corporation brought action against unidentified user of Internet service provider's (ISP's) message board and served subpoena on the ISP in order to discover user's true identity. The Court held that corporation's right to disclosure of user's identity outweighed user's First Amendment right of anonymous free speech.

Dendrite Intern., Inc. v. Doe, 775 A.2d 756 (N.J. App. Div. 2001).

Corporation brought defamation action against unidentified defendants for posting a message on an Internet service provider's (ISP) bulletin board. The Court denied the Corporation's discovery request to compel the ISP to disclose the defendants' identities because the the corporation failed to make a requisite showing of harm from the statement.

E-Discovery

Flagg v. City of Detroit, 252 F.R.D. 346 (E.D. Mich. 2008).

Discovery of text messages stored with the third-party service provider was compelled. The Court reasoned that Stored Communications Act (SCA) did not preclude civil discovery of city's relevant, nonprivileged electronically stored communications that were maintained by a non-party service provider but remained within the city's control.

Columbia Pictures, Inc. v. Bunnell, 245 F.R.D. 443 (C.D. Cal. 2007).

Discovery of the data was compelled when the defendant had the "ability to manipulate at will" how the data was routed because the defendant rerouted the data from its servers to the third party's servers just one month prior to the hearing. The court denied defendants, who sought the protection of Dutch law, to avoid preserving and producing relevant server log information while allegedly facilitating the worldwide downloading of copyrighted movies and music.

Tomlinson v. El Paso Corporation, 245 F.R.D. 474 (D. Colo. 2007).

Discovery of certain electronic documents such as the pension plan and ERISA records was compelled because the employer was in control of digital data held by a third party record-keeper.

Intellectual Property, Copyright

Arista Records, LLC v. Usenet.com, Inc., 633 F. Supp. 2d 124 (S.D.N.Y. 2009).

In the copyright infringement action, the Usenet.com was not allowed to assert an affirmative defense under the Digital Millennium Copyright Act’s (“DMCA”) safe harbor provision when there was “strong evidence of extreme wrongdoing" such as withholding evidential emails and destroying seven hard drives that

held employee-generated data.

Contributory Liability on Cloud Computing Service Providers

Tiffany (NJ) Inc. v. eBay, Inc., 600 F.3d 93 (2d Cir. 2010).

Tiffany, Jewelry seller, brought action against eBay, online auction site proprietor through which counterfeit seller-branded merchandise was sold, alleging trademark infringement, false advertising, or trademark dilution. The Court, although Tiffany asserted that it had brought the infringement to eBay's attention and eBay knew that users were selling counterfeit items, held that eBay's generalized knowledge of infringement was not sufficient to show eBay's knowledge as to specific incidents of infringement with respect to the infringement and dilution claims.

Louis Vuitton Malletier, S.A. v. Akanoc Solutions, Inc., 2009 WL 3062893 (N.D. Cal. Aug. 28, 2009) (verdict).

Vuitton, exclusive distributor of luxury merchandise, filed action against Internet service providers, all

State Laws

Preemption

Laws such as HIPAA include a provision for preemption. For example, HIPAA provides "[a] regulation ... shall not supersede a contrary provision of State law, if the provision of State law imposes requirements ... that are more stringent than the requirements ... imposed under the regulation." It is imperative to understand the state-level laws to which the data might be subject in addition to the Federal laws.

Journal of Legal Technology Risk Management published "Cloudburst: What does Cloud Computing Mean to Lawyers?" in Fall 2010. The article draws lawyer's attention also to the state laws:

State Information Security Laws

Arkansas, California, Connecticut, Maryland, Nevada, Oregon, Rhode Island, Texas, and Utah, for example, provide state-level information security laws to which the data might be subject.

State Breach Notification Laws

State-level breach notification requirements have been enacted in forty-five states.

Helpful Links on HIPAA

Understanding Health Information Privacy

- Summary of HIPAA Privacy Rule
  http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html
- Summary of HIPPA Security Rule
  http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html

Legislative History

The Stored Communication Act

The SCA's legislative history provides that “electronic mail companies are providers of electronic communication services.” - S. REP. NO. 99-541, at 14 (1986); H.R. REP. NO. 99-647, at 63 (1986).

“[T]o the extent that a remote computing service is provided through an Electric Communication Service, then such service is also protected [under section 2701].” - H.R.Rep. No. 99-647, at 63 (1986).

Email messages stored by an Remote Computing Services (RCS) should “continue to be covered by section 2702(a)(2)” if left on the server after they were accessed by the user. - H.R. Rep. No. 99-647, at 65 (1986).

See Jennings v. Jennings, 697 S.E.2d 671 (S.C. Ct. App. 2010) for more detail.

Administrative Laws

The Federal Health Privacy Rule - 45 C.F.R. Part 164, 164.502(e), 164.504(e).

The rules are issued under the authority of the Health Insurance Portability and Accountability Act (HIPAA).

Disclosure of Tax returns - Disclosure or use permitted only with the taxpayer's consent. - 26 C.F.R. § 301.7216-3, Treas. Reg. § 301.7216-3.

Unless § 7216 or § 301.7216-2 specifically authorizes the disclosure or use of tax return information, a tax return preparer may not disclose or use a taxpayer's tax return information prior to obtaining a written consent from the taxpayer.

Back to Top

Secondary Sources

Information under Secondary Sources

Secondary Sources tab contains two (2) sub-tabs:

- U.S. Resources
  - The secondary sources that discuss applicable U.S. legal issues
  - Blogs and other resources
- International Resources
  - The secondary sources that discuss International legal issues with focus on privacy and data protection laws
  - Information about relevant International organizations

Back to Top

The U.S. Resources

Law Reviews and Articles

Cloud Computing & International Privacy Laws

- Mark H. Wittow, Daniel J. Buller, *Cloud Computing: Emerging Legal Issues for Access to Data, Anywhere, Anytime*, 14 J. Internet L. 1 (2010).
  - This paper identifies emerging legal issues as well as exploring new types of claims anticipated in the coming years as a result of various types of security breaches and the increasing use of cloud services for a variety of tasks.
- Timothy D. Martin, *Hey! You! Get Off of My Cloud: Defining and Protecting the Metes and Bounds of Privacy, Security, and Property in Cloud Computing*, 92 J. Pat. & Trademark Off. Soc'y 283 (2010).
  - This paper explores barriers to confidence in Cloud Computing and proposes that solid data ownership boundaries, clear guidelines for law enforcement, clearer penalties for computer crimes, and greater cooperation and standardization among cloud providers to remove barriers to wider adoption of cloud computing.
- Robert S. Friedman and Mark E. McGrath, *Virtual Contacts and Personal Jurisdiction*, N.Y.L.J. S4, (col. 1) (2009).
  - This article discusses personal jurisdiction issues involving electronic contacts such as Web sites, e-mails and instant messages (collectively, e-contacts) and analyzes how courts are handling jurisdictional questions attendant to the next generation of technology, such as forms of "cloud computing," including virtual data rooms and social networks.
- Robert Gellman, World Privacy Forum, *Privacy in the Clouds* (Feb. 23, 2009).
  - This report discusses the issue of cloud computing and outlines its implications for the privacy of personal information as well as its implications for the confidentiality of business and governmental information.

- Miriam Wugmeister, Karin Retzer, & Cynthia Rich, *Global Solution for Cross-Border Data Transfers: Making the Case for Corporate Privacy Rules*. 38 Geo. J. Int'l L. 449 (2006-2007).
    - This paper points out weaknesses of existing approaches to cross-border data transfers and advocates that, by enabling companies to implement consistent privacy policies and practices on a global basis, individuals will be afforded more meaningful privacy protections rather than enforcing the overly complex maze of regulation.
- Joel R. Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace*. 52 Stan. L. Rev. 1315 (2000).
    - This article explores the divergences in approach and substance of data privacy between Europe and the United States. Because the specific privacy rules adopted in a country have a governance function, the article explains how structural divergences make international cooperation imperative for effective data protection in cyberspace.
- Barbara C. George & Deborah R. Gaut, *Offshore Outsourcing to India by U.S. and E.U. Companies: Legal and Cross-Cultural Issues that Affect Data Privacy Regulation in Business Process Outsourcing*. 6 U.C. Davis Bus. L.J. 13 (2006).
    - The article discusses that, since the trend of business process outsourcing is to increase trans-border data flows, it is incumbent upon legislators, regulators, non-governmental organizations, privacy advocates, and U.S. companies to ensure that the Business Process Outsourcing relationship with India is established so all of the safeguards for data privacy are established.
- Frances Ma, Copland v. United Kingdom*: What is Privacy & How Can Transnational Corporations Account for Differing Interpretations?*, 31 Loy. L.A. Int'l & Comp. L. Rev. 291 (2008).
    - Because the privacy perspectives are markedly different between the U.S. and Europe, differences require private entities to create separate business policies and procedures for its employees depending on where they are located. This paper explores how a transnational business must weigh its production and performance interests against its human rights obligations when many questions are left open after the decision in Copland.
- Jennifer McClennan & Vadim Schick, *"O, Privacy": Canada's Importance in the Development of the International Data Privacy Regime*, 38 Geo. J. Int'l L. 669 (2007).
    - This paper provides a survey of data protection legislation in the U.S., Europe, and Canada, examines the current state of the data privacy law in Canada, and suggests a few necessary steps for the U.S. companies doing business in Canada to take in order to ensure compliance with the Canadian data privacy law.
- William Jeremy Robison, *Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act*, 98 Geo. L.J. 1195 (2010).
    - This note concludes that the current advertising supported business model used by many cloud computing providers will not qualify for the privacy protection under the Stored Communications Act (SCA). The note also explores whether the lack of privacy protections for cloud computing is consistent with the legislative intent in adopting the SCA. It further argues the modern form of cloud computing is incompatible with the Fourth Amendment and what motivated the legislature to enact the SCA.
- Christopher Soghoian, *Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era*, 8 J. Telecomm. & High Tech. L. 359 (2010).
    - This paper discusses that the increased risk, that users face from hackers, is primarily a result of cost-motivated design decisions on the part of the cloud providers, who have repeatedly opted to forgo strong security solutions already used in other Internet based industries.

Books

Cloud Computing, Privacy & Data Protection

- Cloud Computing: a Practical Introduction to the Legal Issue by Renzo Marchini
  ISBN: 0580703223This book will introduce cloud computing (briefly) for those new to the concept, comparing the development of this new computing paradigm to other ways of buying computing resource. It will summarize the legal issues which arise, some of which are unique to cloud, others of which are more general but have a unique application to cloud. It will explore these legal issues, covering such areas as security in the cloud, data protection, service levels, and contractual issues. It will provide a practical resource

for those involved in buying or providing cloud services, setting out practical steps to address legal issues both in the regulatory context and in the context of contracts between customer and suppliers. It also deals with issues which arise when the cloud service is used by regulated sectors, such as financial services. - Product Description.

- Computers, Privacy and Data Protection: an Element of Choice by Serge Gutwirth, Yves Poullet, Paul De Hert, Ronald Leenes
  ISBN: 9400706405Indeed, the consequences of technological applications due to unprecedented storage, processing and transmission capacities and to the possibilities of miniaturization, convergence, interoperability and ubiquity, represent powerful triggers and challenges to emerging developments, but they are certainly not the only determining factor. The current developments are also linked to many other sources of action and change, such as business models, security policies, population management, police work and law enforcement, leisure, culture, health policies, practices in the 'real' and in the 'virtual' world and so on. In the face of such dynamism, the "element of choice" unambiguously evokes both the need to collectively take responsibility and direct those developments in a desirable direction, providing the ambit to influence and steer the course of things in a way that matches our expectations not only toward privacy and data protection, but also more broadly, to the kind of world we are building. - From the back of the cover.
- Information Privacy Law by Daniel J. Solove and Marc Rotenberg
  ISBN: 0735555761Information Privacy Law includes insightful analysis of all the major cases including Bartnicki v. Vopper, Watchtower Bible v. Village of Stratton, United States v. Kyllo, McVeigh v. Cohen, United States v. Kennedy, Doe v. 2TheMart, United States v. Simons, and others. Information Privacy Law also includes explanations of key statutes and regulations such as the Freedom of Information Act, Children's Online Privacy Protection Act, European Union Data Protection Directive, Electronic Communications Privacy Act, and more. - Aspen Publishers
- Protectors of Privacy: Regulating Personal Data in the Global Economy by Abraham L. Newman
  ISBN: 0801445493"Protectors of Privacy deals with an increasingly important issue that cuts across international security, international political economy, international law, and comparative political economy. Abraham L. Newman offers an intriguing argument involving the general role of 'regulatory power' and the specific role of the European Union in world politics." - Michael E. Smith, School of International Relations, University of St. Andrews - From the back of cover.
- Negotiating Privacy: The European Union, The United States, And Personal Data Protection by Dorothee Heisenberg
  ISBN: 1588263800

Treatises

- Cloud Computing
  - Info. Security & Privacy: Prac. Guide to Fed, State & Int'l Law § 39:19
  - While there are no laws that specifically address cloud computing, this treatise explores various security and privacy laws on Internet, including state email laws and issues with spyware and phishing.
- Electronic Health Records
  - § 7.11B ELECTRONIC HEALTH RECORDS, 2004 WL 2635854
  - Chapter 7 discusses federal laws such as the Health Information Technology for Economic and Clinical Health Act (HITECH Act) and explores potential issues with the use of Cloud Computing model.
- eDiscovery technology solutions will see rapid development
  - eDiscovery for Corporate Counsel § 27:3
  - To avoid the most serious pitfalls of cloud computing and virtualization (compliance, data retention, privacy, nexus, jurisdiction and taxation), the article discusses that it is critical for the corporate legal department to understand the business goals and articulate legal functional business requirements to protect the business.
- New technologies subject to cyberattacks—Cloud computing
  - Data Sec. & Privacy Law: Combating Cyberthreats § 2:14.100 (2010)
  - Because the security of the user data is one of the major concerns with Cloud Computing, the treatise explores issues with the security threats from from the cloud service provider itself as well as the external threats.
- Personal Jurisdiction

- § 9:12. Nature of the Internet—Push systems and implications for personal jurisdiction, 1 Internet Law and Practice § 9:12

- In the environment where the Internet service providers often “push” data to users, there are fewer questions relating to purposeful availment in a push system. The treatise points out that, although several courts have acknowledged that cloud computing services raise new concerns with respect to Fourth Amendment jurisprudence, to date courts have not addressed what implications these services may have for jurisdictional jurisprudence.

Blogs

There are a number of blogs that discuss legal issues in Cloud Computing.

- Managing Risks in Cloud
  http://blog.firmex.com/managing-cloud-computing-risk
  by Nicole Black
- Cloud Computing: A Legal Maze for Europe
  http://meship.com/Blog/2011/02/13/cloud-computing-a-legal-maze-for-europe/
  by Brian Bryne

Digital Due Process

The Digital Due Process Coalition - Digital Due Process is a diverse coalition of privacy advocates, major companies and think tanks, working together. Digital Due Process advocates reform of the ECPA.

- The Ditigal Due Process Homepage
  http://www.digitaldueprocess.org/index.cfm?objectid=37940370-2551-11DF-8E02000C296BA163
- The Digital Due Process Coalition Members
  http://www.digitaldueprocess.org/index.cfm?objectid=DF652CE0-2552-11DF-B455000C296BA163
- The ECPA of 1986: Principles for Reform
  http://www.digitaldueprocess.org/files/DDP_Burr_Memo.pdf

Cloud Standards Customer Council

The Cloud Standards Customer Council is an end user advocacy group dedicated to accelerating cloud's successful adoption, and drilling down into the standards, security and interoperability issues surrounding the transition to the cloud.

- The Cloud Standards Customer Council Homepage
  http://www.cloud-council.org/index.htm
- About the Council
  http://www.cloud-council.org/about-us.htm
- Resource Hub
  http://www.cloudstandardscustomercouncil.org/resource-hub.htm

Back to Top

International Resources

International Legal References on Data Privacy

Organisation for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

In 1980, the OECD published the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data as the basic principles on personal information usage. Despite their age and the difficulty to apply them directly to growing data collection and management practices, these principles are significant because they influenced many laws in the world including EU data protection laws.

ASIA

The Asia Pacific Economic Cooperation (APEC) - Privacy Framework

In 2005, recognizing the importance of privacy, the APEC published a Privacy Framework to 1) improve information sharing among government agencies and regulators, 2) facilitate the safe transfer of information between economies, 3) establish a common set of privacy principles, 4) encourage the use of electronic data as a means to enhance and expand business, and 5) provide technical assistance to those economies that have yet to address privacy from a regulatory or policy perspective.

AUSTRALIA

- The Privacy Act regulates how the personal information is collected, used, and disclosed, its accuracy and security requirements, and general right to access the information.

CHINA

- Article 38, 39, and 40 of the Chinese Constitution provide the overarching privacy protection while specific law may impose additional restrictions.
    - The Provisional Rules on Management of Individual Credit Information Database, for example, contains the restriction on the use of individual credit information.

INDIA

- The Right to Information Act of 2005 provides right to information for citizens to secure access to information under the control of public authorities as well as setting forth the restrictions on disclosure of personal information.

JAPAN

- The Act on the Protection of Personal Information aims to protect the rights and interests of individuals while taking consideration of the usefulness of personal information. The Act provides only the general requirements and the administrative guidance specific to business sectors must be also reviewed and assessed.

PHILIPPINES

- Section 4 of the Prescribing Guidelines for the Protection of Personal Data in Information and Communications System in the Private Sector issued by the Department of Trade and Industry provides the general principles for the protection of personal data.

EUROPE

EU Member States

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 and Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002

In 1995, the EU adopted the Data Protection Directive ("DP Directive") to provide individuals with protections with regard to the processing of personal data and the free movement of personal data. Further, the EU also adopted the Directive on Privacy and Electronic Communications in 2002 to combat spam and the unconsensual use of personal data in the electronic communications. While the directive itself has limited legal significance, the EU member states have a duty to enact legislation so their national laws conform to the directive. However, the directive is only a legislative template for substantial conformity. Thus, it is imperative to understand the specific member state's laws governing the personal data protection, passed in response to these directives.

AUSTRIA

- D atenschutzgesetz 2000 (DSG 2000) serves as the foundation of data protection law in Austria, and it incorporates the EU's Data Protection Directive. Further, the Austrian data protection commission monitors the national section of the Schengen Information System (N.SIS) and supervise the data protection according to Article 114 of the Convention implementing the Schengen agreement.

FRANCE

- The Data Protection Act of 1978, as amended in 2004, complies with the EU Data Protection Directive. Further, the criminal code punishes the use of personal data for purposes other than those that justified their collection, or storing them beyond a date justified by the purpose of the processing.

GERMANY

- The Federal Data Protection Act, as amended in 2002, complies with the EU Data Protection Directive. Unlike similar Acts in other countries, the

Federal Data Protection Act requires that private businesses that collect, process, and use personal data appoint an in-house data protection officer.

IRELAND

- The Data Protection (Amendment) Act 2003 implements the EU Data Protection Directive. It also allows an individual to object to the use of the personal data for direct marketing.

UNITED KINGDOM (UK)

- The Privacy and Electronic Communications (EC Directive) Regulations 2003 implement the EU Directive on privacy and electronic communications.

Non-EU Member States

Many non-Member States have passed laws consistent with the EU Data Protection Directives to allow the transborder personal data transfer between the Member States and the Non-Member States.

SWITZERLAND

- The Federal Act of Data Protection of 1992 aims to protect the privacy and the fundamental rights of persons when their data is processed. It includes the restrictions on cross-border disclosure of personal data. This Act is deemed adequate under the EU Data Protection Directive.

MIDDLE EAST / AFRICA

While none of the Middle Eastern or African countries are a member of the OECD, some countries provide the principle of privacy protection in their constitutions and others enacted legislation to protect personal information.

ISRAEL

- The Protection of Privacy Law 5741-1981 provides that no person shall infringe the privacy of another without his consent.

TURKEY

- Article 20 of the Constitution of the Republic of Turkey provides that everyone has the right to demand respect for his private and family life. Privacy of individual and family life cannot be violated. Further, aligned with Turkey's application to accede to the European Union, Turkey drafted the Data Protection Act in accordance to the EU Data Protection Directive. However, the Act has not been enacted.

SOUTH AMERICA

The Andean Community issued Decision 439, General Framework of Principles and Rules and for Liberalizing the Trade in Services in the Andean Community. The decision promotes privacy protection regarding the processing and dissemination of personal data. In addition, Chile and Peru are a member economy of the APEC which published a Privacy Framework.

ARGENTINA

- The Argentina Personal Data Protection Act of 2000 purports to provide the comprehensive protection of personal data included in files, records, databases or other data processing technical means -whether public or private- used for reporting purposes. It is also referred to as "Habeas data."

BRAZIL

- Privacy is governed under Article 5 of the 1988 Constitution. However, other laws, such as the Habeas Data Law of 1997, may apply to impose restrictions on the use of personal data.

CHILE

- The Personal Data Act establishes general rules regarding treatment of personal data (any information concerning a person) and sensitive data.

NORTH AMERICA / LATIN AMERICA

Most North American countries restrict the collection, use, and disclosure of personal data through their legislation. On the other hand, the protection of personal data and privacy is governed under constitutions in many Latin American countries.

CANADA

- The Personal Information and Electronic Documents Act purports to establish rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.

MEXICO

- Privacy is generally governed under the 1917 Constitution of Mexico. However, the use of personal information may be also restricted under the specific laws such as the Federal Consumer Protection Law.

NOTE: Only select country's laws and regulations are highlighted to demonstrate the diverse nature of the approaches to Data Privacy. For other countries, Information Shield offers the "International Data Privacy Laws By Country" as a good start.

About OECD

For more information on the OECD, please visit the OECD website:

- The OECD Home
  http://www.oecd.org/
- The History of the OECD
  http://www.oecd.org/document/25/0,3746,en_36734052_36761863_36952473_1_1_1_1,00.html
- Member Countries
  http://www.oecd.org/pages/0,3417,en_36734052_36761800_1_1_1_1_1,00.html

About APEC

For more information on the APEC, please visit the APEC website:

- The APEC Homepage
  http://www.apec.org/
- The History of the APEC
  http://www.apec.org/About-Us/About-APEC/History.aspx
- Member Economies
  http://www.apec.org/About-Us/About-APEC/Member-Economies.aspx

About EU

For more information on the European Union (EU), please visit the EU website:

- The EU Homepage
  http://europa.eu/index_en.htm
- The History of the EU
  http://europa.eu/about-eu/eu-history/index_en.htm
- Member Countries
  http://europa.eu/about-eu/member-countries/index_en.htm

Safe-Harbor

For information on U.S.-EU Safe Harbor Framework, the following links are helpful.

- Introduction to U.S.-EU Safe Harbor
  http://www.export.gov/safeharbor/eu/index.asp
- Guide to Self-Certification
  http://www.export.gov/build/groups/public/@eg_main/@safeharbor/documents/webcontent/eg_main_018879.pdf
- Safe harbor list
  http://safeharbor.export.gov/list.aspx

About the Andean Community

For more information on the Andean Community, please visit the Andean Community website:

- The Andean Community Homepage
  http://www.comunidadandina.org/endex.htm
- The History of the Community
  http://www.comunidadandina.org/ingles/quienes/brief.htm
- Member Countries
  http://www.comunidadandina.org/ingles/who.htm

Helpful Surveys

For additional survey of privacy laws, the following materials may be helpful:

- International Data Privacy Laws by Country
  http://www.informationshield.com/intprivacylaws.html
- Privacy International - PI Reports
  https://www.privacyinternational.org/category/article-type/pi-reports-1

Back to Top

News & Media

Legal News

Cloud Computing and associated legal issues are discussed on several news media available on Internet.

- EPIC offers a section devoted to News on Cloud Computing. - Electronic Privacy Information Center.
- Nicole Black advocates to go back to basics in "Law life: Cloud computing for lawyers: back to basics." - LegalNews, March 17, 2011.
- Corporate council featured "Cloud Computing Down to Earth: A Primer for Corporate Counsel" by Ben Kerschberg on February 28, 2011.
- Marcia Savage advises caution when negotiating with cloud service provider in "Cloud computing contracts: Tread carefully." - SearchCloudSecurity.com, February 16, 2011.
- Kevin F. Brady discussed ethical issues with Cloud Computing in "Cloud Computing—Panacea or Ethical “Black Hole” for Lawyers (The Bencher—November/December 2010)"- The American Inns of Court.
- Cloud computing making inroads at many Maryland law firms - Daily Record, December 5, 2010.

Business & Technology News

Business news highlight and track the market trend in Cloud Computing. In response, many IT providers are improving Cloud Computing technology and implementation strategy to address business and legal challenges in this new paradigm.

- Gartner warns CIOs that Cloud sourcing contract terms often favor the provider, leaving the buyer exposed and it highlights Four Risks CIOs Should Address When Contracting for Cloud Service.- Garnter

- Cloud Computing: Rethink IT. Reinvent Business. - IBM

- IBM works with European Union consortium to resolve privacy and resilience limitations of public cloud infrastructures in a new project called Trustworthy Clouds (TClouds).

- Trustworthy Clouds (TClouds), co-financed by the European Commission, aims to build a prototype Internet-scale infrastructure which allows virtualized computing, network, and storage resources over the Internet to provide scalability and cost-efficiency.

- IBM and Luxembourg Government define how Cloud Computing can be applied to the Financial market.

- Investor's Business Daily published Security Issues Rain on Cloud Computing on December 8, 2009, highlighting that legal and compliance risks are the biggest hurdle to wider adoption of cloud computing. Some 88% of tech buyers do not use cloud due to concerns on data control and security.

  - Investor's Business Daily, nonetheless, reported expected new growth in Cloud Computing on March 28, 2011 in the article "Cloud Computing Moves into New Growth Phase."

RSS Feed from EPIC

EPIC is a public interest research center and publishes e-mail and online newsletter on civil liberties in the information age including issues with Cloud Computing and Privacy laws.

- Annual Computer Security Applications Conference (ACSAC) 2012
- EPIC Argues for Privacy of Driver's Records in Supreme Court Case
- Senate Reauthorizes SAFE WEB Act
- Congress to Scrutinize TSA's "Scanner Shuffle"
- President Issues Secret Cybersecurity Directive, EPIC Seeks Public Release

View Website
View Feed

RSS Feed from K&L

K&L Gates publishes "Legal Cloud Central Blog" to feature blogs focusing on Cloud Computing and SaaS issues and developments.

- US-Japan Report on Cloud Computing Wary of EU Privacy Protections
- Election 2012: What it Means for Emerging Technologies
- Cloud Considerations: E-Discovery
- Virtual Law Offices in the Clouds
- First Circuit's Patco Decision Clarifies Liability Rules for Providers of Online Banking Services: Federal Regulators Provide New Guidance on Cloud Computing

View Website
View Feed

Back to Top