SECURITY AND PRIVACY OF PERFORMING DATA ANALYTICS IN THE CLOUD

A Three-way Handshake of Technology, Policy, and Management

Nidhi Rastogi, Marie Joan Kristine Gloria, and James Hendler

ABSTRACT

The cloud platform has paved the road for faster set up of infrastructure and related goals for both startups and established organizations. However, concerns around security and privacy of user information have suppressed its wider acceptance and an all-encompassing deployment, especially in business-critical applications. We explore security and privacy concerns that occur when data is exchanged between a cloud service provider (CSP) and a primary cloud user. Our thesis asserts that "technology, policy, and sound management" of the cloud service in collaboration have the potential to provide a holistic solution, one that none of the subsets of the approaches can offer separately.

Keywords: cloud computing; policy; privacy; security.

Introduction

The cloud platform offers opportunities for developers to deploy mobile applications dynamically on a scalable on-demand hardware and software platform. It includes some unique features, such as a complete end-to-end infrastructural solution with enough computation and storage resources as well as no maintenance responsibilities (see Figure 1). All these features take into account the need for economies of scale by parties that wouldn't be able to afford them otherwise. Companies like Salesforce, Oracle, Amazon, Google, and IBM have found this model lucrative and have each created a cloud division within their respective organizations. Machine virtualization techniques have been deployed to provide flexible

Nidhi Rastogi: Rensselaer Polytechnic Institute
Marie Joan Kristine Gloria: Rensselaer Polytechnic Institute
James Hendler: Rensselaer Polytechnic Institute

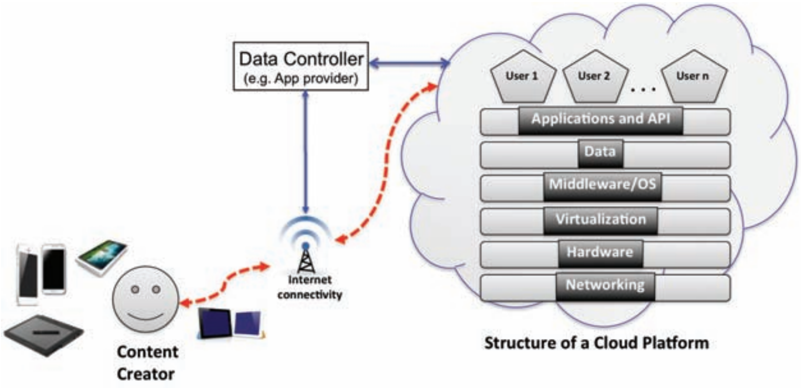


FIGURE 1 The cloud ecosystem.

and cost-effective resource sharing for users both internal and external to the organization. This has encouraged individual developers and small size companies, like Dropbox, to create cloud platform–oriented services and products that are interesting to the end user.

This emergence has led to the quicker delivery of many user-friendly applications to the market, while proving to be a commercially viable option to companies with limited resources. On the technology front, the creation and adoption of this ecosystem has allowed easy collection of mass data from various sources in one place; this "place" is commonly referred to simply as the "cloud." Efficient data mining can be performed on data stored in the cloud to extract potentially useful information, an avenue unexplored at this scale before. As an example, targeted advertising has been known to help many businesses understand consumer behavior. However, data privacy concerns have thwarted the pace of its deployment. The user, who entrusts the cloud service provider (CSP) with personal data, is also expected to extend this trust to third parties on matters related to its access. The platform thus acts like a "black-box" where the CSP is largely in control of gigabytes of user information. This information can range from highly sensitive to publicly available. Concerns are raised when parties that are interested in user-data analytics deploy artificial intelligence (AI) techniques, including machine-learning algorithms, to identify target audiences for various purposes, advertisements being one of them. This has negatively influenced the mindset of data owners, who are provided with no guarantees by the CSPs that further usage of their data is prohibited.[1] Hence, it is difficult for the consumer to believe that the service provider will not share data covertly to a party outside of the original usage agreement.

A strong enabler for preventing unauthorized access of information is encryption. This encodes data of all types into a format that is readable only to authorized parties. Among all the encryptions that aim to maintain data privacy, homomorphic encryption is a suitable solution.[2] Another similar mechanism called parallel homomorphic encryption (PHE) supports intensive computations via evaluation algorithms that can be efficiently executed in parallel.[3] Encryption allows computation on encrypted data within the cloud without having to decrypt it, thus preventing exposure to those who have no legitimate need for data access. However, like many other strong encryption schemes, these protocols come with the additional computational overhead of working on encrypted information. Although PHE is an improvement over homomorphic encryption in terms of faster computation, just like the homomorphic encryption, a lot of work is required to make it viable on a commercial scale.

Although there has been a lot of technical research worth mentioning toward realizing a feasible foolproof solution for preventing unauthorized data access, we redirect the reader's attention toward alternate ways of dealing with the problem. In this article, we suggest a three-pronged strategy to get a grip on this situation driven by: (a) technology, (b) internal policy and management, and (c) state and federal policies. Although our recommendation considers that technology is a powerful agent in preserving data confidentiality in a cloud setup, it is insufficient in providing a complete solution unless backed by appropriate practices. A sound privacy assessment of the cloud also requires transparent pro-user management practices and internal policies such as: (a) software that manages low-risk data cohabitates with those that have similar security needs; (b) a blueprint of threat modeling the cloud service—including software, hardware, and

[1] Chen, Deyan, and Hong Zhao, "Data Security and Privacy Protection Issues in Cloud Computing." In Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on, vol. 1, pp. 647–651. IEEE, 2012.

[2] Craig Gentry, "Fully Homomorphic Encryption Using Ideal Lattices," *Symposium on Theory of Computing (STOC)*, 9, (2009): 169–178.

[3] Seny Kamara and Mariana Raykova, "Parallel Homomorphic Encryption," in *Financial Cryptography and Data Security*, ed. Ahmad-Reza Sadeghi, 213–225. Berlin, Heidelberg: Springer, 2013.

data; and (c) a mechanism that addresses accountability concerns for protecting all data and controls the information used to grant access to the various parties. Lastly, we call for further exploration of external policies on both the state and federal level that offer limits and safeguards for the entire ecosystem. We submit these ideas in the hope that they may generate interest among policymakers, technologists, researchers, and industry professionals to consider potential practical steps toward better data management.

Literature Review

What follows is a brief literature overview of the existing privacy and security concerns related to the cloud platform. For this article, we define the various players in the ecosystem as follows: A cloud service is rendered over a network and can be accessed remotely through the Internet. A CSP is the entity that provides the cloud solution—including application, hardware platform, storage, and other resources. Using these resources is the data controller, which in our case is an entity that has access to end users' personal data of all kinds and in large quantities. This data may have been collected from the primary end user either through applications installed on various personal digital devices or through other means that collect user-generated content like photos, videos, documents, and so on.

A Bird's Eye View of Cloud Computing

The cloud computing platform truly emerged as a consumer-oriented computing paradigm in the early 2000s and soon it became a popular technology.[4] Increased bandwidth and flexible infrastructure comprising a heterogeneous offering of software and hardware supported the increasing use of cloud services. It promised, and delivered, a computation environment to users with varying needs, and later began to be distinguished as three definitive service models (see Figure 2): software-as-a-service (SaaS), platform-as-a-service (PaaS), and information-as-a-service (IaaS).

[4] Peter Mell and Tim Grance, "The NIST Definition of Cloud Computing," *National Institute of Standards and Technology*, 53, no. 6 (2009): 50.

Although there is no standard taxonomy defined, each model has been described based on the most common features covered:[5]

1. SaaS: All the software applications running on a cloud infrastructure are offered to users on-demand under the SaaS model. Also referred to as an application service provider (ASP), its end user gets access to these applications (apps for short) via a thin client or web-based interface on the user device. Some of the key providers are IBM, Salesforce, Oracle, and Microsoft. Cisco is steadily making inroads in application-centric infrastructure for simplified software deployment.
2. PaaS: A platform for building software applications is provided as a part of this service model. The developer, however, does not have access to underlying cloud services that may be modified using the interface. Microsoft's Azure is an example of this.
3. IaaS: In this model, computing resources such as processing, storage, and networks are provided to the user such that modifications can be made at the operating system and application level. Amazon Web Services (AWS) is the IaaS market leader with massive computational resources, aggressive pricing, and an expansive product line.

The vastly different needs covered by these service models are actuated by virtualization, which involves creating a virtual, efficient, isolated, duplicate version of cloud resources divided into multiple execution environments. This abstraction of resources is best made possible by technologies like hypervisor that create and run on virtual machines.[6] Other software, such as Apache Hadoop, allows large scale processing of data sets with a parallel, distributed algorithm on a cluster.[7]

[5] Hassan Takabi, James B.D. Joshi, and Gail-Joon Ahn, "Security and Privacy Challenges in Cloud Computing Environments," *IEEE Security & Privacy* 8, no. 6 (2010): 24-31; Kristin Bent, "The 20 Coolest Cloud Infrastructure, IaaS Vendors Of The 2014 Cloud 100," *CRN*, January 31, 2014, accessed September 3, 2014, http://www.crn.com/slide-shows/cloud/240165705/the-20-coolest-cloud-infrastructure-iaas-vendors-of-the-2014-cloud-100.htm; Gerald J. Popek and Robert P. Goldberg. "Formal Requirements for Virtualizable Third Generation Architectures," *Communications of the ACM*, 17, no. 7 (1974): 412–421.

[6] Arvind Seshadri, Mark Luk, Ning Qu, and Adrian Perrig, "SecVisor: A Tiny Hypervisor to Provide Lifetime Kernel Code Integrity for Commodity OSes," *ACM SIGOPS Operating Systems Review*, 41, no. 6 (2007): 335–350.

[7] Apache, "Hadoop," March 6, 2009, accessed September 1, 2014, http://hadoop.apache.org.

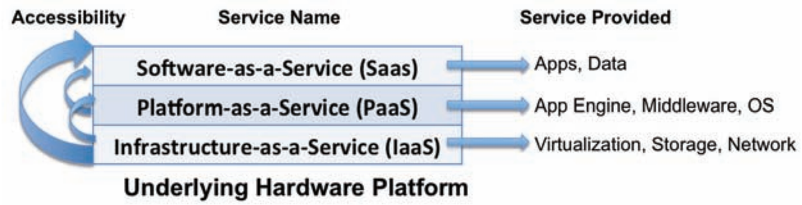

Accessibility
Service Name
Service Provided
Software-as-a-Service (Saas)
Apps, Data
Platform-as-a-Service (PaaS)
App Engine, Middleware, OS
Infrastructure-as-a-Service (IaaS)
Virtualization, Storage, Network
Underlying Hardware Platform

FIGURE 2 Cloud service models and services provided.

The "anywhere, anytime" capability of the Internet ensures a truly global solution for the cloud. Its infrastructure can be deployed using one of the following three models:[8]

1. Private: The cloud provider is the only user of the infrastructure. Organization users have exclusive access to resources, which are located within the premises (physical or virtual) of the company.
2. Public: A single organization provides multiple resources to multiple consumers, which is accessed via web services over the Internet. The overall system is located on-site or off-site, which a third party provider may manage.
3. Hybrid: It is a composition of two or more internal and external cloud providers that, although independent of each other, are bound by technologies that enable interoperability of data and applications.

Privacy: The Fundamentals

In this section, we provide a high-level overview of privacy's legal evolution. We also briefly discuss differences between US and European approaches to privacy. We recommend that those well versed in the fundamentals move on to the next section, which offers a more specified review in context of cloud computing.

Privacy means many things to many people. As such, this social issue is often surrounded by debate: *what is privacy* and *what does it mean*? These questions are informed by different philosophical approaches and theoretical views of privacy's value within a society. The most prominent of these is grounded in US liberal political theory, which places the liberal self as one with the "capacity for rational deliberation and choice."[9] Allen, on the other hand, posits that privacy enables positive liberties such that one is free from "unwanted disclosures, publicity and loss of control

[8] Mell and Grance, 3.

[9] Julie E. Cohen, "What Privacy Is For," *Harvard Law Review*, 126 (2013): 1904–1933.

of personality."[10] From these concepts, multiple theories have emerged that explain privacy in relation to autonomy, personhood, secrecy, liberty, and so on. Warren and Brandeis, in their seminal article "The Right to Privacy," set forth the notion of privacy as a "right to be let [sic] alone."[11] Some view privacy as accessibility to information about another person,[12] while others refer to the harms necessary to understand privacy violations.[13]

In 1973, the US Department of Health, Education, and Welfare introduced the Fair Information Practices (FIPs).[14] This set of defined principles has since helped inform how to evaluate and design systems that may impact individual privacy rights. This framework includes guidance on transparency, individual participation, purpose specification, data minimization, use limitation, data quality and integrity, security and accountability, and auditing.[15] As Schwartz notes, whenever information refers to an *identified* person, all FIP principles should be applied—an argument he later complicates with the introduction of *identifiable* data.[16] International adoption of FIPs is apparent within certain areas of the European Union's data protection plan, which include (but are not limited to) the presence of an independent data protection authority and limits on automated decision making.[17] FIPs are, therefore, critical components for both technical and legal considerations of cloud computing solutions.

In the United States, the legal regime assumes various, complex approaches to address privacy concerns. It should be noted that unlike the European Union, the United States does not have an omnibus information privacy statute. Instead, legal instruments, such as torts, statutes, and case law, are instantiated on the state, federal, and international levels. On the constitutional level, privacy issues challenge protections afforded by the First and Fourth Amendments. In particular, critics of regulating data

[10] Anita L. Allen, "Coercing Privacy," *William & Mary Law Review*, 40 (1999): 752.

[11] Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy," *Harvard Law Review*, IV, no. 5 (1890), accessed August 28, 2014, http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm.

[12] Allen.

[13] Daniel J. Solove, *The Digital Person: Technology and Privacy in the Information Age*, (2007).

[14] Alan Westin, "Records, Computers and the Rights of Citizens." U.S. Department of Health, Education & Welfare, December 1976, accessed September 15, 2014, http://files.eric.ed.gov/fulltext/ED143358.pdf.

[15] National Institute of Standards, "National Strategy for Trusted Identities in Cyberspace: Appendix A—Fair Information Practice Principles (FIPPs)," accessed August 29, 2014, http://www.nist.gov/nstic/NSTIC-FIPPs.pdf.

[16] Paul M. Schwartz, "Information Privacy in the Cloud," *University of Pennsylvania Law Review*, 161 (2012): 1654.

[17] Ibid. 1636.

collection cite that such policies interfere with and impede information flows, thus conflicting with the First Amendment.[18] For example, in *Sorrell v. IMS Health Inc.* (2011), the Supreme Court struck down (in a six to three decision) Vermont's prescription law.[19] The court held that the Vermont statute, which bars disclosure of prescription data for marketing purposes, violated the free speech rights of the data mining firms. The court determined that the prescriber-identifiable data was not fully protected speech, but instead, commercial speech; therefore, it could not be restricted based on the Central Hudson scrutiny test.[20]

In cases of the Fourth Amendment, privacy issues arise in defining a "reasonable expectation of privacy" (as introduced in *Katz v. United States* 389 U.S. 347 [1967]) and the need for a warrant to protect against unreasonable search and seizure by the government. Most notably, the Electronic Communications Protection Act (ECPA) has recently resurfaced in Congress due in large part to increasing criticism of its outdated and insufficient alignment with modern technologies.[21] Comprised of three separate federal statutes—the Stored Communications Act, the Pen Register Statute, and the Wiretap Act—its original intent was to expand Fourth Amendment protections in light of emerging computer technologies, like e-mail. Unfortunately, technology has evolved substantially over the last decade making the act irrelevant and ill-suited as a governing protocol. We discuss further implications of the ECPA as it relates to cloud services in the next section.

State-level statutes to protect consumer data also run the gamut. In some cases, state level protections of privacy are codified within state constitutions, which expressly recognize privacy as a right (e.g., Alaska, Arizona, California, Hawaii, Illinois, Louisiana, Montana, South Carolina, and Washington). According to the National Conference

[18] Solveig Singleton, "Privacy as Censorship: A Skeptical View of Proposals to Regulate Privacy in the Private Sector," *Cato Policy Analysis,* no. 295, accessed August 28 2014, http://www.cato.org/pub_display.php?pub_id=1154.

[19] Vermont State Legislature, "Act Relating to Increasing Transparency of Prescription Drug Pricing and Information," Vt. Stat. Ann. tit. 18, § 4631 (2007), accessed August 28, 2014, https://epic.org/privacy/ims_sorrell/epic_amicus.pdf.

[20] *Central Hudson Gas & Electric Corp. v. Public Service Comm. of New York,* 447 U.S. 557 (1980), accessed August 29, 2014, https://supreme.justia.com/cases/federal/us/447/557/case.html. (Commercial speech can be limited if: [1] truthful and non-misleading; [2] is in support of a substantial government interest; [3] directly advances the government interest asserted; and [4] is not more extensive than necessary to serve that interest.)

[21] *Electronic Communication Privacy Act,* U.S. Code 18 (1986; 2006) U.S.C. §§ 2510–2522, 2701–2712; Center for Democracy & Technology, "Updating ECPA," CDT, accessed August 28, 2014, https://cdt.org/campaign/updating-ecpa/.

of State Legislatures (NCSL), at least 30 states have enacted laws that specify how entities handle personally identifiable information (PII) collected by businesses and governments. These laws include requirements on how to destroy and dispose of PII as well as security breach notification laws and identity theft statutes.[22] In 2013, California enacted the Privacy Rights for California Minors in the Digital World (SB 568), permitting users under the age of 18 to delete or remove content posted online (effective January 1, 2015).[23] According to the bill, website operators must permit a minor who is a registered user to either remove or request removal of information posted on his or her site under the "eraser" provision outlined in Section 22581.[24]

Given the amount of regulatory provisions available, one could conservatively argue that privacy issues in the United States are diminishing. However, despite these numerous legal layers, information privacy remains at risk of being compromised. Schwartz notes that such shortcomings are a result of the law's static nature and inadequate incentives for the multiple parties who manage and store personal data to provide appropriate security and privacy protections.[25] We go further to suggest that the current use of sectoral laws and their narrowly applied approach leaves significant gaps in regulating highly distributed, modular technologies, like cloud services.[26]

Complicating Privacy Policies and the Cloud

As we've outlined thus far, state, federal, and international information privacy policies vary on many different levels. Yet, they all share the challenge of keeping pace with technological advancements. Legal issues of regulating cloud services are already emerging. Kesan et al. distill current legal issues into two categories in the context of cloud computing: data use and procedural issues.[27] Data use includes (but is not limited to) scraping or mining of data, use of public or private information, and the transfer of data. Kesan notes that in most data collection instances, privacy protection

[22] National Conference of State Legislatures, "Privacy Protections in State Constitutions," NCLS, December 11, 2013, accessed August 26, 2014, http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-protections-in-state-constitutions.aspx.

[23] California State Law, "SB-568: Privacy: Internet: Minors; Chapter 336," September 23, 2013, accessed August 27, 2014, http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB568.

[24] Ibid.

[25] Schwartz, 1624.

[26] Ibid., 1649.

[27] Kesan, Hayes, and Bashir, 365.

is unclear due to unsettled notions of whether it should prioritize the quantity of data or types of data.[28] Schwartz pushes further, suggesting that changes in personal data processing have challenged traditional notions of jurisdiction, definitions of PII, and contract law.[29] He identifies three areas of change in personal data processing due to cloud technologies: (1) the nature of information processing as increasingly international; (2) the multidirectional nature of modern data; and (3) the process-oriented management approach, which outsources computing processes in exchange for specialization of service.[30]

As an example of the tensions between the current legal regime and cloud services, we turn our attention back to ECPA, specifically to the Stored Computer Act (SCA) section. When the US Congress enacted ECPA and SCA in 1986, it did so notably within the context of its own technological perspicacity. Kattan summarizes:

> As originally enacted, the SCA attempted to balance the interests of law enforcement against individual privacy rights by dictating the mechanisms by which the government could compel a particular service provider to disclose communications stored on behalf of its customers.[31]

Sections §2702 and §2703 of the SCA specifically address when and why providers may voluntarily disclose information to others and ways in which the government may compel a provider to disclose information, respectively.[32] The SCA also identifies two types of services: electronic communication services (ECS) and remote computing services (RCS). This differentiator is key in determining whether certain communications are in "electronic storage" versus just in "storage."[33] Orin Kerr offers three reasons that challenge the notion of why strong privacy protections online may not extend to the "virtual homes" in cyberspace.[34] First, Kerr speaks

[28] Ibid., 367.

[29] Schwartz, 1628–1632.

[30] Ibid.

[31] Ilana R. Kattan, "Cloudy Privacy Protections: Why the Stored Communications Act Fails to Protect the Privacy Communications Stored in the Cloud," *Vanderbilt Journal of Entertainment & Technology*, 13, no. 3 (2011): 617–656.

[32] *Stored Communications Act*, 18 U.S.C. (2006), § § 2703(a)–(b).

[33] Kesan, Hayes, and Bashir, 402.

[34] Orin S. Kerr, "A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It," *George Washington Law Review* 72, no. 6, (2004): 3. Accessed August 29, 2014, http://courses.ischool.berkeley.edu/i205/s10/readings/users-guide-SCA.pdf.

directly to expectations of privacy online and the role of third parties like Internet service providers (ISPs); second, he also recommends a review of the rules governing grand jury subpoenas; and third, he recognizes ISPs as private actors, which means that strong protections are not extended under the Fourth Amendment.[35] Whether CSPs presumably fall under the RCS category or are identified as private actors (like ISPs) remains unclear under the current Act and its language. For e-mail service, which may be "stored" on the cloud, the government would only need a subpoena to compel the sharing of such information.

More perplexing legal issues surface when data is transferred across servers, state lines, and international borders. Kesan writes that the question over jurisdiction of data on the cloud surfaces due to "(1) the lack of borders in cyberspace; and (2) the vast differences between privacy laws in different locations."[36] In the United States, information privacy law does not provide government officials with the authority to block international transfers of personal information. It also does not offer any laws to regulate the processing of information unless specifically forbidden by law or regulated through other parameters.[37] Because of these jurisdictional challenges, the Terms of Service (ToS) agreements between CSPs and their customers carry the burden of outlining where the data is stored and which laws apply.[38]

To illustrate the complexity of jurisdiction in the context of CSPs, we turn to the ongoing litigation over whether Microsoft must comply with a warrant authorizing the search and seizure of e-mail accounts hosted by the company.[39] Since 2013, Microsoft has objected to the warrant, citing that the US courts are not authorized to issue warrants for "extraterritorial searches." Defined in *Morrison v. National Australian Bank Ltd.*, the doctrine holds that the "legislation of Congress, unless a contrary intent appears, is meant to apply only within the territorial jurisdiction of the United States."[40] In this case, Microsoft's argument hinges on the physical location of the data (stored in Ireland), while the government's rebuttal reasons that Microsoft is subject to US jurisdiction;

[35] Ibid., 4–5.

[36] Kesan, Hayes, and Bashir, 368–369.

[37] Schwartz, 1636–1637.

[38] Kesan, Hayes, and Bashir, 369.

[39] Christopher Kuner, "U.S. Warrants for Overseas Data Trample Foreign Privacy Laws," *MIT Technology Review*, August 22, 2014, accessed August 26, 2014, http://www.technologyreview.com/view/530316/us-warrants-for-overseas-data-trample-foreign-privacy-law.

[40] *Morrison v. Nat'l Austl. Bank Ltd.,* 561 U.S. 247, 248 (2010).

therefore, where the data is stored is irrelevant. Recently affirmed by Judge Loretta A. Preska of the US District Court for the Southern District of New York, the decision highlights unresolved tensions over jurisdiction because of conflicting international privacy law and technology outpacing policymaking. Moreover, as Kuner astutely points out, this particular discourse lacks any insight for potential safeguards for the consumers and users of services like Microsoft's e-mail application.[41]

As cloud services grow, it is evident that current legal standards and regulations will need to be reformed. For some, to do so may require both legislative and FCC action.[42] Others suggest increased transparency by cloud providers as one solution. We contend, however, that policy alone cannot shoulder the entirety of preserving privacy. Instead, legal and policy reform requires a reconceptualization of contemporary data management flows and a shared investment with industry and technology. Next, we offer additional perspectives that move toward a fuller understanding of privacy issues within the current cloud offering.

Putting it Together: Security and Privacy Concerns in the Cloud

In this section, we discuss security and privacy concerns that have significantly affected the deployment of the cloud platform.

Unauthorized Data Sharing

Multi-tenancy is a part of the public or community cloud offering with the ability to roll out services to multiple users simultaneously. This supports reduced overhead and higher availability of applications for the provider through solutions management. For instance, the ZFS storage capabilities,[43] along with hypervisors, offer customized solutions down to choosing the software version, thus encouraging a modular and parallel approach. Takabi et al. further elaborate that among the unique features of the cloud is its ability to manage resource utilization efficiently by offering a partitioned virtualized space for every customer subscribed to the service.[44] This multi-tenancy is

[41] Kuner.

[42] Kevin Werbach, "The Network Utility," *Duke Law Journal*, 1761 no. 60 (2011).

[43] Mark Peters, "Oracle ZFS Storage Software," Oracle, September 2003, accessed September 3, 2014, http://www.oracle.com/us/products/servers-storage/storage/nas/esg-brief-analyst-paper-2008430.pdf.

[44] Takabi, Joshi, and Ahn.

partially responsible for bringing the overall cost of the infrastructure down, which is why it is a great provision on behalf of the provider.

At one point during the cloud's market growth, multi-tenancy was driven by technology available at the time. Multi-tenancy architecture was accessible at the application level. Since then, several large companies have driven a major innovation wave in the cloud space leading to mature technology in the hardware, software, and virtualization space. Hence, multi-tenancy in the same storage space is no longer a means of true cost reduction. An upgrade from this solution is, however, not a priority with some companies, including Oracle.[45] The need to move to anything else has been found to be unwarranted and in opposition to their business values. Although saving an enormous amount of money, time, and human resources in creating the infrastructure from scratch is clearly an attractive offer, profit making is still the primary goal. However, prioritizing profits over the quality of the product wouldn't allow sustainability for too long. As a customer, allowing one's data to reside on a multi-tenant platform poses several privacy and security related challenges. We will discuss some of these challenges shortly.

Another big privacy concern is data being accessed by the service provider itself. The rationale is straightforward; there is a huge demand for data of all kinds in the Internet community. Many companies earn their livelihood by analyzing this data and selling it to interested parties at profitable rates. Platform owners usually have access and control over data inhabiting in any part of the platform, and they may take advantage of being in this unique position. If big data analytics has given data controllers the power to extract interesting analysis from the datasets, it has also increased avenues of privacy violations. The rationale behind using the cloud as a service comes understandably from reduced setup and operational costs, increased computational performance, elastic scalability, and so on. This has been made possible by various service models including software (SaaS), platform (PaaS), and infrastructure (IaaS) that are offered through convenient and affordable pricing models.

The current technological barriers focus only on providing security measures in the conventional sense. Some of these are described in the following section.

[45] Kathryn Perry, "Multi-Tenancy and Other Useless Discussions," Oracle Applications Blog, July 12, 2012, accessed September 3, 2014, https://blogs.oracle.com/applications/entry/multi_teanancy_and_other_useless.

Cloud Platform–Related Attacks

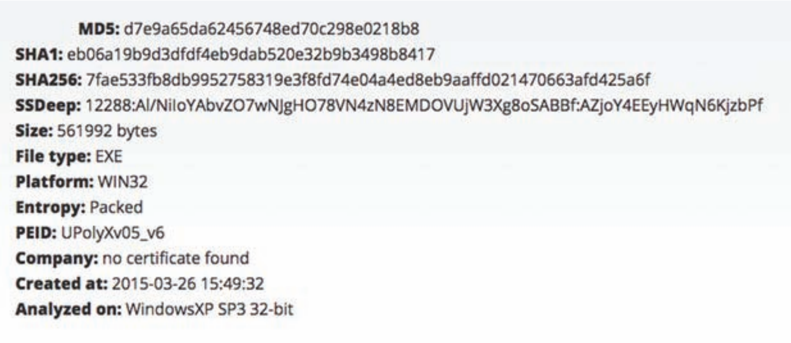
CSPs are the current favorite targets of cyber criminals, and we can expect to see more sophisticated attacks emerge in the future.[46] They attract cyber criminals just as banks attract robbers. A database located in the cloud is similar to an information bank with many customers, and cyber criminals are interested in using this data malevolently or in other unauthorized ways. Therefore, attacking a CSP exposes an entirely new and unconventional family of attack surfaces on the platform. These vulnerabilities, and those implicit to other components of the infrastructure, lead to many security gaps that adversaries can deploy in their favor. As an effort to thwart the efforts of the adversary or attacker, the security expert can take several measures.

The security personnel should understand attacks that are specifically geared toward the cloud platform. It is possible to assign the responsibility of securing the system to someone with experience in protecting enterprise networks. There is definitely a basic skill that both should possess—the ability to configure, design, and break security of systems.[47] Certifications from Cloud Security Alliance, Microsoft, Cisco, SANS, and many other certification providers help significantly in getting hands-on experience by means of laboratory sessions and theory classes. These certifications usually provide a satisfactory understanding of how various security systems work and of the common attacks and protection mechanisms. This understanding can be applied safely to many systems and can also be upgraded as technology advances. Various blogs, threat reports by security firms, and other organizations can keep one current with new threats on the horizon. Enough detail is provided about each threat and that progressively enhances the knowledge base of the evolving threats landscape. Figure 3 provides an example of a malware threat seen on a security blog recently.[48]

[46] "McAfee® Labs 2014 Threats Predictions," McAfee Reports, January 1, 2014, accessed September 3, 2014, http://www.mcafee.com/us/resources/reports/rp-threats-predictions-2014.pdf.

[47] Bruce Schneier, "So You Want to Be a Security Expert," Schneier on Security, July 5, 2012, accessed September 3, 2014, https://www.schneier.com/blog/archives/2012/07/how_to_become_a_1.html.

[48] Alexander Adamov, "NRGBOT," LAVASOFT, July 19, 2013, accessed September 3, 2014, http://www.lavasoft.com/mylavasoft/malware-descriptions/blog/nrgbot.



MD5: d7e9a65da62456748ed70c298e0218b8
SHA1: eb06a19b9d3dfdf4eb9dab520e32b9b3498b8417
SHA256: 7fae533fb8db9952758319e3f8fd74e04a4ed8eb9aaffd021470663afd425a6f
SSDeep: 12288:Al/NiloYAbvZO7wNJgHO78VN4zN8EMDOVUjW3Xg8oSABBf:AZjoY4EEyHWqN6KjzbPf
Size: 561992 bytes
File type: EXE
Platform: WIN32
Entropy: Packed
PEID: UPolyXv05_v6
Company: no certificate found
Created at: 2015-03-26 15:49:32
Analyzed on: WindowsXP SP3 32-bit

FIGURE 3 Example of a worm description.

Using similar skills and a sound understanding of the cloud infrastructure, security personnel may feel sufficiently equipped against known threats. The attack scenarios do not, however, completely overlap in the two environments.

We could write countless papers if one were to cover existing and potential attacks implicit to cloud platforms. But our goal is to take a systemic approach and provide mechanisms to protect the overall infrastructure instead of just focusing on safety measures through security-related approaches. Our approach is novel because it explores pragmatic ways to inform the primary user of the system's capability to store data securely and in a measurable way. We recognize that the complexity of these attacks will increase as the systems continue to evolve and provide increased functionalities. Heterogeneity of constituent systems and the software binding them will also increase overall attack surfaces. With this evaluation, we propose our solution in the next section.

Main Contributions

Cloud security implementers are in a prime position to develop privacy-preserving technologies to protect unlawful access of data. This is the foremost step to gain data controllers' trust for sharing data with CSPs. But, it does not offer a foolproof solution guaranteeing privacy and security of all data. Much is dependent on the environment in which the solution is implemented. A strong data encryption technique will protect the data from certain types of malicious intentions and approaches. There are other facets of illegal data access that necessitate new ways of protection.

Our thesis revolves around the idea of binding the distinct approaches of a technologist, a policymaker, and a business owner into a combined, cohesive perspective through a secure service. Each dimension brings a critical assessment to the table but cannot guarantee a complete solution individually. In this section, we will evaluate each approach separately. Later, we propose a unified cohesive solution.

The Technologist's Approach

Users of cloud services usually range from individual software application developers to small-business owners who have at least a few thousand customers. Large corporations may also take advantage of the cloud to offload, conservatively speaking, part of their system. As mentioned in the article earlier, cloud-computing infrastructure is still maturing and much work needs to be done on several frontiers—security and privacy of data being one of them. If proper data protection is not guaranteed for users, loss and exposure will ensue even in a protected premise.[49] In light of the data privacy–related attacks we discussed in the previous section, we recommend performing a threat analysis of the overall system as a mandatory exercise. As we explain later, the mandate must be one assumed by the company itself and not instigated from a public policy side.

Systems change configuration with each addition or removal of a hardware or software object. With the elasticity of resources that a cloud provides, a comparative threat analysis with each major upgrade will definitely offer key insights into gaping security holes and new privacy concerns resulting from the change. Before we discuss the performance of a security threat analysis, we first need clarity of its meaning.[50] A commonly accepted definition of threat, factors that create threat to a system, and ways of measuring different types of threat will be advantageous in delivering effective assessment results. For the purpose of this article, we define a threat as "anything that is capable of acting in a manner resulting

[49] Diana Kelley, "How Data-Centric Protection Increases Security in Cloud Computing and Virtualization," *Security Curve*, July 19, 2013, accessed September 3, 2014, https://cloudsecurityalliance.org/wp-content/uploads/2011/11/DataCentricProtection_intheCloud.pdf.

[50] Mouad Lemoudden, Ben N. Bouzza, Bouabid El Ouahidi and D. Bourget, "A Survey of Cloud Computing Security Overview of Attack Vectors and Defense Mechanisms," *Journal of Theoretical & Applied Information Technology*, 53, no. 2 (2013): 325–330.

in harm to an asset and/or organization; for example, acts of God (weather, geological events, etc.); malicious actors; errors; failures."[51]

This clarification will help to avoid unforeseen incidents, as its impact has been realized and remedies planned in advance. It is often useful to define many separate threat models for a given system. Each model defines a narrow set of possible concerns to focus on. In the case of cloud services, possibilities of both a security breach and un-handled privacy need to be modeled. This exercise can help to assess the probability of attacks, the potential means of harm, and the significance given to stored data, and thus help limit customer concerns.

Threat modeling has the potential to become an integral part of the process where privacy and security are relevant concerns. Some of the questions that need to be answered are the following:

1. What types of attacks need to be modeled in a cloud environment?
2. What does threat modeling mean for a cloud platform?
3. What tools and technologies can be used to accomplish the modeling task?
4. Will threat modeling help in creating an insurance plan when a data breach takes place?
5. How can a CSP share the threat model with the customer in a readable format?

There are some existing tools that can be used to perform threat modeling for any asset that needs protection. Bruce Schneier developed attack trees, which is a way of thinking and describing the security of systems and subsystems.[52] A list of possible attack vectors is created for the entire system that helps make decisions regarding how to improve security.

The usability of threat modeling can be maximized if the security architect thoroughly understands the architecture of a general public cloud platform. Although individual cloud-based platforms offer a broad spectrum of technologies and services, this should in no way hamper the impact this systemic analysis will have on appraisal of existing security gaps and, hence, proposed solutions.

Another proposed solution is to cohabitate data with the same level of sensitivity and privacy needs. This first requires a classification of the

[51] The Open Group, "Risk Taxonomy," January 1, 2009, accessed September 3, 2014, http://pubs.opengroup.org/onlinepubs/9699919899/toc.pdf.

[52] Bruce Schneier, "Attack Trees," Schneier on Security and *Dr. Dobb's Journal.* December 1, 1999, accessed September 3, 2014, https://www.schneier.com/paper-attacktrees-ddj-ft.html.

various user data into pre-defined sensitivity levels. These levels can be based on existing federal- or state-defined policies, on cost incurred in case of a data loss, or they can even be user-designated. The ToS document can outline this agreement between the service provider and user. This proposition has the potential to increase trust on the management of privacy that safeguards databases with critical data. More resources can be deployed specifically for these systems as opposed to system-wide implementation of stronger security. To further reduce ambiguity, privacy and security concerns regarding data can be defined bearing the following points in mind:

1. Definition of data that needs protection.
   a. Who owns the data (individual/organization)?
   b. What information does the data contain?
2. Financial implications associated with data theft, unauthorized access, or loss.
3. Impact on owner of the data if a third party accesses the data in an unauthorized way.
4. Federal- or state-imposed restrictions on access of that data.
5. Time period for which the sensitivity of the data is maximal.
6. To elaborate further, some examples are as follows: Is the information related to a person's health records or does it contain sensitive information like Social Security number, passport number, driver's license number, or anything similar that can serve as unique identification of a person? Does the information pertain to a banking account? Further questions of this kind, if asked, can inform the service provider of the appropriate services needed to store and protect the data.

Policymaker's Approach

In this article, we examine privacy concerns and security protections of consumer data afforded by cloud technologies, public policies, and internal data management practices. As we've advocated throughout the article, a successful and secure cloud solution requires the integration of all three elements. From the policymaking perspective, we offer three recommendations: refocusing the Federal Trade Commission's (FTC) role; offering pro-privacy incentives; and re-prioritizing personally identifiable information as a spectrum.

Our first recommendation urges a reconstitution of baseline protections, similar to FIPs, that better map onto cloud platform data flows and prioritize consumer protection. We do not suggest a segmented, dedicated set of guidelines. Instead, we offer cloud services as a gold-standard use case from which such guidelines can be evaluated. In turn, industry and trade associations can then provide provisions to identify risk of loss for online fraud,[53] which we suggest can be displayed to consumers as a rating scale similar to the "energy star" logo.

Our second recommendation calls for stronger enforcement mechanisms and regulation of data control (e.g., data mobility, data withdrawal, secondary-use).[54] For some, the answer may be found in self-regulation via personal data control technologies. We, however, remain skeptical of this solution for three reasons. First, usable technical mechanisms that enable such control on the user/customer level are only beginning to emerge. Consider the development of decentralized personal data stores (PDS) or infomediaries (e.g., Mydex, MyInfoSafe, Singly), which are being marketed as repositories for personal data that give users full control and management of their data flow.[55] Although projections for the PDS market are optimistic (e.g., £1 billion by 2016 in the United Kingdom alone),[56] consumer adoption remains to be seen.[57] Second, a growing number of empirical studies suggest that personal control of data may not elicit rational behavior or good decision making by the user.[58] Lastly, end user self-regulation is ineffective if the legal standards are missing to protect consumers from unfair trade practices. Consider PDS users who in all technical aspects control their own data flows. Current privacy policies are unclear of how protection extends beyond the PDS system administrator and the owner of the data.

Currently, the US FTC is most widely recognized for influencing the development and enforcement of personal data regulations, policies, and industry/company practices. This includes oversight pertaining to a wide range of security and privacy policies, such as the Fair Credit Reporting Act (FCRA), the Gramm-Leach-Bliley Act (GLB), and the Children's Online

[53] Kesan, Hayes, and Bashir, 462.

[54] Ibid., 464.

[55] Arvind Narayanan et al., "A Critical Look at Decentralized Personal Data Architectures." arXiv:1202.4503 (2012).

[56] Ctrl+Shift. "Personal Data Stores". April 30, 2014, accessed 24 April 2015, https://www.ctrl-shift.co.uk/index.php/research/product/64.

[57] While some analysts would characterize Facebook as a type of PDS, we do not make the same classification here. Instead, we refer to PDS projects that emphasize complete user control of data distribution and collection regardless if the data is stored centrally or distributed.

[58] Alessandro Acquisti and Jens Grossklags, "Privacy and rationality in individual decision making." *IEEE Security & Privacy*, 2 (2005): 24–30.

Privacy Protection Act of 1998 (COPPA). In 2000, the FTC issued a report to Congress outlining its own condensed version of four core principles of privacy protection: notice/awareness, choice/consent, access/participation, and integrity/security. These have largely been criticized as being too narrow, focusing primarily on website privacy policies. Moreover, the FTC relies on its power to regulate unfair trade practices by filing complaints based on deceptive procedural practices. In 2014, the FTC brought enforcement actions against matters of over 130 spam and spyware cases and more than 40 general privacy lawsuits, including Snapchat, Inc., TRUSTe, Inc., Innovative Marketing, Inc., and so on.[59] While this work has brought progress, the FTC is limited in its utility in the absence of rule-making authority. We urge that in light of this limitation that both Congress and the FTC seriously consider the passage of general consumer privacy legislation. The White House's Consumer Privacy Bill of Rights (2012) offers a starting framework. Additionally, the FTC should—in collaboration with industry and trade associates—develop a set of metrics, similar to our suggested consumer risk of loss assessment rating.

As indicated previously, one critical weakness of US privacy law and regulation is the lack of incentive mechanisms for data controllers. Currently, data breaches or violations of specific policies (e.g., COPPA) result in monetary penalties. Yet, some have argued that these penalties do not go far enough to ensure consumer data protection. Thus, we ask whether other incentives may help generate a pro-privacy stance among such companies. One avenue may be the proliferation and adoption of the "public-benefit corporation" status. State-chartered, this status allows for corporations to allow a public benefit, in this case privacy, to be part of its charter purpose in addition to maximizing profits. The idea is to increase transparency and accountability of the company's efforts to protect said benefit for its customers and shareholders. On October 23, 2014, the "ad-free and never sell users' data" social networking startup, Ello, formalized its status as a b-corporation in what they noted was "the strongest legal terms possible."[60] This is a promising first step for other companies that seek to prioritize the protection of consumer data as part of their main

[59] Federal Trade Commission. (2014). "2014 Privacy and Data Security Update". n.d., accessed April 27, 2015, https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update2014/privacydatasecurityupdate_2014.pdf.

[60] Jacob Kasternakes, "Ello Becomes a Public-Benefit Corporation with Mandate Not to Sell Ads," *The Verge*, October 23, 2014, accessed October 27, 2014, http://www.theverge.com/2014/10/23/7049141/ello-becomes-public-benefit-corporation-mandates-no-ads.

service offerings. Yet, whether this will impact the business's bottom line or increase the user base remains unclear. Though, as consumers become more data literate, such distinctions should inform purchasing decisions. More importantly, such policies should encourage more transparent open data practices. To ensure the viability of this recommendation, it is first worth conducting a cost analysis for both the state and for the company in consideration.

In addition to an alternative corporate structure, policymakers and companies need to re-evaluate their understanding of *personally identifiable information*. First, as we've outlined thus far, all data (particularly in the cloud) should be considered to be the primary asset. Second, a plethora of research over the past decade has significantly challenged the boundaries of de-anonymization, thus complicating any formal definition of PIIs as outdated. However, like Schwartz and Solove, we too consider wholly discarding PIIs as a misstep. Instead, as they propose in their PII 2.0 model, privacy should be considered on a "continuum that begins with no risk of identification at one end, and ends with identified individuals at the other."[61] In many ways, this allows for specific contexts and events to help determine the sensitivity of particular data. For example, in medical use cases that may include third-party mobile applications, understanding the privacy spectrum for the data in use helps frame the legal safeguards that may need to be triggered.

From the Business Owners

The article concerns itself with the data management flow between two specific entities: the CSP and users. For our purposes, we have limited the "user" or data controller definition to include developers, start-ups, small-business owners, and so on. We, therefore, assume a level of technical proficiency and skill-set from the user. As such, we urge these users—small-business developers—to create and initiate the following steps (based on the earlier discussions): *generate a threat model* and *share a blueprint* in a layman format in addition to the ToS agreement.

Earlier, we offered the following questions to ask as one begins their modeling: What types of attacks need to be modeled in a cloud

[61] Paul Schwartz and Daniel J. Solove, "PII 2.0: Privacy and a New Approach to Personal Information," *Privacy and Security Report*, November 23, 2012, accessed August 27, 2014, http://docs.law.gwu.edu/facweb/dsolove/files/BNA-PII-FINAL.pdf.

environment? What does threat modeling mean for a cloud platform? What tools and technologies can be used to accomplish the modeling task? Will threat modeling help in creating an insurance plan when a data breach takes place? After creating this model, we advocate that business owners share their models with their users. This would serve as a supplemental document to the ToS agreement, which outlines specifics of the data management flow. A second document should also be provided that discusses insurances against data breaches or mismanagement of data. We equate such an approach to a landlord with multiple tenants. Each tenant receives documentation of the property that highlights certain types of information, like the security of an area and liability for lost or damaged property. By adopting these practices, both CSPs and data controllers are clear about their data practices from data sharing to reselling, storage, withdrawal, deletion, and so on. We believe that the onus lies on these entities to build and gain user trust, and that those users should demand nothing less than this level of transparency.

Conclusion: The Big Picture

In light of these discussions, we turn our attention toward recommendations and additional points of interest that will aid in securing personal data in the cloud. First and foremost, while technologies like strong encryption may be sufficient in protecting sensitive data, they are not the complete solution. What happens when data is breached? Who is held accountable and liable? What happens when the government wants the data for an investigation? Therefore, internal management policies and legal standards are needed. Thus far, this article has primarily focused on the CSP to data controller business relationship. Unfortunately, even at this level, the data management flow in the cloud is complex. As we, along with others, have stated, multi-tenant, multi-directional flows on the cloud complicate legal protections. How, then, can we move forward?

From an internal management perspective, one point of interest is the latest decision by Apple, Inc. to explicitly ban its developers from reselling health data collected using its HealthKit API to advertising platforms, data brokers, or information resellers.[62] Apple will, however, allow developers

[62] Megha Kedia, "TOS Update Bars Apple HealthKit Developers from Selling Personal Data to Advertisers," *Techie News UK*, August 30, 2014, accessed August 31, 2014, http://www.techienews.co.uk/9717410/tos-apple-healthkit-developers-personal-data-advertisers/.

to share health data (with user consent) with third parties for "medical research purposes." Since its announcement, several questions have already emerged: Will this encourage consumers to share more of their personal health data? How will this be appropriated internationally? For our purposes, we ask whether Apple's move helps fill in the gaps of HIPAA, which currently only bars private entities, like health providers and insurance companies, from communicating patient information to third parties. Could Apple's decision set the tone for future technology data practices for all companies? While we wait to see if others follow suit, we encourage policymakers and civil society to continue efforts to better structure current policies and statutes.

The future of privacy on the cloud remains uncertain. How private industry, consumers, and the government will approach the need to preserve data integrity will require a combined effort. The steps we have outlined here merely scratch the surface. As As we've reiterated throughout the article, each approach—technical, regulatory, or business—are insufficient solutions on their own. The key is to pursue a comprehensive and collective approach.

BIBLIOGRAPHY

Acquisti, Alessandro, and Jens Grossklags. "Privacy and Rationality in Individual Decision Making." *IEEE Security & Privacy*, 2 (2005): 24–30.

Adamov, Alexander. "NRGBOT." LAVASOFT. July 19, 2013. Accessed September 3, 2014. http://www.lavasoft.com/mylavasoft/malware-descriptions/blog/nrgbot.

Albanesius, Chloe. "Disney's Playdom Fined $3 Million for Violating Kids' Privacy." *PC Magazine*. May 16, 2011. Accessed August 28, 2014. http://www.pcmag.com/article2/0,2817,2385444,00.asp.

Allen, Anita L. "Coercing Privacy." *William & Mary Law Review*, 40 (1999): 752.

Apache. "Hadoop." March 6, 2009. Accessed September 2014. http://hadoop.apache.org.

Bent, Kristin. "The 20 Coolest Cloud Infrastructure, IaaS Vendors of the 2014 Cloud 100." CRN. January 31, 2014. Accessed September 3, 2014. http://www.crn.com/slide-shows/cloud/240165705/the-20-coolest-cloud-infrastructure-iaas-vendors-of-the-2014-cloud-100.htm.

California State Law. "SB-568: Privacy: Internet: Minors. Chapter 336." September 23, 2013. Accessed August 27, 2014. http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB568.

Cashmore, Pete. "Xanga Fined $1 Million for Violating Children's Privacy." Mashable. September 7, 2006. Accessed August 27, 2014. http://mashable.com/2006/09/07/xanga-fined-1-million-for-violating-childrens-privacy/.

Center for Democracy & Technology. "Updating ECPA." CDT. Accessed August 28, 2014. https://cdt.org/campaign/updating-ecpa/.

Central Hudson Gas & Electric Corp. v. Public Service Comm. of New York, 447 U.S. 557 (1980). Accessed August 29, 2014. https://supreme.justia.com/cases/federal/us/447/557/case.html.

Chen, Deyan, and Hong Zhao. "Data Security and Privacy Protection Issues in Cloud Computing." In Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on, vol. 1, pp. 647-651. IEEE, 2012.

Chester, Jeff. "Children's Privacy Advocates Praise FTC on Proposed Safeguards to Protect Children's Information Online." In Center for Digital Democracy press release. September 15, 2011. Accessed August 29, 2014. http://democraticmedia.org/childrens-privacy-advocates-praise-ftc-proposed-safeguards-protect-childrens-information-online.

Cohen, Julie E. "What Privacy Is For." *Harvard Law Review*, 126 (2013): 1904–1933.

Ctrl+Shift. "Personal Data Stores." April 30, 2014. https://www.ctrl-shift.co.uk/index.php/research/product/64.

Electronic Communication Privacy Act. U.S. Code 18 (1986; 2006) U.S.C. §§ 2510–2522, 2701–2712.

Electronic Privacy Information Center (EPIC). "COPPA's Provisions." EPIC. Accessed August 28, 2014. http://epic.org/privacy/kids/.

Electronic Privacy Information Center (EPIC). "Criticisms of COPPA." EPIC. Accessed August 28, 2014. http://epic.org/privacy/kids/.

Federal Trade Commission (FTC). "Path Social Network App Settles FTC Charge It Deceived Consumers and Improperly Collected Personal Information from Users' Mobile Address Books." FTC Press release. February 1, 2013. Accessed August 28, 2014. http://www.ftc.gov/news-events/press-releases/2013/02/path-social-networking-app-settles-ftc-charges-it-deceived.

Federal Trade Commission (FTC). "2014 Privacy and Data Security Update". n.d. https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2014/privacydatasecurityupdate_2014.pdf.

Gentry, Craig. "Fully Homomorphic Encryption Using Ideal Lattices." *Symposium on Theory of Computing* (*STOC*), 9, (2009): 169–178.

Kamara, Seny, and Mariana Raykova. "Parallel Homomorphic Encryption," in *Financial Cryptography and Data Security*, ed. Ahmad-Reza Sadeghi, 213–225. Berlin, Heidelberg: Springer, 2013.

Kasternakes, Jacob. "Ello Becomes a Public-Benefit Corporation with Mandate Not to Sell Ads." *The Verge*. October 23, 2014. Accessed October 27, 2014. http://www.theverge.com/2014/10/23/7049141/ello-becomes-public-benefit-corporation-mandates-no-ads.

Kattan, Ilana R. "Cloudy Privacy Protections: Why the Stored Communications Act Fails to Protect the Privacy Communications Stored in the Cloud." *Vanderbilt Journal of Entertainment & Technology*, 13, no. 3 (2011): 617–656.

Kedia, Megha. "TOS Update Bars Apple HealthKit Developers from Selling Personal Data to Advertisers." *Techie News UK*. August 30, 2014. Accessed August 31, 2014. http://www.techienews.co.uk/9717410/tos-apple-healthkit-developers-personal-data-advertisers/.

Kelley, Diana. "How Data-Centric Protection Increases Security in Cloud Computing and Virtualization." *Security Curve*. July 19, 2013. Accessed September 3, 2014. https://cloudsecurityalliance.org/wp-content/uploads/2011/11/DataCentricProtection_intheCloud.pdf.

Kerr, Orin S. "A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It." *George Washington Law Review*, 72, no. 6, (2004). Accessed August 29, 2014. http://courses.ischool.berkeley.edu/i205/s10/readings/users-guide-SCA.pdf.

Kesan, Jay P., Carol M. Hayes, and Massoda N. Bashir. "Information Privacy and Data Control in Cloud Computing: Consumers, Privacy Preferences, and Market Efficiency." *Washington & Lee Law Review*, 70 (2013): 365. Accessed August 27, 2014. http://scholarlycommons.law.wlu.edu/wlulr/vol70/iss1/6.

Kuner, Christopher. "U.S. Warrants for Overseas Data Trample Foreign Privacy Laws." *MIT Technology Review*. August 22, 2014. Accessed August 26, 2014.

http://www.technologyreview.com/view/530316/us-warrants-for-overseas-data-trample-foreign-privacy-law.

Lemoudden, Mouad, Ben N. Bouzza, Bouabid El Ouahidi, and Daniel Bourget, "A Survey of Cloud Computing Security Overview of Attack Vectors and Defense Mechanisms." *Journal of Theoretical & Applied Information Technology*, 53, no. 2 (2013): 325–330.

Martin, Timothy D. "Hey! You! Get Off My Cloud: Defining and Protecting the Metes and Bounds of Privacy, Security, and Property in Cloud Computing." *Journal of Patents & Trademark Office Society*, 92, (2010): 283–294.

"McAfee® Labs 2014 Threats Predictions." January 1, 2014. Accessed September 3, 2014. http://www.mcafee.com/us/resources/reports/rp-threats-predictions-2014.pdf.

Mell, Peter, and Tim Grance. "The NIST definition of cloud computing." *National Institute of Standards and Technology* 53, no. 6 (2009): 50.

Morrison v. Nat'l Austl. Bank Ltd., 561 U.S. 247, 248 (2010).

National Conference of State Legislatures. "Privacy Protections in State Constitutions." NCLS. December 11, 2013. Accessed August 26, 2014. http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-protections-in-state-constitutions.aspx.

National Institute of Standards. "National Strategy for Trusted Identities in Cyberspace: Appendix A - Fair Information Practice Principles (FIPPs)." Accessed Aug. 29, 2014. http://www.nist.gov/nstic/NSTIC-FIPPs.pdf.

Narayanan, Arvind, Solon Barocas, Vincent Toubiana et. al. (2012). "A Critical Look at Decentralized Personal Data Architectures." arXiv:1202.4503.

Nissenbaum, Helen. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, CA: Stanford University Press, 2010.

The Open Group. "Risk Taxonomy." January 1, 2009. Accessed September 3, 2014. http://pubs.opengroup.org/onlinepubs/9699919899/toc.pdf.

Perry, Kathryn. "Multi-Tenancy and Other Useless Discussions." Oracle Applications Blog. July 12, 2012. Accessed September 3, 2014. https://blogs.oracle.com/applications/entry/multi_teanancy_and_other_useless.

Peters, Mark. "Oracle ZFS Storage Software." Oracle. September 2003. Accessed September 3, 2014. http://www.oracle.com/us/products/servers-storage/storage/nas/esg-brief-analyst-paper-2008430.pdf.

Popek, Gerald J., and Robert P. Goldberg. "Formal Requirements for Virtualizable Third Generation Architectures." *Communications of the ACM*, 17, no. 7 (1974): 412–421.

Prosser, William L. "Privacy." *California Law Review*, 48 (1960): 389.

Schneier, Bruce. "Attack Trees." Schneier on Security and *Dr. Dobb's Journal*. December 1, 1999. Accessed September 3, 2014. https://www.schneier.com/paper-attacktrees-ddj-ft.html.

Schneier, Bruce. "So You Want to Be a Security Expert." Schneier on Security. July 5, 2012. Accessed September 3, 2014. https://www.schneier.com/blog/archives/2012/07/how_to_become_a_1.html.

Schwartz, Paul M., and Daniel J. Solove, "PII 2.0: Privacy and a New Approach to Personal Information." *Privacy and Security Repor*t, November 23, 2012. Accessed August 27, 2014. http://docs.law.gwu.edu/facweb/dsolove/files/BNA-PII-FINAL.pdf.

Seshadri, Arvind, Mark Luk, Ning Qu, and Adrian Perrig. "SecVisor: A Tiny Hypervisor to Provide Lifetime Kernel Code Integrity for Commodity OSes." ACM SIGOPS. *Operating Systems Review*, 41, no. 6 (2007): 335–350.

Singleton, Solveig. "Privacy as Censorship: A Skeptical View of Proposals to Regulate Privacy in the Private Sector." *Cato Policy Analysis*, no. 295. Accessed August 28 2014. http://www.cato.org/pub_display.php?pub_id=1154.

Solove, Daniel J. *The Digital Person: Technology and Privacy in the Information Age*. New York: New York University Press, 2007.

Solove, Daniel J. "Identity Theft, Privacy and the Architecture of Vulnerability." *Hastings Law Journal*, 54, p. 1227 (2003). Accessed August 28, 2014. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=416740.

Stored Communications Act. 18 U.S.C. (2006), § § 2703(a)–(b).

Takabi, Hassan, James B.D. Joshi, and Gail-Joon Ahn. "Security and Privacy Challenges in Cloud Computing Environments." *IEEE Security & Privacy*, 8, no. 6 (2010): 24–31.

Vermont State Legislature. "Act Relating to Increasing Transparency of Prescription Drug Pricing and Information." Vt. Stat. Ann. tit. 18, § 4631 (2007). Accessed August 28, 2014. https://epic.org/privacy/ims_sorrell/epic_amicus.pdf.

Warren, Samuel D., and Louis D. Brandeis. "The Right to Privacy." *Harvard Law Review*, IV, no. 5. (1890). Accessed August 28, 2014. http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm.

Werbach, Kevin. "The Network Utility." *Duke Law Journal*, 1761, no. 60, (2011). Accessed August 28, 2014. http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1505&context=dlj.

Westin, Alan. "Records, Computers and the Rights of Citizens." U.S. Department of Health, Education & Welfare. December 1976. Accessed September 15, 2014. http://files.eric.ed.gov/fulltext/ED143358.pdf.