CLOUD COMPUTING AND COMPLIANCE WITH KEY CONSUMER PROTECTION LAWS AND REGULATIONS

FEBRUARY 2013

Alysa Z. Hutnik
Partner[1]
Kelley Drye & Warren LLP
3050 K Street, NW
Washington, DC 20007
202.342.8603
ahutnik@kelleydrye.com

This briefing provides an overview of key consumer protection legal considerations for cloud computing service providers, including an overview of applicable cloud computing terminology, general consumer protection obligations, best practices to limit third-party liability risks, consumer privacy and data security requirements, and guidance for responding to requests for customer data.

RELEVANT CLOUD COMPUTING BACKGROUND

I. THE CLOUD COMPUTING VALUE PROPOSITION

Cloud computing provides a means by which companies can avoid acquiring and maintaining computer equipment and software. Cloud computing allows computer technology to be easily accessed as a service over the Internet or *via* a private network from any location, so that computer technology, software programs, and data can be available when and where the user needs them. Specific elements of the cloud computing value proposition include the following:

- The customer only pays for as much technology capacity as it needs. For computer processing, a company using cloud computing can avoid the capital expenditure and the ongoing expense of maintaining the computer infrastructure. The same concept applies to the software application, allowing the company to avoid the upfront license fee;

- Flexible pricing on a pay-for-use basis is a big piece of the value proposition, along with the rapid increase and decrease of usage with minimal involvement by the service provider. Rather than buying and maintaining server capacity and operating systems or paying upfront licensing fees, an enterprise can acquire that same capability from a cloud provider, access it over the Internet, and pay a pre-defined price for the service.

[1] Special thanks goes to Matthew Sullivan, an associate at Kelley Drye & Warren LLP, who co-authored this publication.

II. DEFINITIONS

The term "cloud computing" is used in a variety of contexts within the information technology industry. The Commerce Department's National Institute of Standards and Technology (NIST) has attempted to provide structure to the cloud computing industry by defining the three basic types of service models for cloud computing as follows:[2]

- Cloud Infrastructure as a Service (IaaS) — involves the provisioning of fundamental computer resources (*e.g.*, processing, storage, networks);

- Cloud Software as a Service (also known as "Software As a Service" or "SaaS") — involves access to a provider's software applications running on a cloud infrastructure; and

- Cloud Platform as a Service (PaaS) — involves the capability to deploy onto the cloud infrastructure applications created by the user with provider-supported programming languages and tools.

In addition, NIST describes the following four models for deployment of the cloud infrastructure:[3]

- **"**Private clouds**"** maintain all the technology components, servers, and software for a single organization. The solution may be managed by the user or a third party but is provided for the benefit of only one organization. The customer makes better use of its current assets; for example, not every laptop has to be loaded with the software and have the data stored on it. These private clouds are increasingly being deployed within larger enterprises.

- A **"**public cloud**,"** such as salesforce.com, Amazon's cloud offering, or Google's Gmail, is available to anyone or to large industry groups and in either case is owned by the provider of the service. This deployment model offers the greatest potential flexibility and savings but also involves granting the service provider the substantial control over the enterprise's technology capabilities. Many large enterprises are using this deployment for discrete services and are evaluating ways to further use the model.

- The service models may be deployed using a **"**community cloud**,"** which NIST defines as cloud infrastructure shared by several organizations and that supports a specific community that has shared concerns, such as the mission of the organizations or security, privacy, policy, or regulatory compliance.

- **"**Hybrid clouds**"** consist of a combination of two or more of the three preceding models.

---

[2] NIST, The NIST Definition of Cloud Computing (Sept. 2011), *available at* http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

[3] *Id.*

III. RATIONALE FOR EVOLVING CONSUMER PROTECTION LAWS AND REGULATIONS TO ADDRESS CLOUD COMPUTING

Traditional, or pre-cloud, computer networking environments were defined by the following characteristics:

- Point-to-Point Transfers – data transfers were discrete, scheduled, and occasional, and relied upon proprietary transfer protocols and specialized communications lines
- Non-networked – the use of centralized databases and segmented customer files

Cloud computing has introduced a new paradigm in the storage and flow of consumer data that is defined by the following characteristics:[4]

- The scale of data flows, individually and in the aggregate, has increased massively
- Data flows are now multi-directional
- Processing involved in data flows has expanded to include highly complex and process-oriented steps implemented within systems of networks
- Oversight over data flows has evolved into a model of collaboration and resource commitments

COMPLIANCE WITH CONSUMER PROTECTION LAWS & REGULATIONS

I. GENERAL CONSUMER PROTECTION CONSIDERATIONS FOR CLOUD COMPUTING PROVIDERS

A. Negotiations Relating to Legal Compliance

Negotiations between the cloud service provider and its potential customer should include discussions on compliance with applicable laws and regulations. The cloud service provider should be willing to contractually agree that it is complying with laws generally applicable to its business. Similarly, the client will need to provide assurances that it will remain in compliance with laws applicable to its business upon commencement of the cloud computing offering. As with traditional outsourcing and software licensing arrangements, addressing compliance with changes in laws over time may be challenging depending on the laws applicable to the delivery and receipt of the cloud computing services.

Providers of cloud service tailored for specific regulated industries may agree to monitor and modify their offerings to address changes in laws over time. In any event, a regulated customer

[4] Presentation, *Emerging Law and Policy Issues in Cloud Computing - Managing Global Data Privacy in the Cloud* (Mar. 19, 2010), Professor Paul Schwartz, Berkeley Law, University of California, *available at* http://www.law.berkeley.edu/files/Schwartz.pdf.

will need to conclude that it can maintain its compliance with laws and will need to develop a reasonable plan for migrating off the cloud computing platform if necessary to comply with changes in laws that are not addressed by the provider's offering.

B. Enforcement of Consumer Protection Laws and Regulations

With respect to consumer protection legal obligations, much of the enforcement authority for applicable laws and regulations resides with the U.S. Federal Trade Commission ("FTC") and the state attorneys general.

1. FTC Authority

Section 5 of the FTC Act prohibits unfair or deceptive acts or practices.[5] Through policy statements, the FTC has provided its interpretation of *unfair* or *deceptive* business practices.

- A deceptive act or practice is based on three core elements: (a) a representation, omission or practice, (b) about a material fact, (c) that is likely to mislead a consumer acting reasonably under the circumstances.[6] For a cloud service provider, a deceptive act or practice could relate to information that the provider gives to clients explaining how it will handle and safeguard the clients' data.

  - Example – Deceptive Practices: ***U.S. v. Path, Inc.* (2013)**[7] – In January 2013, the FTC announced a settlement with social networking app developer Path, Inc. over charges that it deceived its users, in violation of Section 5, by collecting personal information from their mobile device address books without their knowledge and consent. According to the FTC's Complaint, Path automatically, and without users' consent, collected and stored available names, addresses, phone numbers, email addresses, dates of birth, and Facebook and Twitter usernames contained in a user's address book.

- An unfair act or practice is also based on three core elements: (a) an act or practice that causes substantial injury to consumers, (b) which consumers cannot reasonably avoid, and (c) which is not offset by benefits to consumers or competition.[8] In the cloud computing context, an unfair practice could relate to the cloud provider's failure to take reasonable measures to protect the consumer data maintained within its cloud.

---

5 15 U.S.C. § 45.

6 FTC Policy Statement on Deception (1983), *appended to Cliffdale Assocs.*, 103 F.T.C. 110, 174 (1984).

7 *U.S. v. Path, Inc.*, No. C-13-0448 (N.D. Cal. Complaint Filed Jan. 31, 2013), *available at* http://www.ftc.gov/os/caselist/1223158/130201pathinccmpt.pdf.

8 FTC Policy Statement on Unfairness, *reprinted in Int'l Harvester Co.*, 104 F.T.C. 949, 1070 (1984).

- Example – Unfair Practices: ***In re Vision I Properties, LLC (d/b/a CartManager Int'l.)* (2005)**[9] – CartManager licensed an online shopping cart software to retailers and provided a hosted online service to thousands of small online retail merchants. According to the FTC, some merchants who used CartManager's software stated in their privacy policies provided to customers that they did not sell, trade, or lend customer information. Nevertheless, CartManager allegedly collected and rented the personal information of nearly one million consumers who shopped at merchant sites. The FTC claimed that CartManager did not adequately inform consumers or merchants that it would collect and rent this information and that it acted knowing that renting the information was contrary to merchants privacy practices. The FTC claimed that CartManager's actions constituted unfair acts or practices in violation of Section 5.

Violations of Section 5 of the FTC Act can present significant legal, reputational, and compliance risks for cloud service providers. A determination about whether a particular act or practice may be construed as unfair or deceptive will depend on an analysis of the facts and circumstances. Although individual violations or inbound complaints may appear isolated, they may, when considered in the context of additional information, including other violations or complaints, raise concerns about unfair or deceptive acts or practices.

2. State Attorneys General

Most states have enacted consumer protection laws that prohibit unlawful, unfair or fraudulent business acts or practices.[10] State Attorneys General have broad authority to enforce these laws to protect the residents of their states. In addition, many state statutes expressly provide that their consumer protection laws are to be construed in a manner consistent with the FTC Act and its interpretations by the FTC.[11]

II. THIRD-PARTY LIABILITY FOR CLOUD SERVICE PROVIDERS

Cloud service providers can inadvertently expose themselves to third-party liability issues by overlooking red flags relating to the business practices of their customers. The FTC continues to take aggressive action in imposing liability on companies that handle consumer data and that partner with entities that engage in fraud or other unlawful practices. The FTC's Bureau of Consumer Protection, for example, has increased its focus on third-party liability as a policy issue. The FTC's determination of liability is based on whether a party "knew, or should have known"[12] or "consciously avoided knowing"[13] that it was assisting or facilitating the fraudulent activities of a client or partner.

---

9 *In re Vision I Properties*, No. C-4135 (Final Consent Apr. 26, 2005), Complaint *available at* http://www.ftc.gov/os/caselist/0423068/050426comp0423068.pdf.

10 *See, e.g.*, Cal. Bus. & Prof. Code §§ 17200 *et seq.*, 17500 *et seq.*

11 *See* Md. Code, Com. Law § 13-105.

12 *See., e.g., U.S. v. ACB Sales & Serv.*, 590 F. Supp. 561, 575 n.11 (D. Ariz. 1984) (§5(m) of the FTC Act requires "that the defendant or his agent have some knowledge, actual or constructive, of the requirements of the [rule]" such that defendant "know or should have known" that the conduct was unlawful.").

Under the "knew or should have known" standard, entities have some duty to investigate their clients' potentially fraudulent business practices.[14] In contrast, the "conscious avoidance" standard may be met if there is evidence that the entity knew or deliberately ignored the fraudulent conduct.[15] Under both standards, the FTC will consider whether clear warning signs were ignored—intentionally or unintentionally—and whether the company failed to enforce its own procedures designed to identify and mitigate a client's fraud. For example, SaaS providers that operate a legitimate software product that, nevertheless, can be used for fraudulent purposes would be at risk for regulator scrutiny depending on the level of visibility that the provider has into its clients' businesses or its ability to monitor clients' use of its software.

A. Risk Factors for Third-Party Liability

The following elements represent potential risk factors that could expose the cloud service provider to potential liability for the conduct of its clients:

- Lack of Due Diligence: A client's initial application information (or missing information), or materials submitted by potential clients during the initial negotiations for service, may provide early warning signs of unfair or deceptive behavior. The FTC expects a certain level of due diligence to identify such warnings signs using screening procedures that can include collecting background information on the potential client, checking references, and verifying the intended use of the cloud service.

- The Client's Business Model: Certain businesses and industries (*e.g.*, mortgage relief services, telemarketing, government grant services, credit card promotions) automatically attract increased scrutiny from regulators based on their potential for fraud. Regulators have stated that even a client's company name may present some evidence of fraudulent intent. Cloud providers that target services to high-risk industries should conduct reasonable due diligence into their client's business practices.

- Complaints: Complaints about unauthorized activity (for a SaaS provider, this could be complaints directly relating to the client's use of your hosted software) may originate from customers, law enforcement, the Better Business Bureau, and even employees. The FTC will evaluate the number of complaints as well as handling and response to such complaints.

---

13 *See, e.g.*, Telemarketing Sales Rule, 16 C.F.R.§ 310.3(b) (Assisting and facilitating – "It is a deceptive telemarketing act or practice and a violation of this Rule for a person to provide substantial assistance or support to any seller or telemarketer when that person knows or consciously avoids knowing that the seller or telemarketer is engaged in any act or practice that violates §§ 310.3(a), (c), or (d), or §310.4 of this Rule.").

14 *See* Telemarketing Sales Rule, 60 Fed. Reg. 43852 (Aug. 23, 1995), n. 103, citing to *Citicorp Credit Services, Inc.*, FTC Dkt No. C-3413 (Consent Order, Feb. 4, 1993) (In finding that Citigroup knew or should have known about its clients' fraudulent activities, the FTC stated that [t]he final consent order imposes a duty on Citigroup Credit Services to investigate merchants with high chargeback rates, and to terminate them if they are found to be engaging in fraudulent, deceptive or unfair practices.").

15 *See* 68 Fed. Reg. 4580, 4612 (Jan. 29, 2003).

- Support of and Visibility into Clients' Business Activities: The extent to which the cloud provider can view and access its client's data or provide "hands-on" services that assist with the client's business activities will be one factor that regulators will consider when assessing whether the cloud service provider was aware that a client was engaging in illegal business practices.

B. Examples of Third-Party Liability Enforcement Activity

- *FTC v. YourMoneyAccess, LLC* (2010)[16] – Financial Services Industry:
  - The FTC, along with the attorneys general of seven states, alleged that Your Money Access, LLC ("YMA"), a payment processor, violated Section 5 of the FTC Act by unfairly processing debit transactions to consumers' bank accounts, and violating the Telemarketing Sales Rule ("TSR") by assisting sellers or telemarketers that it knew, or consciously avoided knowing, were violating the TSR.
  - YMA allegedly accepted clients whose applications contained signs of deceptive activity (no physical address), including sales scripts with statements that were highly likely to be false. The FTC's Complaint further alleged that YMA closely monitored its merchant clients' return rates, yet continued to process payments despite 20 to 80 percent of transactions that were returned or reversed.
- *FTC v. InterBill* (2009)[17] – Financial Services Industry:
  - FTC alleged that InterBill, a payment processor, violated Section 5 of the FTC Act by unfairly processing debt transactions to consumers' bank accounts on behalf of Pharmacycards, a fraudulent provider of discount pharmacy cards.
  - Prior to working with Pharmacycards, InterBill allegedly failed to follow its own new client procedures, which included collecting adequate background information, checking merchant references, and verifying a physical address. The FTC further alleged that InterBill failed to obtain proof that consumers had authorized debits to their accounts, and "knew or should have known" of unauthorized transactions based on a return or cancellation rate of 70 percent, along with complaints from consumers and banks. In June 2009, a federal court ordered InterBill to cease its illegal practices and pay $1.7 million in consumer redress.
- *U.S. v. Ebersole* (2012)[18] – Telemarketing

---

[16] *FTC v. YourMoneyAccess, LLC*, No. 07 5147 (E.D. Pa. Complaint Filed Dec. 6, 2007), *available at* http://www.ftc.gov/os/caselist/0523122/071211complaint.pdf.

[17] *FTC v. InterBill, Ltd.*, No. 2:06-cv-01644 (D. Nev. Complaint Filed Dec. 26, 2006), *available at* http://www.ftc.gov/os/caselist/0423192/070108cmp0423192.pdf.

[18] *U.S. v. Ebersole*, No. 3:12-cv-00105-LRH-VPC (D.C. Nev. Filed Feb. 23, 2012).

- FTC alleged that Voice Marketing, Inc., an hosted telemarketing software provider, assisted and facilitated companies engaged in unauthorized telemarketing in violation of the Telemarketing Sales Rule. According to the FTC, Voice Marketing provided substantial assistance to clients by giving them access to computers, telecommunications services, and a dialing software available online that the telemarketer clients used to place millions of phone calls with prerecorded messages that contained sales solicitations.

- *FTC v. Global Marketing Group* (2007)[19] – Financial Services and Telemarketing

  - According to the FTC, Global Marketing Group ("GMG") processed payments on behalf of clients whose sales scripts clearly indicated that the clients' intended to violate the Telemarketing Sales Rule and industry rules that prohibit the processing of electronic banking transactions for outbound telemarketers.

  - The FTC claimed that GMG's support and assistance included drafting and reviewing sales scripts, fielding customer complaints, and payment processing and order fulfillment services that were conducted prior to performing any due diligence into its client's business practices.

C. Best Practices to Minimize Potential Third-Party Liability Scrutiny

- Know your clients and business partners, and implement procedures to conduct reasonable due diligence for evaluating potential new clients or partners;

- Turning a blind eye won't absolve your company of responsibility. You may be held liable if you knew or should have known or deliberately ignored that a client is engaging in deceptive practices. If there is an indication that a client may be engaging in illegal activity through the use of the cloud service, failing to investigate is not a good business strategy.

- "Red flag" evidence of a client or partner's questionable conduct already may be in your files. Establish procedures for regularly reviewing client correspondence, regulator or consumer inquiries concerning your clients, and other telltale signs of trouble. Cloud providers should ensure that they adhere to their internal best practices and closely monitor third-party feedback relating to potentially questionable/suspect businesses.

- "Trust, but verify." Protect your organization's reputation by monitoring the performance of companies you're doing business with on an ongoing business.

III. PRIVACY & DATA SECURITY CONSIDERATIONS FOR CLOUD PROVIDERS

When offering public or private cloud computing capacity, the provider must be aware of privacy and information security compliance issues. Certain privacy and data security

[19] *FTC v. Global Marketing Group, Inc.*, No. 8:06-cv-02272 (M.D. Fla. Filed Mar. 19, 2007), *available at* http://www.ftc.gov/os/caselist/0623186/070319globalmktggrpamndcmplt.pdf.

obligations may arise from several sources, including regulatory requirements and contractual obligations.

A. Patchwork of Key Laws and Regulations

Currently in the United States, there is no comprehensive privacy legislation at the federal level. Instead, the privacy law is made up of a patchwork of key laws and regulations that address privacy issues for different segments of personal information that may be stored in the cloud, consumers, or industries as identified below.

1. Federal Laws

The primary federal regulator in the privacy arena is the FTC, which has brought privacy and data security related investigations and actions against businesses using its general authority under Section 5 of the FTC Act. Section 5 of the FTC Act is the most broadly applicable privacy law. Similarly, the FTC also enforces the Gramm-Leach-Bliley Act ("GLB Act"),[20] which regulates similar conduct by financial institutions. The GLB Act and its promulgating privacy regulation[21] include requirements such as providing consumers with initial and recurring privacy notices and the opportunity to opt out of having the consumer's nonpublic personal information shared with nonaffiliated third parties.

Personal information collected online from children under the age of 13 is governed by the Children's Online Privacy Protection Act ("COPPA"),[22] and its implementing rule the COPPA Rule.[23] Notably, the COPPA Rule has a broader definition of "personal information" than is found under the GLB Act and several other laws and includes screen or user names where the information can be used to identify the child; photographs, video, and audio, geolocation information; unique device identifiers; and persistent identifiers such as cookies and IP addresses.

Additionally, any service provider that collects consumer credit information may be required to safeguard customer information in a manner consistent with the Fair and Accurate Credit Transactions Act ("FACTA"),[24] which added new provisions to the Fair Credit Monitoring Act ("FCRA")[25] to address identity theft. FCRA and FACTA limit how certain types of customer information may be used and shared by a business, in addition to requiring certain information security practices. Further, under the FCRA Red Flags Rule, amended by the Red Flag Program Clarification Act,[26] a business that acts as a "creditor" must maintain reasonable procedures to

---

20 15 U.S.C. §§ 6801-6809.

21 GLB Privacy Rule, 16 C.F.R. Part 313.

22 15 U.S.C. §§ 6501-6506.

23 16 C.F.R. Part 312.

24 15 U.S.C. § 1681 *et seq.*

25 *Id.*

26 S. 3987 (enacted Dec. 18, 2010).

develop and implement an identity theft prevention program designed to identify the "red flags" of identity theft and protect customer information.

The Health Insurance Portability and Accountability Act ("HIPAA")[27] restricts how covered entities can use health information, and also requires covered entities to generally implement "appropriate administrative, technical, and physical safeguards" to protect such health information.[28]

Additionally, a student's education records and personal information must be protected by educational institutions in accordance with the Family Educational Rights and Privacy Act[29] and its promulgated regulation.[30] Further, electronic communications generally are covered by the Electronic Communications Privacy Act ("ECPA"),[31] which, as described further below, addresses issues such as eavesdropping, wiretaps, and protection of stored communications.

2. State Laws

In addition to federal laws, several state laws add to the patchwork of key privacy laws. The principal regulator at the state level to enforce appropriate privacy and data security practices is the state attorney general. The tools available to state regulators and litigants have increased in recent years because of recently enacted state laws on privacy and information security. Additionally, for states that have not enacted specific privacy and information security laws, the state attorneys general may use their general authority to prohibit unfair or deceptive acts or practices under the relevant state consumer protection law.

The California Online Privacy Protection Act[32] requires operators of commercial websites that collect personal information from California residents to post a privacy policy that identifies the types of personal information collected on the website and the types of third parties with whom this information may be shared. The California "Shine the Light" law[33] also requires any company that discloses personal information to a third party for that party's own marketing purposes to disclose such practice to the consumer and either provide certain information about the types of information shared and the third parties with whom it is shared, or provide the consumer with the ability to opt-out of such sharing.

State attorneys general track information technology issues that may impact consumer privacy. For example, Maryland Attorney General Doug Gansler, the current President of the National

---

27 42 U.S.C. § 1306.

28 The HIPAA Security Rule, 45 C.F.R. § 164.500-164.534, also sets forth more detailed provisions governing the security standards for protecting electronic health information.

29 20 U.S.C. § 1232g.

30 34 C.F.R. Part 99.

31 18 U.S.C. § 2510-2522.

32 Cal. Bus. & Prof. Code § 22575-22579.

33 Cal. Civ. Code § 1798.83-1798.84

Association of Attorneys General ("NAAG"), recently launched a new Internet Privacy Unit tasked with the following functions:[34]

- Monitor companies to ensure compliance with state and federal consumer protections laws;
- Work with industry and privacy advocates to educate businesses and inform consumers of their privacy rights;
- Pursue enforcement actions where appropriate.

As a result of this initiative, cloud service providers can expect increased scrutiny of privacy and data security practices, increased enforcement in response to consumer concerns, and active monitoring to determine whether providers are honoring their statements to implement reasonable safeguards to protect consumer data.

B. Regulatory Privacy Frameworks With Implications for Cloud Providers

In 2012, two regulatory agencies issued final versions of major reports on privacy that have implications for cloud service providers:

1. FTC Privacy Framework

In March 2012, the FTC released a final report setting forth best practices for consumer privacy protection.[35] The report reflects the FTC Commissioners' and staff's current views on privacy protection. The report contains three overarching recommendations that apply to cloud providers' collection, use, and protection of their customers' data:

- **Privacy By Design**

This principle encourages entities to build in and promote privacy throughout their organization and at every stage of product development. Substantive privacy by design principles include data security, reasonable collection limits, sound retention practices, and data accuracy[36]—some of these principles are already required under the FTC's interpretation of Section 5 of the FTC Act, such as requirements that companies must provide reasonable security and disposal practices for consumer data. The new framework combines these requirements with recommendations regarding how entities should limit data collection and retention, and promote data accuracy.

---

[34] Press Release, "Attorney General Gansler Forms Internet Privacy Unit," Maryland Office of the Attorney General (Jan. 28, 2013), *available at* http://www.oag.state.md.us/Press/2013/012813.html.

[35] FTC, Protecting Consumer Privacy in an Era of Rapid Change – Recommendations for Businesses and Policymakers (2012), *available at* http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.

[36] *Id.* at 23.

The recommended data collection and retention standards are flexible, with standards based on the type of relationship, and use and sensitivity of the data (*e.g.*, data collection that is inconsistent with the context of a particular transaction should be accompanied by appropriate disclosures; data should be properly disposed "once the data has outlived the legitimate purpose for which it was collected"). Similarly, an entity should take reasonable steps to ensure that data is accurate, with the reasonableness of an entity's efforts determined by the use and sensitivity of the information (*e.g.*, an entity would not need to take special measures to ensure the accuracy of data used for marketing purposes, but accuracy efforts should be more robust for data used to determine a consumer's eligibility for benefits).

The FTC recommends that the substantive principles should be carried out through comprehensive data management procedures that are maintained throughout the life cycle of a product or service.[37] The report notes that its recent Consent Orders for Google and Facebook[38] illustrate the elements that a comprehensive privacy program should include.

- **Simplified Consumer Choice**

With respect to public cloud services (*e.g.*, Gmail), the FTC's recommendations allow an entity to collect and use data for practices that are consistent with the context of the transaction, the company's relationship with the consumer, or those transactions authorized by law without obtaining the consumer's consent.[39]

Certain specified practices would not typically require consumer choice.[40] These practices include fulfillment, fraud prevention (*e.g.*, practices designed to prevent security attacks or phishing), internal operations (*e.g.*, frequency capping or product improvement), legal compliance and public purpose (*e.g.*, intellectual property protection or using location data for emergency services), and most first-party marketing practices. But, if a company combines these practices with other practices that are not consistent with the interaction, consumer choice should be provided.

Where choice is needed, entities should provide choices at a time and in a context in which the consumer is making a decision about his or data. This principle focuses on providing consumers with clear and conspicuous choice mechanisms that are meaningful and relevant, such as offering choice "directly adjacent to where the consumer is entering his or her data" for online transactions or prominently at the point-of-purchase for offline transactions.

---

[37] *Id*. at 25-26. As one example of appropriate data management measures, the FTC recognized Mozilla for using SSL communication to encrypt the user data maintained within its cloud storage system.

[38] *In the Matter of Google, Inc.*, FTC Docket No. C-4336 (Oct. 13, 2011) (consent order), *available at* http://www.ftc.gov/os/caselist/index.shtm; *In the Matter of Facebook, Inc.*, FTC Docket No. 092 3184 (Nov. 29, 2011) (consent order), *available at* http://ftc.gov/os/caselist/0923184/index.shtm.

[39] *Id*. at 35.

[40] *Id*. at 36.

The Commission also recommends that companies should obtain affirmative express consent before (1) using consumer data in a materially different manner than represented when the data was collected; and (2) collecting children's information, financial and health information, Social Security numbers, precise geolocation data, and other sensitive information.[41]

- **Transparency**

The Commission report also recommends that companies increase the transparency of data practices to increase consumers' awareness regarding how and for what purposes companies collect, use, and share data.[42] In general, the Commission recommends that privacy notices should be clearer, shorter, and more standardized to enable better comprehension, allow consumers to easily compare different entity's notices, and encourage companies to use privacy as a competitive tool.

2. Dept. of Commerce Privacy Green Paper

In February 2012, the White House released its data privacy framework that includes consumer "ground rules" intended to govern how commercial entities collect and use consumers' personal information available on the Internet and through other networked technologies. [43]

The framework establishes a Consumer Privacy Bill of Rights ("Bill of Rights") that includes baseline consumer privacy protections that apply to all commercial uses of "personal data," which the framework broadly defines as "any data, including aggregations of data, which is linkable to a specific individual," and includes data that is linked to a specific computer or other device. The Bill of Rights is based on general and adaptable Fair Information Practice Principles ("FIPPs") and includes the following seven principles: individual control, transparency, security, access and accuracy, limited data collection, and accountability. The report states that these Bill principles will help strengthen consumer trust in networked technologies and, therefore, preserve the economic benefits of cloud computing, location-based services, and other services.[44]

To address privacy concerns with cross-border data flows associated with cloud computing services, the report encourages increased engagement with international partners to increase interoperability in privacy laws. Specifically, the framework supports mutual recognition of different commercial data privacy frameworks, including joint enforcement efforts that are conducted according to publicly-announced policies. The Administration also encourages international stakeholders to identify globally-accepted accountability mechanisms, such as the Asia-Pacific Economic Cooperation's ("APEC") voluntary system of Cross Border Privacy

---

41 *Id*. at 48.

42 *Id*. at 60.

43 Internet Policy Task Force, Dept. of Commerce, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (2012), *available at* www.whitehouse.gov/sites/default/files/privacy-final.pdf.

44 *Id*. at 6.

Rules,[45] that can be used to develop international codes of conduct that would simplify compliance burdens faced by multinational organizations.[46]

C. Privacy and Data Security Contractual Obligations

Privacy and information security obligations may originate from contractual commitments made to end-users and business partners, such as representations and promises made in a privacy policy. These promises may range from whether and how the cloud provider shares customer information, the level of security provided to such stored information, and the types of service providers with whom the company shares customer data and for what purposes. If any of these representations in the privacy policy change over time, the cloud provider should assess whether it is a material change that could trigger additional notice and consent obligations before applying the updated policy.

Additionally, the cloud service providers' clients often need to take certain due diligence and contractual measures with any third parties with whom they share customer data to confirm that the parties will protect the data as well. Thus, cloud providers should expect that clients may need to conduct appropriate due diligence of the cloud computing service provider's privacy policy and data safeguards.[47] The contract between the cloud service provider and the client often will address issues including the following:

- A specific description of how the cloud provider will safeguard customer data stored;
- The process for the service provider to provide notice to the company if the provider suffers (or may have suffered) a data breach;
- If feasible, obligations to keep the company's data logically separate from other data; and
- Confirmation that the cloud computing services comply with promises the company has made to its customers.

IV. DISCLOSURE OF CUSTOMER DATA

A timely issue impacting cloud service providers that maintain customer information in their data centers is the extent to which the provider is legally obligated to respond to requests for customer data (from law enforcement, or otherwise). The legal obligations for responding to these types of requests are found within the Electronic Communications Privacy Act and the Federal Rules of Civil Procedure.

---

[45] *See* APEC Cross Border Privacy Rules System, *available at* http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/CBPR/CBPR-PoliciesRulesGuidelines.ashx.

[46] *Supra*, n. 37 at 31.

[47] *See* W. Michael Ryan and Christopher M. Loeffler, *Insights Into Cloud Computing, Intellectual Property & Technology Law Journal* (Nov. 2010), *available at* http://www.kelleydrye.com/publications/articles/1406/_res/id=Files/index=0/1406.pdf.

A. The Electronic Communications Privacy Act ("ECPA")

The Electronic Communications Privacy Act ("ECPA")[48] was passed in 1986 to expand and revise federal wiretapping and electronic eavesdropping provisions. ECPA, which includes the Wiretap Act,[49] the Stored Communications Act,[50] and the Pen-Register Act,[51] regulates when electronic communications can be intercepted, monitored, or reviewed by third parties, making it a crime to intercept or procure electronic communications unless otherwise provided for under law or an exception to ECPA. ECPA defines "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce." This definition focuses on the transfer of the data—the time during which the packets of data are traveling between one point and the other.

Individuals who violate ECPA face up to five years of jail time and a $250,000 fine. Victims are also entitled to a civil suit of actual damages, in addition to punitive damages and attorney's fees.

The growth of cloud computing has resulted in calls for ECPA reform. Whereas an email stored on a home computer would be fully protected by the 4th Amendment warrant requirement, an email stored on a remote, cloud computing server may not be. More information, including documents, emails, pictures, personal calendars, audio recordings, and locational data is stored in the cloud. These types of information are offered little protection under current laws. Protections for locational data, in particular, have been widely discussed, but, to date, have not been added.

On September 20, 2012, the Senate Judiciary Committee adopted an amendment to the bill that appends provisions drafted by Committee Chairman Senator Patrick Leahy (D-VT) to revise ECPA. The amendment would require law enforcement to obtain a search warrant in order to access personal email and electronic communications stored by a third-party service provider. In addition, the legislation requires that the Government notify the individual whose account was disclosed, and provide him/her with a copy of the search warrant within 3 business days of the Government's receipt of the communications.

---

[48] The Electronic Communications Privacy Act of 1986 (ECPA), Pub. L. 99-508, Oct. 21, 1986, 100 Stat. 1848 (1986).

[49] Wire and Electronic Communications Interception and Interception of Oral Communications, 18 U.S.C. Chapter 119.

[50] Stored Wire and Electronic Communications and Transactional Records Access, 18 U.S.C. Chapter 121.

[51] Pen Registers and Trap and Trace Devices, 18 U.S.C. Chapter 206.

On November 29, 2012, the Judiciary Committee adopted by voice vote several amendments to the legislation offered by Senator Leahy in response to concerns raised by law enforcement.[52] The amendments included the following:

- Clarification that the bill does not apply ECPA's warrant requirement to other federal laws, such as the Wiretap Act;
- Extension of time period (from 3 to 10 business days) during which the Government must give notice; and
- Requirement that service providers notify the Government of their intent to inform a consumer about a request for electronic communications at least 3 business days before such notice is given.

The last activity on this legislation occurred on November 29, 2012, when the U.S. Senate Judiciary Committee approved *The Electronic Communications Privacy Act Amendments Act of 2012* (H.R. 2471).

B. Civil Discovery Requests for Data Stored in the Cloud

In addition to implementing procedures to respond to information requests from law enforcement, cloud service providers also must develop a policy that addresses their customer data production obligations in response to civil discovery requests for data stored on the cloud.

Specifically, Federal Rules of Civil Procedure Rules 34 and 45 require parties and nonparties, respectively, to produce electronically stored information ("ESI") within their "possession, custody, or control."[53] "Control" is defined as the "legal right to obtain documents upon demand."[54] By application, courts have found the "right to obtain" applies where the respondent had either a contractual right[55] or agency authority to access the data, or where the respondent was legally required to have the data readily available for inspection.[56] Case law to date has not addressed the discovery of data stored in the cloud computing context, and the extent to which a cloud provider "controls" such data has yet to be litigated. In the absence of applicable precedent, a cloud service provider's production obligations are limited to data that the provider has a "legal right to obtain."

---

[52] A section-by-section breakdown of the ECPA amendments is available at http://www.leahy.senate.gov/press/section-by-section-breakdown-of-senator-leahys-ecpa-amendment

[53] Fed. R. Civ. P. 34(a)(1).

[54] *See In re Bankers Trust Co.*, 61 F.3d 465, 469 (6th Cir. 1995).

[55] *See e.g., Flagg v. City of Detroit*, 252 F.R.D. 346 (E.D. Mich. 2008) (finding that defendant city had "control" over the text messages preserved by third party SkyTel pursuant to their contractual relationship).

[56] *See e.g., Tomlinson v. El Paso Corp.*, 245 F.R.D. 474 (D. Colo. 2007) (holding ERISA legally required defendant employers to ensure that employment records be readily available for inspection such that they had "control" over data, even though it was in the possession, custody and control of a third party).

Questions and factors that the cloud provider must consider when evaluating whether it has a legal right to obtain customer data in response to a civil discovery request include the following:

- Even though the cloud provider may manage the underlying cloud infrastructure (*e.g.*, for a public cloud computing platform), do clients have the ability to control certain network infrastructure components such as firewalls, load balancing, and virtual private network ("VPN") capabilities?
- Can customers deploy and run arbitrary software, including operating systems and applications? If so, is the customer solely responsible for the operation of the applications and for their content, including the collection, storage, use, disposal, accuracy, and security of the data?
- Under the terms of the cloud services agreement, does the customer maintain full possession, custody, and control over—and all legal obligations regarding retention and production of—all hardware, software, applications, data, databases, and content provided or used by the customer and/or its end users to access the cloud services?
- To what extent can the cloud provider control its customers' data? Specifically, does the cloud provider have administrative rights to control data on its customers' virtual machines or within their data layers?
- Does the cloud provider monitor the content of data moved and stored in the cloud, or does it rely solely on the customer assurances that their activities comply with applicable privacy and other laws, and can only lock non-compliant customers out of the cloud platform and/or terminate their accounts?

Identifying answers to these question will enable the cloud service provider to determine whether it has administrative control over its customers' data and, thus, whether it has an obligation to produce such information in response to subpoena requests for such third party data pursuant to Fed. R. Civ. P. 34 and 45.

V. GENERAL CONSIDERATIONS AND BEST PRACTICES FOR COMPLIANCE WITH CONSUMER PROTECTION LAWS AND REGULATIONS

When seeking to offer cloud services to companies or consumers, the provider must consider the full range of legal, regulatory, and compliance issues that are relevant to itself and its customers that govern, among other things, the cloud provider's access restrictions to client data, service quality, data transparency, cost, overall privacy and data security protections, consumer protection obligations, and technological needs and innovation. Specific factors that cloud service providers should consider when assessing compliance with key consumer protection laws and regulations include the following:

1. **Type of the Data Maintained in the Cloud** – Cloud providers should carefully consider the unique risks associated with each type of business information — including, for example, personnel information linked to a customer's employees, partners, or customers, or trade

secret and proprietary information, or payment card information — that it maintains in its systems. This may influence the types of protections that it implements.

2. **Location of the Data in the Cloud** – The jurisdiction(s) in which the data is located will determine the range of laws that apply to that data. Certain customers may seek to limit their data to certain locations and may wish to collaborate on developing contract provisions that expressly identify the geographic area where their data will be stored or processed. As a result, cloud providers should internally evaluate the extent to which they are willing to identify where their cloud servers are based geographically, or provide assurances on the location of a customer's data, and whether this is feasible to their business.

3. **Client and cloud provider's status under the U.S.-EU Safe Harbor Framework ("Safe Harbor")** – To address international consumer privacy concerns and obligations, a U.S. cloud provider might ensure that it and its European-based clients are Safe Harbor certified if EU personal information will be transferred to a US-based cloud provider or to US-based facilities.

4. **Cloud provider's ability to access the personal data** – Cloud providers may be able to configure their cloud to ensure that they cannot access a client's personal data stored in the cloud, thereby making it technologically impossible for the provider to comply with a law enforcement request to produce a client's business records without involving the client. Such an approach may provide a more effective means to avoid involuntary disclosure of a client's data in response to a law enforcement request than attempting to limit the client's data to specific servers or geographic locations.

In addition, the following provides a summary of key customer data handling considerations that should be addressed during contract negotiations between a cloud provider and its clients:

1. **Compliance with laws and regulations**. Cloud providers will need to negotiate specific service agreement terms that adequately address the geographic locations where the client's data can be stored/processed, the provider's obligations to provide the client with prior notice and an opportunity to object to disclosure when the client's data is subject to a third party request (such as in the form of a subpoena or otherwise), and specific requirements concerning the types of security and privacy terms that apply to the data.

2. **Ownership of the Data**. A service agreement between a cloud provider and a client should expressly state whether the client retains exclusive ownership over all of its data (and metadata of such data), and whether the cloud provider acquires any rights or licenses through the agreement, including intellectual property rights or licenses, to use the organization's data for its own purposes; and whether the cloud provider acquires any interest in the data; and whether and under what timeframe the provider must return all data and metadata to the client upon termination of service.

3. **Data Visibility**. The service agreement should specify the extent to which clients have visibility into the security controls and processes employed by the cloud provider. For example, the service agreement might describe the client's right to audit controls using a

third party, identify thresholds for alerts and notifications, and specify the level of detail and schedule for reporting.

4. **Privacy and Data Protection**. The cloud provider should communicate to clients how it controls access to the stored data, and secures the data while at rest, in transit, and in use. Service agreements also should stipulate sufficient measures to ensure that any data sanitization (fully expunging data from storage media) is performed appropriately throughout the system lifecycle.

5. **Data Continuity**. The service agreement should include provisions and procedures that govern data availability, data backup and recovery, and disaster recovery.

6. **Incident Response**. The service agreement should identify the type of incidents that are reportable by the cloud provider (such as data breaches) versus those that are not reportable (such as intrusion detection alarms).

###