THE COLUMBIA
SCIENCE & TECHNOLOGY
LAW REVIEW

VOL. XVII STLR.ORG SPRING 2016

ARTICLE

FEDRAMP, CONTRACTS, AND THE U.S. FEDERAL GOVERNMENT'S MOVE TO CLOUD COMPUTING: IF AN 800-POUND GORILLA CAN'T TAME THE CLOUD, WHO CAN?[†]

Kevin McGillivray[*]

Despite the many advantages of cloud computing, moving IT services outside of an organization's physical boundaries means lost or reduced control over data and greater reliance on third parties. Risks associated with this loss of control are problematic for governments particularly as they relate to data privacy and data security. Given their position of public trust and responsibility for citizen data, governments occupy a complex role when using cloud services. The assumption that governments are able to effectively negotiate contracts with Cloud Service Providers (CSPs), and meet legal and organizational requirements, is widely championed. But is purchasing power enough? As the U.S. federal government is poised to be one of the largest purchasers and

* 2016 Kevin McGillivray. Doctoral Fellow, Norwegian Research Center for Computers and Law (NRCCL), Department of Private Law, University of Oslo (UiO). E-mail: kevin.mcgillivray@jus.uio.no. The author would like to thank his colleagues at the NRCCL and the Department of Private Law for their valuable comments on earlier drafts of this Article. This Article was written, in part, while working on the Confidential and Compliant Clouds (Coco Cloud) EU research project. COCO CLOUD, http://www.coco-cloud.eu. All hyperlinks are current as of February 20, 2016. Regarding the title, an "800-pound gorilla" is an American English expression for a person or organization so powerful that it can act without regard to the rights of others or the law. The phrase is rooted in a joke riddle: "Where does an 800-lb. gorilla sit?" The answer: "Anywhere it wants to." *800-pound Gorilla,* Wikipedia (July, 24, 2015), https://en.wikipedia.org/wiki/800-pound_gorilla.

consumers of cloud services, these questions are pertinent for the U.S. government in addition to governments across the globe considering similar moves.

The Article examines the adoption of cloud computing by the U.S. federal government and evaluates whether the U.S. cloud computing risk management program (FedRAMP) provides adequate tools to manage the risks associated with cloud computing. In evaluating FedRAMP, the Article examines legal requirements applicable to the federal government's use of cloud computing and assesses how legal requirements are reflected in the FedRAMP program. The Article further evaluates cloud procurement by federal agencies and considers whether the contracts that agencies have entered into with CSPs are consistent with FedRAMP and other legal mandates. The primary sources for this evaluation are agency audit reports and agency cloud computing contracts obtained through Freedom of Information Act (FOIA) requests. The Article places particular focus on missing contract terms or terms that are in conflict with either the requirements of the FedRAMP program or U.S. federal law. The legal focus of the Article is primarily contract and data privacy law.

I. INTRODUCTION

A recent awareness campaign by the Free Software Foundation Europe created a poster providing: "[t]here is no cloud – just other people's computers."[1] That message resonated with many across the web. The idea of placing data on a fluffy cloud gives users a certain feeling of comfort. However, the reality of the situation is that data stored on cloud computing infrastructures is done outside of the control of the data owner—requiring a great deal of reliance on the Cloud Service Provider (CSP) in determining where the data is stored and how it is secured. When that user is the United States (U.S.) government and the data the government is storing belongs to U.S. citizens, the need for careful planning and legal compliance increases sharply. The following Article evaluates cloud computing adoption by U.S. federal agencies and evaluates some of the technical risks and contractual challenges agencies face in their move to procure more cloud computing services. More importantly, the Article examines some of the questions the federal government ought to be asking before placing the personal data of U.S. citizens on someone else's computer.

Cloud computing is being billed as the future of Information Technology (IT) consumption. Advertisements for cloud computing can be found on television, plastered throughout airports, and are prominent in many technical and non-technical publications. Discussion of use and regulation of cloud computing has been widespread in both U.S. and Europe.[2] From legislative documents to U.S. Supreme Court decisions, the economic, social, and legal impact of the cloud phenomena is being widely evaluated.[3] Promises of cost savings, worldwide availability, and state-of-the-art computing services that can be purchased on an "on

---

1. FREE SOFTWARE FOUNDATION EUROPE (2015), http://download.fsfe.org/advocacy/stickers/thereisnocloud/thereisnocloud-v2-74x74.pdf.

2. *See, e.g.*, Vivek Kundra, OFFICE E-GOV'T & INFO. TECH., FEDERAL CLOUD COMPUTING STRATEGY (2011), https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/federal-cloud-computing-strategy.pdf; *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions*, COM (2012) 529 final, (Sept. 27, 2012).

3. *See, e.g.*, *Am. Broad. Cos. v. Aereo, Inc.*, 134 S. Ct. 2498 (2014). *See also Riley v. California*, 134 S. Ct. 2473, 2491 (2014) (discussing the impact of the ubiquity of cloud computing on police searches of mobile phones stated stating that "[c]loud computing is the capacity of Internet-connected devices to display data stored on remote servers rather than on the device itself. Cell phone users often may not know whether particular information is stored on the device or in the cloud, and it generally makes little difference.").

demand" basis are enticing to many users.[4] In addition to businesses and consumers adopting cloud computing, governments are also making changes in the way they consume IT.[5] In a time of reduced government spending and austerity measures, reduced tax revenues, and the ever increasing cost of IT solutions, many national and even local governments are finding cloud computing an attractive proposition. Accordingly, many governments either have an active strategy to adopt cloud computing or are crafting one.[6]

In the U.S., the reality of the current IT landscape is that federal agencies need IT services—and they want to pay much less for them. By leveraging off the advantages of cloud computing, the federal government aims to obtain the services it needs, but at a much lower cost than it is currently paying. Simply put, cloud computing provides an important tool for providing state-of-the-art IT at a lower cost. However, the cost of services is but one factor. Equally important, federal agencies using cloud computing will still need to meet complex regulatory requirements while also maintaining a high level of control and oversight over their data. The following Article evaluates aspects of the U.S. federal government's strategy to adopt cloud computing using the Federal Risk and Authorization Management Program (FedRAMP) to address the many risks associated with cloud computing. In evaluating FedRAMP, the Article examines legal requirements

---

4. WAYNE JANSEN & TIM GRANCE, NAT'L INST. OF STANDARDS & TECH., GUIDELINES ON SECURITY AND PRIVACY IN PUBLIC CLOUD COMPUTING 8–10 (2011) (providing that in addition to cost savings, cloud computing may offer increased security, specialized staff, greater platform strength, and improved backup and recovery, among other benefits).

5. Although the Article primarily focuses on U.S. federal level agencies, the terms "government" or "state" are used broadly to include adoption of cloud services by governments on the national, regional, agency, municipal, or local government level.

6. *See, e.g.*, Kundra, *supra* note 2. For example, in the United States (U.S.), the federal government is pursuing a "cloud first" strategy. European governments are also pursuing cloud computing although many nations are at a very early stage. Dimitra Liveri, & M.A.C Dekker, *Report of the European Union Agency for Network and Information Security on the Security Framework for Governmental Clouds*, (Feb. 26, 2015), https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/governmental-cloud-security/security-framework-for-govenmental-clouds. *See also* Morten Jørsum et al., *Nordic Public Sector Cloud Computing—a discussion paper*, (Nordic Council of Ministers 2012) (Den.), http://www.norden.org/en/publications/publikationer/2011-566 (evaluating cloud computing uptake and government strategies in Denmark, Finland, Iceland, Norway, and Sweden).

applicable to the federal government's use of cloud computing and assesses how legal requirements are reflected in the FedRAMP program.

This Article has five parts. Section one provides the introduction. In section two, the Article describes and analyzes the U.S. federal government's cloud computing strategy—FedRAMP. This section also evaluates key aspects of the legal framework that U.S. federal agencies must meet in order to comply with U.S. law. In section three, the Article considers practical examples of agencies adopting cloud and compliance challenges they have encountered under FedRAMP in meeting contract requirements. In section four, the Article evaluates revised contract terms at FedRAMP and individual agencies and considers a possible road forward. Section five provides the conclusion.

A. Cloud Computing Definition and Properties

At its core, cloud computing is a method of providing users with on-demand computing services over a network. Although an evolving definition, the classification of cloud computing by the National Institute of Standards and Technology (NIST) has been widely used in the U.S. and Europe.[7] The NIST definition provides "cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[8] There are various models available, some allowing broad access

---

7. For instance, the European Commission used this definition in its cloud adoption strategy. *See* European Comm'n, *supra* note 2, at 3 n.5. *See also Opinion of the Article 29 Data Protection Working Party on Cloud Computing*, at 25 n.50, WP (2012) 196 (July 1, 2012), http://ec.europa.eu/justice/data-protection/article29/documentation/opinionrecommendation/files/2012/wp196_en.pdf.

8. Peter Mell & Timothy Grance, NAT'L INST. OF STANDARDS & TECH., SPECIAL PUB. 800-145, THE NIST DEFINITION OF CLOUD COMPUTING 2–3 (2011). In Europe, the European Union Agency for Network and Information Security (ENISA) has provided the following definition for government clouds: "A Gov Cloud is an environment running services compliant with governmental and EU legislations on security, privacy and resilience (what). A Gov Cloud is a secure and trustworthy way (private Cloud or public Cloud) to run services under public body governance (how). A Gov Cloud is a deployment model to build and deliver services to state agencies (internal delivery of services), to citizens and to enterprises (external delivery of services to society) (for whom)." Liveri & Dekker, *supra* note 6, at 3.

by many users (public cloud). Others models are provided on a more limited basis (private or community cloud). In cloud computing, there are generally five major types of participants: the cloud consumer (cloud client), cloud provider, cloud carrier, cloud auditor, and integrator (cloud broker).[9] These parties do not always have distinct roles and may wear multiple hats in any given cloud service.[10]

When referencing different parties to cloud computing services, there is no uniformity in the terms used to reference parties in different jurisdictions. In the U.S., the term "cloud consumer" is often used.[11] This is problematic for legal experts that associate "consumer" with a non-professional living person, entitled to additional protections when entering into contracts.[12] In the context of much of this Article, the end-user or "consumer" of the services is the U.S. federal government, a party that clearly falls outside of a "non-professional party" designation. In the EU, the end-user of a cloud service is sometimes deemed a "cloud client."[13] Although arguably better for legal experts, this term is equally problematic for technologists as it has a specific and independent meaning regarding computer hardware accessible via server. To avoid confusion, when referencing a government user procuring cloud services, I use the term "cloud adopter" rather than "cloud consumer" or "cloud client."

Despite the many benefits, the use of cloud computing is not without risks from the user's perspective. Moving IT services

---

9. LEE BADGER ET AL., NAT'L INST. OF STANDARDS & TECH., SPECIAL PUB. 500-293, US GOVERNMENT CLOUD COMPUTING TECHNOLOGY ROADMAP VOLUME II RELEASE 1.0 (Draft): USEFUL INFORMATION FOR CLOUD ADOPTERS 19 (2011) (the NIST cloud computing reference architecture defines five major actors).

10. FANG LIU ET AL., NAT'L INST. OF STANDARDS & TECH., SPECIAL PUB. 500-292, NIST CLOUD COMPUTING REFERENCE ARCHITECTURE: RECOMMENDATIONS OF THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY 4 (2011).

11. *Id.*

12. *See, e.g.*, Directive 2011/83, of the European Parliament and of the Council of 25 October 2011 on Consumer Rights, 2011 O.J. (L304) 64, 72 (defining "consumer" as "any natural person who, in contracts covered by this Directive, is acting for purposes which are outside his trade, business, craft or profession").

13. *See, e.g.*, *Report of the European Network & Information Security Agency for Cloud Computing: Benefits, risks and recommendations for information security*, at 21 (Daniele Catteddu & Giles Hogben eds.) (Nov. 20, 2009), https://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment.

outside of an organization's physical boundaries leads to reduced control over data and greater reliance on third parties.[14] The CSP makes key decisions on central information management issues such as the physical location of the infrastructure, use of subcontractors, and security methods. Moreover, the CSP makes these decisions on a standard basis, regardless of an individual user's needs. The CSP's infrastructure is often on global scale, spread across many providers, the full extent of which may not be fully visible to the end-user. These factors bring additional security and privacy risks.[15] The multi-tenant infrastructure, which involves sharing resources with unknown users, increases these risks.[16] Additionally, security controls commonly used in traditional IT hosting to meet information confidentiality, integrity, availability, and privacy requirements may be unavailable in cloud computing.[17]

---

14. JANSEN & GRANCE, *supra* note 4, at 12.

15. Dan Svantesson & Roger Clarke, *Privacy and Consumer Risks in Cloud Computing*, 26 COMP. L. & SEC. REV. 391, 391–94 (2010). In addition to data loss and other privacy concerns, the movement to a more centralized structure may reduce user interactions, sharing of information, and ultimately collaboration and creation online. *See* David Lametti, *The Cloud: Boundless Digital Potential or Enclosure 3.0?*, 17 VA. J. L. & TECH. 190, 197 (2012). *See also* Primavera De Filippi & Miguel Said Vieira, *The Commodification of Information Commons: The Case of Cloud Computing*, 16 COLUM. SCI. & TECH. L. REV., 102, 105–06 (2014) (arguing that cloud computing technologies may be designed in a way that restricts the use of information to a greater degree than intended under copyright law).

16. JANSEN & GRANCE, *supra* note 4, at 11. Rather than actual physical separation (i.e., customer data being stored on different servers) the cloud relies on logical separation of data, which has vulnerabilities that can be exposed by malicious users. These include overcoming the logical separation mechanisms, allowing the malicious user to attack others in the shared infrastructure. Kevin McGillivray, *Conflicts in the Cloud: Contracts and Compliance with Data Protection Law in the EU*, 17 TUL. J. TECH. & INTELL. PROP. 217, 236 (2014) (discussing the case of Megaupload and the negative impact illegal acts of some users can have on all users on shared infrastructure).

17. JANSEN & GRANCE, *supra* note 4, at 10–12. Additional concerns with security and privacy in the cloud infrastructure include system complexity which creates a larger attach surface, movement from delivery of the service on a private intranet to deliver over the Internet—increasing access to attackers. These aspects of cloud computing create challenges for ensuring data integrity and availability. *See also* Scott Paquette et al., *Identifying the Security Risks Associated with Governmental Use of Cloud Computing*, 27 GOV'T INFO. Q. 245, 248–51 (2010) (providing that controls commonly used or available in traditional IT hosting to meet information security, confidentiality, and privacy requirements may be unavailable in the cloud computing environment).

By putting third-party CSPs in charge of these services, particularly for "mission critical" applications, the government is extremely dependent on CSPs when data outages or losses occur.[18] When a government moves to cloud, whether a municipality officers can answer their email, welfare applications can be processed, or bills can be sent to citizens may depend almost entirely on their CSP's response time instead of the governments IT department.[19] In some cases this is likely a positive change. When measuring CSPs "uptime" against traditional IT services, the cloud response is often impressive.[20] However, the reality of the situation is that for the public sector to perform its mandate, it relies heavily on a third-party.

B. Questions Surrounding States Contracting onto Cloud

In order to maximize the benefits of cloud computing, many CSPs offer their contract terms on a one-size-fits-all basis. For governments, the contract terms contained in these offers are generally unacceptable. Thus, many governments are adapting their procurement methods. In theory, governments are large enough purchasers of IT services that they ought to be able to effectively negotiate with CSPs. The U.S. federal government is poised to be one of the largest purchasers and consumers of cloud computing globally.[21] As the story goes, the disadvantages

---

18. Scott Paquette et al., *supra* note 17, at 251.

19. Denial of government services ranges in severity from the relevantly inconsequential instance such as a minor delay in registering a vehicle or delayed access to a website to being denied services. It is not difficult to imagine cases where core services become unavailable and losses of consequence occur resulting in harm to citizens and loss of confidence in government services. *See* State of Indiana v. Int'l Bus. Mach., 4 N.E.3d 696 (Ind. Ct. App. 2014).

20. *See, e.g.*, OFFICE OF AUDITS, OFFICE OF THE INSPECTOR GEN., NASA REPORT NO. IG-13-021, AUDIT REPORT: NASA'S PROGRESS IN ADOPTING CLOUD-COMPUTING TECHNOLOGIES 3–5 (2013). As part of NASA's Cloud-Computing Initiative it developed its own private-cloud called "Nebula." *Id.* at 3. In 2011, NASA tested Nebula against cloud services provided by Amazon and Microsoft to determine the system that provided the most stable and cost effective cloud platform. *Id.* at 5. This comparison determined that the services offered by Amazon and Microsoft "had matured to be more reliable and cost effective and offered much greater capacity and better IT support than Nebula." *Id.* NASA thus discontinued Nebula. *Id.*

21. Fed. Chief Info. Officers Council, Chief Acquisition Officers Council & Fed. Cloud Compliance Comm., CREATING EFFECTIVE CLOUD COMPUTING CONTRACTS FOR THE FEDERAL GOVERNMENT: BEST PRACTICES FOR ACQUIRING IT AS A SERVICE 2 (2012), https://cio.gov/wp-content/uploads/downloads/2012/09/cloudbestpractices.pdf (maintaining that "the Federal

commonly cited in the asymmetrical relationship typical between Small and Medium Sized Enterprises (SMEs) or consumers contracting with CSPs are not present—or are at least greatly reduced—when governments negotiate.[22] The assumption that governments are able to effectively negotiate contracts with CSPs, and meet legal and organizational regulatory requirements, is widely championed. But is purchasing power enough?

This Article challenges the assertion that purchasing power alone is a sufficient condition to obtain compliant cloud computing services—at least in the case of U.S. federal agencies. If other necessary conditions, such as adequate risk management, are not in place, the advantages gained by purchasing power may not result in obtaining a compliant system.[23] In other words, even with greater purchasing power, government agencies must plan sufficiently and appreciate where cloud computing diverges from traditional IT outsourcing services—starting with their understanding and application of the definition of cloud computing. For the U.S. government to leverage its purchasing power, federal agencies need tools, such as standardized contracts

---

Government holds the position as the single largest purchaser in this new market") [hereinafter "CIO Council"]. *See also* Avidan Y. Cover, *Corporate Avatars and the Erosion of the Populist Fourth Amendment*, 100 IOWA L. REV. 1441, 1474 (2015) (discussing extensive use of cloud computing in the U.S. federal government including "[a]t least 42,000 federal government employees and contractors" using Google Apps).

22. W. Kuan Hon, Christopher Millard & Ian Walden, *Negotiating Cloud Contracts: Looking At Clouds From Both Sides Now*, 16 STAN. TECH. L. REV. 79, 89 (2012) (providing that regulated industries, including government bodies and financial institutions, more often attempt to negotiate cloud contract terms to meet their needs). CHRISTOPHER J. MILLARD ET AL., CLOUD COMPUTING LAW 75 (Christopher J. Millard ed., Oxford University Press 2013) (stating that "[l]arge users such as governments are demanding more customer-friendly terms."). Alberto G. Araiza, Note, *Electronic Discovery in the Cloud*, 10 DUKE L. & TECH. REV. 1, 15 (2011) ("while powerful entities may successfully negotiate favorable terms of a contract, smaller or inexperienced clients may be subject to one-sided agreements").

23. MATTHEW METHENY, FEDERAL CLOUD COMPUTING: THE DEFINITIVE GUIDE FOR CLOUD SERVICE PROVIDERS 169–194 (Syngress 2012). In addition to systems to manage information security—the primary focus of FedRAMP—other risk management processes focus on legal risks that can be "treated by legal means." Tobias Mahler, *Defining Legal Risk*, *in* COMMERCIAL CONTRACTING FOR STRATEGIC ADVANTAGE - POTENTIALS AND PROSPECTS CONFERENCE PROCEEDINGS, 10 (Turku University of Applied Sciences 2007), http://ssrn.com/abstract=1014364.

and updated clauses or cloud-specific precedents, to adequately account for agency needs in cloud computing.[24]

The Article further considers how the U.S. government addresses the challenges of cloud computing through its cloud-specific risk management program. There are many legal issues that impact the use of cloud computing, including: consumer protection, intellectual property, data privacy, and contract law.[25] To emphasize these issues, this Article evaluates legal regulations and analyzes contract terms that may have an impact on the federal agency's ability to access data that is being stored with a CSP and thus impact the agency's ability to protect the privacy and integrity of citizen data. In its program, the U.S. government places significant attention on security and technical measures. However, in order to obtain cloud systems that are "fit-for-purpose" the government must also have adequate tools in place to manage risks—including clear contract standards. These issues have not received adequate focus.

In light of the challenges posed by cloud adoption, the Article analyzes the following questions: When governments become adopters of cloud computing, what legal or compliance obligations apply to their use of the services?[26] What are the main barriers for federal agencies procuring cloud computing—particularly in the areas of data privacy and data security? What tools do governments use or should they develop to meet the necessary legal obligations? In addressing these questions, the Article examines how the needs of governments *are* or *ought to be* expressed in the contracts governments enter into with CSPs. In addition to evaluating what *ought to be in the contracts*, the Article evaluates *what is included* in the contracts between U.S. federal agencies and CSPs. The question then becomes whether there is a compliance gap between what the procurement systems require and what the contracts actually contain. If so, what are the potential problems or risks created for citizen and government data?

---

24. *See infra* Section 5 (evaluating challenges faced by U.S. Federal Agencies).

25. *See, e.g.*, Hon, Millard & Walden, *supra* note 22, at 79.

26. Although this Article primarily considers the role of governments as users or consumers of cloud it is clear that states are also taking on roles separate from the role of consumer. For example, the U.S. government also acts as participant in standards development, regulator, and to some extent a cheerleader of the cloud computing market. Although these roles may also impact procurement of services, they remain beyond the scope of this Article.

Critical analysis on these points is undertaken primarily through evaluating agency audits and agency contracts obtained through requests made under the Freedom of Information Act (FOIA).[27] "From a legal perspective, the cloud embodies a new template for interactions: all interactions in the cloud—unlike those that occur purely via the Internet—are contract-based."[28] Understanding this "new template"—to the extent that it is novel—and how governments may use it to obtain secure and lawful cloud computing systems is therefore crucial in understanding the legal landscape facing all users of cloud computing.[29]

C. Public Actors Using Private Tools

Although moving in-house IT services to cloud computing is an increasingly popular goal for governments, many challenges currently stand in the way. In addition to the concerns held by private businesses and consumers, governments have additional obligations hindering uptake.[30] For example, governments represent citizens who are the beneficiaries of potential savings from cloud computing—but citizens also bear the burdens of

---

27. Public Information; Agency Rules, Opinions, Orders, Records, and Proceedings, 5 U.S.C. § 552 (2015) [hereinafter "FOIA"]. Contracts and other documents obtained through FOIA requests are on file with the author. Although requests were made for cloud computing contracts from all agencies audited by The Council of the Inspectors General on Integrity and Efficiency (CIGIE), not all agencies provided such agreements. *See infra* note 58. Additionally, the breadth of agency FOIA responses by agencies varied considerably. While some provided substantial disclosure of contracts, others provided heavily redacted information, contracts that did not match the dates of the audit, or were unable to located documents provided to auditors. Some agencies, such as the Environmental Protection Agency, simply did not respond. As a result, the author has been unable to independently verify some aspects of the internal audits conducted by governmental accountability offices and the CIGIE. The conclusions are therefore primarily based on government audits rather than contracts obtained pursuant to FOIA.

28. Damon C. Andrews & John M. Newman, *Personal Jurisdiction and Choice of Law in the Cloud*, 73 MD. L. REV. 313, 328 (2013).

29. DLA PIPER U.K. LLP, *Comparative Study on* Cloud Computing C*ontracts* 27, 29 (European Union 2015) (maintaining that "cloud contracts" are not generally seen as unique or a new category of contract and are therefore subject to the same general principles applicable to all contracts). However, legal scholars in some jurisdictions have categorized cloud computing contracts as "'sui generis contracts,' not regulated by the existing principles." *Id.* at 29.

30. Urs Gasser & David R. O'Brien, Research Pub. No. 2014-6, Governments and Cloud Computing: Roles, Approaches, and Policy Considerations 7–8 (The Berkman Ctr. for Internet & Soc'y at Harvard Univ. 2014), http:// ssrn.com/abstract=2410270 (select "Download This Paper").

government oversights in procurement and operation of cloud computing. Given their responsibility to the public, government actors are often required to provide a greater level of transparency in their procurement and operating processes.[31] However, cloud computing structure is often based on proprietary technology and does not lend itself to transparency. In addition to challenges posed by organization of the services, government users must also adapt to changes in contracting and procurement methods.[32]

When governments enter into the private ordering/contracting arena to obtain goods and services they are treated much like any other private party.[33] As succinctly stated by one author, "the government does not cease to be the government simply because it is placing a contract."[34] Governments obtain the same benefits or utility of contracting such as risk allocation and organization—but must also play by the rules of private ordering.[35] However, unlike private actors, governments often have additional requirements dictating aspects of their contracting processes. Some of these requirements—such as transparency and accountability—are not always easily met in contracting practices.

Even if governments are required to play by the same rules as private parties while contracting, they do not necessarily have all of the same tools at their disposal to mitigate risks adopted by private users. For example, in addressing a risk a CSP might be able to provide a contract term excluding warranties or liability, define

---

31. A. C. L. DAVIES, THE PUBLIC LAW OF GOVERNMENT CONTRACTS 41 (Oxford Univ. Press 2008).

32. CIO Council, *supra* note 21, at 2 (with changes in the way the government purchases IT moving from outsourcing to cloud computing comes a "learning curve" to effectively contract and procure cloud services). *See, e.g.*, Michael J. Brito, *Cloud Computing, Multi-Sourcing Create New Challenges in Outsourcing*, *in* INSIDE THE MINDS: BEST PRACTICES FOR MANAGING OUTSOURCING TRANSACTIONS 151 (Thomson Reuters 2014).

33. Wendy Netter Epstein, *Contract Theory and the Failures of Public-Private Contracting*, 34 CARDOZO L. REV. 2211, 2228 (2013) (providing that "public-private contracts will function like traditional commercial agreements and indeed the law treats these agreements essentially the same as traditional commercial agreements.").

34. DAVIES, *supra* note 31, at 88.

35. LEE A. BYGRAVE, INTERNET GOVERNANCE BY CONTRACT 38–39 (Oxford Scholarship Online 2015) (providing that contracts are useful in that they provide "glue for an agreement."). This is not to say that the U.S. federal government is by any means a "novice" when it comes to contracting with private providers. The U.S. government uses private contractors to provide services ranging from building maintenance to military operations in the battle field. Kimberly N. Brown, *Outsourcing, Data Insourcing, and the Irrelevant Constitution*, 49 GA. L. REV. 607, 617–18 (2015).

jurisdiction or law to a location more favorable to them, or even obtain insurance for risks that they cannot manage through security or other means. The types of risks governments face do not always lend themselves to the same degree of flexibility. Although there are situations where a state can simply write a check—or perhaps have an insurer do so—not all damages incurred by governments can be recompensed monetarily.

For governments, complications in procuring cloud-based services range from minor procedural to substantive legal issues such as accounting for and protecting the privacy rights of citizens.[36] On the procedural side, some challenges to the adoption of cloud computing by states are immediately apparent in the bidding and procurement processes. This may include, among other formalities, the requirement that bids be submitted in fixed prices. This makes comparing cloud computing, which often use "pay-for-use" or "pay-as-you-go" arrangements, difficult to equate with traditional outsourcing arrangements.[37] Although not necessarily "apples to oranges," it may leave mandatory boxes in the procurement application unchecked. Additionally, government users are often subject to publicly mandated computing and security requirements that may be difficult to account for in cloud computing.[38]

---

36. Marina Bregou et al., CLOUD SEC. ALL. & PROCUREMENT INNOVATION FOR CLOUD SERVICES. IN EUROPE, D3.1, *Procurement Barriers Report* 28–29 (Procurement Innovation for Cloud Serv. in Europe 2015) (European Union), http://www.picse.eu/sites/default/files/D3.1_Procurement_Barriers_Report_V12_28.05.2015_0.pdf (ranking the following issues as the greatest barriers to cloud adoption by EU governments: (1) "Lack of confidentiality assurance and IPR management", (2) "SLAs not clearly defined", (3) "Unclear privacy policies", (4) "Difficulties with defining requirements", (5) "Stringent legal and regulatory requirements").

37. PROCUREMENT INNOVATION FOR CLOUD SERV. IN EUROPE, *Procuring Cloud Services Today: Experiences and Lessons Learned from the Public Sector 1-3*. (Procurement Innovation for Cloud Serv. in Europe 2015) (European Union), http://www.picse.eu/sites/default/files/Procuring%20cloud%20services%20today_22072015.pdf (a survey of ten European entities that procured or considered procuring cloud services found procuring "on-demand" and "pay-per-use" services as a main difficulty in addition to privacy and security concerns).

38. *See, e.g.*, Laura P. Taylor, FISMA COMPLIANCE HANDBOOK 23, (Patricia Moulder et al. eds., Syngress, 2nd ed. 2013). The Federal Information Security Management Act (FISMA) requires the head of federal agencies to develop agency-wide programs and take specific measures, such as formal security assessments, to mitigate cybersecurity risks to agency data. Federal Information Security Management Act of 2002, Pub. L. No. 107-347, § 301, 116 Stat. 2899, 2946–2955 (2002) (prior to 2012 Amendment).

In addition to the value of citizen data or information individually, collectively this information is extremely important for governments. Issues of "data sovereignty" also play into adoption of cloud by a government.[39] One author argues that "public sector information embodies the past, the present, and the future of a country."[40] Governments need to also consider the public responsibly they have to ensure security and integrity over their data in the long term for historical and archival purposes, among other custodial roles.[41] In addition to specific data needs, governments cannot outsource their more general long-term research and policy goals such as creating a competitive market for all providers.

D. The U.S. Federal Government Dives in Head First into Cloud Computing: But Is the Water Too Shallow?

In 2009, the U.S. federal government began planning a shift in data storage from agency-owned data centers to cloud based services.[42] The goal of this shift is to reduce the Federal government's investment in IT services and to reverse the trend of

---

39. The term "data sovereignty" is not uniformly defined. As it is most often expressed it generally encompasses the ability of an actor to *control* the physical location where its data resides. Kristina Irion, *Your Digital Home is No Longer Your Castle: How Cloud Computing Transforms the (Legal) Relationship Between Individuals and Their Personal Records*, 23 INT'L J. OF L. & INFO. TECH. 348, 356 (2015) (U.K.). Acknowledging the lack of a standard definition, Richard Kemp defines the concept as having "an intuitively understood meaning of when a person's *right to deal* as she or he wishes with her or his own data may be overridden, typically through involuntary disclosure to or access by a third party." RICHARD KEMP, CLOUD COMPUTING AND DATA SOVEREIGNTY 1 (2015), (emphasis added) http://www.kempitlaw.com/wp-content/uploads/2015/10/Cloud-Computing-and-Data-Sovereignty.pdf.

40. Kristina Irion, *Government Cloud Computing and National Data Sovereignty*, 4 POL'Y & INTERNET 40, 53 (2012).

41. Archival and other requirements might also serve as a barrier to adopting cloud computing. For example, in Norway the "Archive Statute" requires that all public archive material be stored within Norway. Lov om Arkiv 4 desember 1992 nr. 24 §§ 9(b) (Nor.). This limits the use of CSPs to those with servers physically located in Norway.

42. Patricia Moloney Figliola & Eric A. Fischer, CONG. RESEARCH SERV., R42887, OVERVIEW AND ISSUES FOR IMPLEMENTATION OF THE FEDERAL CLOUD COMPUTING INITIATIVE: IMPLICATIONS FOR FEDERAL INFORMATION TECHNOLOGY REFORM MANAGEMENT 1 (2015), https://www.fas.org/sgp/crs/misc/R42887.pdf.

increasing data center expenditures.[43] Currently, the federal government's annual IT expenditures top $80 billion.[44] From the contracting phase to the operational stage of data centers, the federal government spends significant amounts of money on a per agency basis to store and manage its data.[45] Outside of peak usage times, much of the computing power purchased in this manner remains unused for substantial periods of the year.[46] Estimates on the savings created by using cloud computing average 50%, but vary widely by agency.[47]

In 2011, the White House presented a plan to reorganize and improve the federal IT policy landscape. Central in its plan was a "cloud first" strategy, which would essentially make cloud solutions the default option for federal agencies.[48] The strategy is reasonably straightforward. If a secure and cost-effective cloud option exists, federal agencies are required to consider implementation of that service.[49] If an agency has a current strategy that does not include cloud computing, it must re-evaluate its policy to include cloud computing. This "cloud first" strategy has not been without its critics.[50] Like users in the private sector, chief information officers at federal agencies have raised concerns about security levels available with cloud; cost (and feasibility) of migration to cloud from current legacy systems; and the loss of control that is part and

---

43. *See id.* at 13–14. To specifically address this problem, the Federal Data Center Consolidation Initiative (FDCCI) was created. *See* Fed. Chief Info. Officers Council, *Data Center Consolidation and Optimization*, CIO.gov, https://cio.gov/deliver/data-center-consolidation/ (last visited Feb. 25, 2016). The goals of the initiative include reducing costs from software to operations, reducing energy consumption, and embracing "Green IT". *Id.* Federal investment in IT grew from 46 billion USD in 2001 to 81 billion USD in 2010. Figliola & Fischer, *supra* note 42, at 13.

44. U.S. Gov't Accountability Off., GAO-14-753, Cloud Computing: Additional Opportunities and Savings Need to Be Pursued 3 (2014).

45. Kundra, *supra* note 2, at 7 (maintaining that by using a cloud computing model for IT services, data center infrastructure expenditure can be reduced by approximately 30%, translating into an estimated $20 billion savings of IT spending).

46. *Id.*

47. Figliola & Fischer, *supra* note 42, at 7. Projected agency savings range from 10% to 250%.

48. Kundra, *supra* note 2 at 2.

49. *Id.*

50. Sasha Segall, *Jurisdictional Challenges in The United States Government's Move to Cloud Computing Technology*, 23 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 1105, 1108 (2013) (highlighting concerns around keeping data servers "secure, governed, and protected" in the cloud).

parcel with use of cloud computing.[51] Concerns that have been particularly salient among information officers are overall reliability, availability, privacy, and portability of federal data stored on the cloud.[52]

From the beginning of the program, the U.S. cloud computing strategy set high goals for cloud adoption by federal agencies. However, few have met their mark. A 2012 report by the Government Accountability Office noted some progress on federal cloud adoption but determined that better planning was needed.[53] A follow-up report in 2014 examined the status of several agencies adopting cloud computing solutions.[54] An increase was found in the number of agencies using cloud computing from 21 to 101 since the 2012 report.[55] Although cloud computing adoption and usage has increased, total investment in cloud computing only makes up approximately 1% of the total federal budget for IT spending.[56] For a "cloud first" policy, growth has been slow at best.

In addition to slow growth, there has been considerable confusion and improper implementation of cloud computing by many agencies. Recent audits of government agencies using cloud computing has shown major gaps in the contracts used to procure cloud systems and uncovered uneven, and in some cases nonexistent, application of FedRAMP and other federal requirements.[57] One audit of seven federal agencies concluded that the agencies failed to include applicable security requirements and did not negotiate appropriate contract terms before transferring data onto the shared cloud infrastructure.[58] These actions put both government data and federal monies at risk.[59]

---

51. Figliola & Fischer, *supra* note 42, at 6–7.

52. *Id.* at 9–12. Gasser & O'Brien, *supra* note 30, at 7–8 (citing a GAO report finding that 22 of 24 federal agencies surveyed reported that they were either concerned or very concerned about the potential information security risks of using cloud).

53. U.S. GOV'T ACC'T OFF, GAO-12-756, INFORMATION TECHNOLOGY REFORM: PROGRESS MADE BUT FUTURE CLOUD COMPUTING EFFORTS SHOULD BE BETTER PLANNED (2012).

54. U.S. GOV'T ACC'T OFF, *supra* note 44.

55. *Id.*

56. *Id.*

57. Evaluated *infra* at part 2.

58. The Council of the Inspectors General on Integrity and Efficiency [hereinafter "CIGIE"], *The Council of the Inspectors General on Integrity and Efficiency's Cloud Computing Initiative* 20 (2014), https://www.ignet.gov/sites/default/files/files/Cloud%20Computing%20Initiative%20Report(1)(1).pdf. (auditing the following departments: Department of Energy (DOE), Environmental Protection Agency (EPA), National Labor Relations Board (NLRB), United

Generally, governments use existing services already offered by private CSPs, rather than building "government" clouds.[60] In other words, government clouds, at least in the case of the U.S. and the United Kingdom (UK), are procurement, risk assessment, and certification methods—not plans for developing cloud computing technology.[61] Therefore, governments are pursuing what could be deemed "compliance through template" or "compliance through procurement contract" as they are requiring that private providers meet their needs, on their terms, rather than becoming CSPs.

In its cloud computing strategy, the U.S. government maintains that, like other governments that purchase cloud computing in bulk, it will be able to effectively negotiate contract terms with CSPs and obtain necessary concessions to meet federal security and privacy requirements. This apparent government advantage exists for several reasons. For example, unlike consumers or SMEs, governments purchase services in large quantities and on a payment-for-use rather than a data-for-use basis.[62] Governments use their bargaining position in an attempt to obtain services that satisfy their complex requirements in areas such as the following: security and privacy requirements; liability of CSPs and their suppliers;

States Department of Agriculture (USDA), United States Postal Service (USPS), National Aeronautics and Space Administration (NASA), and the Office of Personnel Management (OPM)). The author has obtained "cloud" contracts from these agencies through requests under the Freedom of Information Act (FOIA).

59. *Id.*

60. Office of the Inspector General (OIG), NASA, *supra* note 20, 4–5. This is not to say that governments have stayed completely out of the cloud business. For example, NASA created its own cloud computing service "Nebula" instead of contracting with a CSP to produce the service. However, after benchmarking Nebula against the capabilities of commercial CSPs including Amazon and Microsoft, it determined that public clouds were more reliable, cost effective, and had better offerings and support. As a result, NASA discontinued the Nebula project.

61. Millard et al., *supra* note 22, at 108–10 (providing background on the UK's Govcloud procurement program).

62. JANSEN & GRANCE, *supra* note 4, at 6. NIST has categorized classes of "public clouds" based on whether the service is paid for or supported by advertising. The services used by the U.S. federal government can be categorized in NIST's third class of public cloud, defined as "clouds whose services are fee-based and whose terms of service are negotiated between the organization and the cloud provider." In this Article, I follow the NIST definition in the "payment-for-use" category. For examples of "data for use," *see* Chris Jay Hoofnagle & Jan Whittington, *Free: Accounting for the Costs of the Internet's Most Popular Price*, 61 UCLA L. REV. 606, 626–28 (2014) (stating that many online providers offering free services track and monitor user behavior to deliver advertisements in addition to other monetization of user data).

warranties; and service levels.[63] A key-component of the U.S. cloud strategy is the FedRAMP program, which is evaluated in the next section.

E. FedRAMP—A Roadmap to Compliant Cloud Computing?

To provide a system for addressing the risks present in cloud computing–and to streamline cloud adoption–the federal government created the FedRAMP program.[64] The FedRAMP program is mandatory and must be implemented by federal agencies using cloud computing.[65] FedRAMP is designed to provide a standardized approach to security assessment, authorization, and monitoring of cloud computing. The aim of the FedRAMP evaluation is to create a "do once, use many times" system to maximize efficiency in cloud adoption.[66] The FedRAMP program provides a means for agencies to authenticate that certain controls are in place before adopting cloud computing.[67] By creating a government-wide standard, FedRAMP is intended to provide federal agencies with the means to rapidly adopt cloud

63. Millard et al., *supra* note 22, at 89 (providing that regulated industries, including government bodies and financial institutions, more often attempt to negotiate cloud contract terms to meet their needs). *Id.* at 75 (stating that "[l]arge users such as governments are demanding more customer-friendly terms.").

64. METHENY, *supra* note 23, at 217. As early as 2009, a cloud computing security group began evaluating the question of implementing adequate security and monitoring for multi-agency outsourcing. *See* Steven VanRoekel, Security Authorization of Information Systems in Cloud Computing Environments (Office of Management and Budget ed., Dec. 8, 2011). https://www.fismacenter.com/fedrampmemo.pdf (requiring that all "low and moderate impact level" cloud services adopted by agencies must comply with FedRAMP requirements in 2011). However, CSPs that were in the acquisition phase in 2012 were given until June 5, 2014 to become FedRAMP compliant. *Id.* at n. 10.

65. Defense Information Systems Agency (DISA), *Department of Defense (DoD) Cloud Computing Security Requirements Guide Version 1 Release 1* (Jan. 12, 2015), https://info.publicintelligence.net/DoD-CloudSecurity.pdf. This mandate comes from the Office of Management and Budget (OMB) [hereinafter "DISA"].

66. FedRAMP, *Program Overview*, https://www.fedramp.gov/about-us/about/ (FedRAMP's "do once, use many times" framework estimates a savings of 30–40% of government costs, as in addition to hourly costs of agency security assessments).

67. *See, e.g.*, Taylor, *supra* note 38 (describing FedRAMP as "FISMA [Federal Information Security Management Act] for the cloud."). The FISMA Act requires the head of federal agencies to develop agency-wide programs and take specific measures to mitigate cybersecurity risks to agency data.

computing and mitigate risk while also reducing many of the risk-evaluation and procurement expenses common in IT-hosting.[68]

As a method for cloud procurement, FedRAMP uses best practices and contract templates for cloud acquisition using a risk management approach for assessing services offered by CSPs.[69] The overall program goals of this standardized system are to provide cloud based systems that have (1) adequate security, (2) eliminate duplication of effort including risk management costs, and (3) enable "rapid" and cost-effective procurement systems for federal agencies to purchase services.[70] Standardized procurement has advantages for providers as well as governments. For example, unlike the Federal Information Security Management Act (FISMA), under FedRAMP a CSP provider is able to sell the same computing service to many agencies without undergoing or repeating an expensive authorization process many times.[71]

Primary participants or stakeholders in the FedRAMP process include Third Party Assessor Organizations (3PAOs), federal agencies, the FedRAMP Joint Authorization Board (JAB), and CSPs.[72] 3PAOs are "cloud auditors" tasked with performing independent third-party assessments of FedRAMP controls. The JAB is the primary governance body for the FedRAMP program and makes decisions regarding standards and processes that must be met for a CSP to host federal data.[73] The FedRAMP Project Management Office (PMO) and JAB establish processes and standards for security and authorization systems that have the greatest ability for application on a government wide basis.[74] CSPs that meet security and audit requirements set by the JAB are eligible to receive Provisional Accreditation.[75] The overall requirements vary depending on the type of data being stored and

68. *See, e.g.*, Kundra, *supra* note 2, at 29 (providing that "Federal Government contracts will also provide riders for state and local governments. These riders will allow all of these governments to realize the same procurement advantages of the Federal Government.").

69. METHENY, *supra* note 23, at 171–72.

70. Figliola & Fischer, *supra* note 42, at 17.

71. Taylor, *supra* note 38, at 295. FedRAMP does not replace the Federal Information Security Management Act (FISMA), the main federal standard for computing services, but provides a specific roadmap for cloud based services while also applying many of the same security controls (i.e., NIST SP 800-53).

72. FEDRAMP PMO, *Guide to Understanding FedRAMP Version 2.0* 13 (June 6, 2014) (discussing the actors establishing and communicating technical standards).

73. DISA, *supra* note 65, at 8.

74. FEDRAMP PMO, *supra* note 72, at 13.

75. DISA, *supra* note 65 at 8.

the level of data sensitivity. Data are categorized and then divided into three categories including low-impact, moderate-impact, or high-impact systems based on the security objectives of confidentiality, integrity, or availability.[76]

The FedRAMP Security Authorization Process has three main steps. The first step is a security assessment based on the U.S. National Institute of Standards and Technology (NIST) Risk Management Framework.[77] The applicant CSP must verify that they meet the framework via independent audit conducted by a 3PAO accreditor. If the JAB is satisfied, it grants CSPs provisional Authority to Operate. The second step allows individual agencies to review the FedRAMP security requirements and compare them to their own agency needs. At this stage, an agency can add additional requirements on CSPs to fit their specific security needs. However, the baseline security established in step one will not need to be repeated for accredited CSPs. Third, after the original authorization is obtained, ongoing security assessment requirements remain in place.[78] To meet this requirement, CSPs that acquire provisional Authority to Operate will continue to be monitored by the Department of Homeland Security and FedRAMP to meet ongoing security needs, but have the advantage of being able to provide an accredited system.

If CSPs are unable to meet the technical requirements, or are unwilling to negotiate certain aspects of their standard contracts, they will be ineligible to provide cloud computing to federal agencies.[79] In that sense, the federal government offers its terms on a take-it-or-leave-it basis using a series of templates creating a reverse contract of adhesion by requiring that CSPs accept their terms. FedRAMP templates are developed by information officers from several federal agencies and must be adopted by a CSP.[80] To

---

76. Susan Zevin, *FIPS Publication 199—Standards for Security Categorization of Federal Information and Information Systems* 6 (Department of Commerce ed., 2004), http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.

77. UNITED STATES POSTAL SERVICE, CLOUD SECURITY, 60 (2013), https://about.usps.com/handbooks/as805h.pdf [hereinafter "USPS"]. The NIST RMP focuses on risk at the information system level focusing on (1) Risk Framing, (2) Risk Assessment, (3) Risk Response, (4) Risk monitoring. METHENY, *supra* note 23, at 175–180. 2013. Metrics or other information to document these steps may be required contractually—particularly as part of service level agreements. *Id.* at 182.

78. FedRAMP, *supra* note 66.

79. *See, e.g.*, DISA, *supra* note 65.

80. FEDRAMP PMO, *supra* note 72, at 11.

be considered FedRAMP compliant, the CSP must meet the following criteria:

> The system security package has been created using the required FedRAMP templates
>
> The system meets the FedRAMP security control requirements
>
> The system has been assessed by an independent assessor
>
> A Provisional Authorization, and/or an Agency ATO, has been granted for the system
>
> An authorization letter for the system is on file with the FedRAMP Program Management Office.[81]

In addition to the challenges of shifting its IT consumption, the Federal Government must also re-examine aspects of its contracting models when it comes to cloud. This requires, among other steps, making certain that procurement methods used acknowledge the differences between procuring traditional IT services and procuring cloud.[82] Being able to make this distinction is crucial to meeting compliance requirements, keeping data secure, and protecting federal investment.[83]

F. Legal Framework: Meeting Statutory and Administrative Requirements

The following section highlights core legal requirements that must be considered by federal agencies adopting cloud computing. Legal requirements falling under the umbrella of data privacy law in the U.S. are often described as a "patch-work."[84] Laws that must

---

81. *Id.*

82. Andrew Joint & Edwin Baker, *Knowing the Past to Understand the Present– Issues in the Contracting for Cloud Based Services*, 27 COMPUTER L. & SECURITY REV. 407, 412–15 (2011).

83. CIO COUNCIL, *supra* note 21, at 3.

84. Samantha Diorio, *Data Protection Laws: Quilts versus Blankets*, 42 SYRACUSE J. INT'L L. & COM. 485, 491 (2014) (describing the American system of privacy law as a patchwork). Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, § 201, 100 Stat. 1848, 1860–1868 (codified as amended at 18 U.S.C. §§ 2701–2711). Children's Online Privacy Protection (COPPA) 15 U.S.C. §§ 6501–6506; Pub. L. 105-277. Gramm-Leach-Bailey Act Pub. L. 106-102, 113 Stat. 1338, codified in relevant part at 15 U.S.C. §§ 6801–6809 and §§ 6821–6837. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001,

be incorporated originate from many sources.[85] The point of departure in determining the applicability of data privacy regulations in the U.S. generally hinges on whether the data can be considered Personally Identifiable Information (PII).[86] If PII will be stored on the service, the agency must account for data privacy requirements.[87] The designation of whether a federal agency stores PII is therefore central in evaluating applicable compliance requirements.[88] In the context of federal agencies, PII has been defined as:

> Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.[89]

Pub. L. No. 107-56, 115 Stat. 272 (2001). Fair Credit Reporting Act (FCRA) 15 U.S.C. § 1681b(f).

85. Carol M. Hayes, Jay P. Kesan, & Masooda N. Bashir, *Cloud Services, Contract Terms, and Legal Rights*, 17 No. 6 J. OF INTERNET L. 3, 3–7 (2013) (providing an overview of US Privacy law applicable to cloud computing).

86. Paul M. Schwartz, *Information Privacy in the Cloud*, 161 U. PA. L. REV.1623, 45–46 (2013) (evaluating the threshold for application of data privacy laws in the U.S. and the EU and finding that "the U.S. threshold approach to defining personal information is reductionist when compared with the European Union's expansionist approach" although both consider similar factors in reaching the determination).

87. Privacy Act of 1974, 5 U.S.C. § 552a(m)(1) (1974) [hereinafter "Privacy Act"] ("When an agency provides by a contract for the operation by or on behalf of the agency of a system of records to accomplish an agency function, the agency shall, consistent with its authority, cause the requirements of this section to be applied to such system.").

88. LEE BYGRAVE, DATA PRIVACY LAW: AN INTERNATIONAL PERSPECTIVE 129 (Oxford University Press 2014). (This is not limited to the U.S. or federal context as "data privacy law generally applies solely to 'personal' data or information.").

89. Erika McCallister, & Karen Scarfone, *NIST Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* B1, NAT'L INST. STANDARDS & TECH. ES-1 (2010). *See* METHENY, *supra* note 23, at 181–82 (providing examples of data that likely qualify as PII in a U.S. context). *See also* BYGRAVE, *supra* note 88, at 129–139 (providing a detailed discussion of determining whether data is "personal" and falls under the protection of EU data privacy law).

However, even the definition of what is considered PII varies depending on the regulations being applied or the industry being regulated.[90] For example the healthcare, financial services, banking, and education sectors all have specific regulatory requirements for data usage.[91] Other sectors have no individualized or mandatory requirements allowing the parties to negotiate and determine the legal requirements by contract to a much greater extent.[92] Added requirements, including those related to data breach notification, originate from state law as well as federal, but vary by among others, sector, data type.[93] For federal agencies, additional "patches" are added to this regulatory quilt by administrative requirements, internal agency standards, and federal IT security requirements.[94] This makes U.S. privacy

90. Paul M. Schwartz & Daniel J. Solove, *Reconciling Personal Information in the United States and European Union*, 102 CAL. L. REV. 877, 887–88 (2014). This determination also varies by legal system and within legal systems. See BYGRAVE, *supra* note 88, at 101 (providing that even within the EU, member have their "own unique mix of rules."). Compared to the U.S., the European approach to defining what is considered "personal" data is generally considered more expansive as it covers "any information relating to an identified or identifiable natural person."

91. HIPAA, *supra* note 84.

92. *See* BYGRAVE, *supra* note 35, at 118. In the U.S., parties can contract out of data privacy responsibilities to a much greater extent than is allowed under EU data protection law. *See also* Kevin McGillivray, *supra* note 16, at ¶¶ 225–27 (discussing the role of contracts in cloud computing).

93. For example, the "HIPAA Breach Notification Rule," 45 C.F.R. §§ 164.400–164.414, requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information. *See, e.g.*, Samson Esayas, *Breach Notification Requirements Under the European Union Legal Framework: Convergence, Conflicts, and Complexity in Compliance*, 31 J. MARSHALL J. INFO. TECH. & PRIVACY L. 317 (2015) (providing an overview of breach notification rules in the EU).

94. *See, e.g.*, Minimum Security Requirements for Federal Information and Information Systems, FIPS Publication 200. *See* Taylor, *supra* note 38, at 8 (providing additional regulations impacting federal use in "Compliance Overview"). *See also* Personal Identity Verification (PIV) of Federal Employees and Contractors [FIPS Publication 201-1], Security Requirements for Cryptographic Modules [FIPS Publication 140-2], Standards for Security Categorization of Federal Information and Information Systems [FIPS Publication 199]. For NIST Security requirements *see* NIST Definition of Cloud Computing [NIST SP 800-145], Computer Security Incident Handling Guide [NIST SP 800–61, Revision 2], Contingency Planning Guide for Federal Information Systems [NIST SP 800-34, Revision 1], Engineering Principles for Information Technology Security (A Baseline for Achieving Security) [NIST SP 800-27, Revision A], Guide for Assessing the Security Controls in Federal Information Systems [NIST SP 800-53A], Guide for Developing Security Plans for Federal Information Systems [NIST SP 800-18, Guide to Understanding

law flexible, but also somewhat chaotic.[95] This stands in contrast to European data protection law, which broadly requires a legal basis for any processing of personal data or PII.[96]

CSPs providing services under the FedRAMP scheme must comply with a myriad of laws in the areas of data privacy and data security, although they arguably have a less demanding data privacy regulation to comply with than their European counterparts.[97] Further, if a federal agency stores PII, it is required to comply with the Privacy Act of 1974 (Privacy Act) and the E-Government Act of 2002, among others.[98] Given all these sources of rules and procedures, the compliance picture quickly becomes

---

FedRAMP Version 1.2, Apr. 22, 2013 Page 12 Revision 1], Guide for Developing the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach [NIST SP 800-37, Revision 1], Guide for Mapping Types of Information and Information Systems to Security Categories [NIST SP 800-60, Revision 1], Guide for Security-Focused Configuration Management of Information Systems [NIST SP 800-128], Information Security Continuous Monitoring for Federal Information Systems and Organizations [NIST SP 800-137], Managing Information Security Risk [NIST SP 800-39], Recommended Security Controls for Federal Information Systems [NIST SP 800-53, Revision 4], Risk Management Guide for Information Technology Systems [NIST SP 800-30], Security Considerations in the System Development Life Cycle [NIST SP 800-64, Revision 2], Technical Guide to Information Security Testing and Assessment [NIST SP 800-115].

95. Justin Brookman, *Protecting Privacy in an Era of Weakening Regulation*, 9 HARV. L. & POL'Y REV. 355, 357–59 (2015) (arguing that although the U.S. protections are largely based on the same principles as other nations, the protection in the U.S. is comparatively weaker). *But see* Kenneth A. Bamberger and Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247 (2010), http://scholarship.law.berkeley.edu/facpubs/1305 (suggesting that even if the approach "on the books" is fragmented and less expensive than other jurisdictions, privacy practices—at least by select large corporations—are much more uniform and extensive than the law requires).

96. Schwartz, *supra* note 86, at 1634–35 (stating that "[u]nlike the European Union, the United States lacks an omnibus information privacy statute and instead regulates this area through sectoral laws alone"). For a detailed discussion of differences between the systems *see* Schwartz & Solove, *supra* note 90. *See also* BYGRAVE, *supra* note 35, at 118–19 (in addition to scope of coverage, the EU system also places much greater limits on the parties ability to "contract around core data privacy rights.").

97. *See* Schwartz, *supra* note 86, at 1638 (discussing the complexity of applying privacy law to the cloud in the European Union).

98. *See* Privacy Act, *supra* note 87 (providing principles for data privacy focusing on factors including "collection limitation, data quality, purpose specification, use limitation," among others). Similarly, the E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, requires federal agencies to protect and ensure the security of PII of U.S. citizens.

complex.[99] Guidance provided in the Federal Acquisition Regulations (Acquisition Regulations or FAR) on compliance with, for example, the Privacy Act is relatively vague.[100] For a relevant, yet manageable overview of these regulations as they relate to federal security and operational requirements, the Article focuses primarily on laws applicable to federal agency users under the Acquisition Regulations, along with other requirements prescribed for federal information systems.[101]

Federal agencies are required to adhere to certain laws or regulations when contracting for services, including the adoption of cloud computing. The Acquisition Regulations are the uniform policies and procedures for acquiring services by contract for all executive agencies.[102] The Acquisition Regulations require that the contracting officer ensures agency contracts safeguard the interests of the U.S.[103] This requirement includes examining contracts entered into by federal agencies to make certain they meet regulatory requirements. The Acquisition Regulations are applicable to federal agencies storing information relating to citizens and other types of government data. Pursuant to the Acquisition Regulations, "operation of a system of records"

---

99. Wendy L. Currieb & Jonathan J.M. Seddona, *Cloud Computing and Trans-border Health Data: Unpacking U.S. and EU health care regulation and compliance*, 2 HEALTH POL'Y & TECH. 2, 229–41 (2013) (providing examples of this complexity, particularly when adding in both U.S. and EU regulations as they apply to the healthcare sector). In addition to those requirements, pursuant to FISMA, agencies are required to implement programs that protect PII residing on their systems—or systems they utilize for computing needs. *See* TIM GRANCE, ERIKA MCCALLISTER & KAREN SCARFONE, NAT'L INST. STANDARDS & TECH, *NIST Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* (2010) (providing that in addition to protection during storage, PII must also be "collected, maintained, and disseminated in accordance with Federal law.").

100. *See* 48 C.F.R. § 52.224 (2012). *See also* Joshua S. Parker, *Lost in the Cloud: Protecting End-User Privacy in Federal Cloud Computing Contracts*, 41 PUB. CONT. L.J. 385, 404 (2012).

101. JANSEN & GRANCE, *supra* note 4, at 16. The main source of federal procurement rules is the Federal Acquisition Regulations (FAR), which are issued by the Secretary of Defense (for defense procurement) and the administrator of NASA (non-defense procurement). In addition, federal agencies may issue their own supplements—within the scope of specific agency needs. DAVIES, *supra* note 31, at 58.

102. STEVEN W. FELDMAN, ET AL., GOVERNMENT CONTRACTS IN A NUTSHELL 3 (West 5th ed. 2011). U.S. Federal procurement is primarily governed by two main statutes: (1) the Federal Property and Administrative Services Act of 1949 and (2) the Federal Armed Services Procurement Act of 1948. DAVIES, *supra* note 31, at 58.

103. 48 C.F.R. § 1.602-2 (2013).

includes "any of the activities associated with maintaining the system of records, including the collection, use, and dissemination of records."[104] Based on this broad definition, the Acquisition Regulations apply to agency records being stored using cloud computing.

The Acquisition Regulations are applicable to a wide variety of information stored on the cloud and require the "protection of individual privacy" for records containing PII such as health data, financial information, among others.[105] The Acquisition Regulations take a relatively expansive view of the kind of data considered to be PII. Data stored by an agency on a system of records is considered "personal" in the context of executive agency contracting where "any records under the control of any agency" use "the name of the individual" or an "identifying number, symbol, or other identifying particular assigned to the individual."[106] If PII will be stored in the service, the Acquisition Regulations require that the agencies systems meet security and privacy requirements above those required for non-personal data.[107] For the purposes of criminal liability and penalties, agency officers and employees may also be held liable under the Acquisition Regulations.[108] Criminal liability extends beyond agency employees to contractors and their employees.[109] On this basis, CSPs providing cloud computing to federal agencies may also face liability under the act.[110]

---

104. 48 C.F.R. § 24.101 (2014).

105. *Id.* (under the Acquisition Regulations, the term "record" includes "any item, collection, or grouping of information about an individual" that is maintained by an agency).

106. *Id.* § 52.224-2(c)(1)–(3) (2013). *See also* Privacy Act § 552 a (a)(4)–(5) (2013).

107. 48 C.F.R. § 24.101 (2014). METHENY, *supra* note 23, at 83–84 (distinguishing "privacy," "security," and "confidentiality" as interrelated but separate aspects of data management). Pursuant to the Acquisition Regulations, and requirements under the Privacy Act, contractors must also ensure that notice of Privacy Act compliance requirements is included in "every solicitation and resulting subcontract." *See* 48 C.F.R. § 52.224-2(2). In addition to general civil liability, the Acquisition Regulations provide for criminal liability for violations. 48 C.F.R. § 24.102(b) (2014).

108. *Id.*

109. *Id.* § 24.102(b) (2014)

110. CIO COUNCIL, *supra* note 21, at 17.

II. CONTRACT CHALLENGES AND DEFICIENCIES—FEDERAL AGENCIES PROCURE CLOUD COMPUTING

This section evaluates the application of the FedRAMP system to agency cloud computing procurement based on government audits of executive agencies with a focus on missing or insufficient contract terms. To complete this analysis, the Article considers general problems with contract templates and best practices guides provided as part of the FedRAMP program–in addition to the application of these tools. Likewise, specific contracting problems or shortcomings at individual agencies are examined. Finally, standard contract terms that will be required in future FedRAMP agreements are evaluated. This section also assesses areas where agencies failed to include aspects of the Acquisition Regulations and other federal regulations.

In the specific case of FedRAMP, the federal government's contracting performance while moving to the cloud has been stormy at best. Despite the availability of specific security and performance standards, guidelines, and "best practices" for entering into cloud computing contracts, few polices have been implemented or followed adequately by federal agencies.[111] For agencies storing data with a CSP, the terms of the contract provide the rights and liabilities of the parties using the service from the beginning to termination of the service. In order to protect federal data throughout the life of the service, agencies must clearly define obligations and roles of the parties that will be handling federal data in contract terms with the CSP. The combination of contract terms and statutory legal requirements creates a complex picture for storing federal data on the cloud. Unlike private parties, federal agencies are limited in their ability to opt-out or avoid certain requirements.[112]

In a recent audit by the Council of the Inspectors General on Integrity and Efficiency (CIGIE) 77 contracts used by federal

---

111. *Id.* Several agencies, such as the DOE among others, failed to implement these terms. *See* Gregory H. Friedman, *Department of Energy (DoE) Office of Inspector General, Office of Audits and Inspections, Audit Report: The Department of Energy's Management of Cloud Computing Activities*, 2–3 (2014).

112. The use of contracts, although flexible, is also subject to mandatory rules–many of which revolve around security and data privacy obligations. *See, e.g.*, EMILY M. WEITZENBÖCK, A LEGAL FRAMEWORK FOR EMERGING BUSINESS MODELS: DYNAMIC NETWORKS AS COLLABORATIVE CONTRACTS 156–57 (Edward Elgar Publishing 2012) (discussing the effect of mandatory rules on contracts in the common and civil law contexts).

agencies to procure cloud computing were evaluated.[113] In their evaluation, the auditors found that all 77 contracts entered into by individual agencies were lacking specifications or required elements for compliance with federal data management.[114] The total value of the contracts evaluated was assessed at $1.6 billion. Contracts evaluated in this audit were selected from a pool of 348 agreements, with a combined value of approximately $12 billion.[115] If the 77 contracts evaluated in this audit are representative of the entire pool of cloud agreements, much of the U.S. federal government's cloud investment may be at risk. Further, the audit calls into question the security, integrity, and confidentiality of data stored in the cloud by federal agencies. As more government information is moved to cloud computing, these contractual oversights have the potential to weaken security and privacy protections that guard government data including the PII of citizens. Specific areas of omitted contract terms and their potential consequences are considered in more detail in the following sections.

A. Definitional Problems: What Constitutes Cloud Computing and How Should it be Expressed in Agency Contracts?

The first issue contributing to incomplete agency contractual compliance and risk assessment for cloud computing was confusion around the definition of cloud computing.[116] Although expansive and arguably imprecise, the NIST definition provided *supra* has essentially become the standard definition for classifying cloud computing.[117] Although discussions regarding the novelty of cloud computing as a new technology or just a new business model are ongoing, the NIST definition does provide federal agencies with a means to classify certain services as cloud computing.[118] Nevertheless, many federal agencies failed to

113. CIGIE, *supra* note 58, at 7.

114. *Id.* at 7.

115. *Id.* at 1.

116. *Id.* at 14.

117. MELL & GRANCE, *supra* note 8, at 7. *See* Timothy J. Calloway, *Cloud Computing, Clickwrap Agreements, and Limitation on Liability Clauses: A Perfect Storm*, 11 DUKE L. & TECH. REV. 163, 166 (2012) (arguing that the "federal government's definition of cloud computing is anything but clear.").

118. Filippi & Vieira, *supra* note 15, at 117 (defining cloud computing as "[a]n online infrastructure with huge computational power that is able to store and process very large amounts of data locally on the device for one user and in the cloud for another."); *see also* Andrews & Newman, *supra* note 28, at 325 (maintaining that cloud computing is more than a "buzzword").

understand that the services they were procuring were cloud computing offerings.[119]

For instance, the Department of Energy, with cloud computing contracts valued at over $30 million, failed to apply the NIST definition to many of the IT hosting services employed by the agency.[120] As a result, the Department of Energy did not have an overall inventory of the cloud computing it was using.[121] This "misdiagnosis" is not a minor point. The Department of Energy's Office of the Chief Information Officer reported 44 ongoing cloud initiatives to the Office of Management and Budget (OMB). In an independent audit conducted by the CIGIE, 130 cloud initiatives at the Department of Energy were revealed.[122] The Department of Energy therefore misidentified over 65% of its cloud computing services. The Department of Energy was not alone as many other agencies showed similar shortcomings in the audit. For instance, the United States Department of Agriculture (USDA) also failed to maintain an accurate inventory of its cloud computing systems, failing to list eight systems that should have been designated as cloud computing.[123]

Definitional confusion is not inconsequential in this area. Defining a service as cloud provides the cornerstone for making certain that security and privacy needs required by FedRAMP are applied. Therefore, if an agency misinterpreted, mislabeled, or misunderstood that a technology was a cloud computing service, they also likely failed to include crucial contract terms and security measures designed to meet the unique risks of cloud computing. This oversight reduced the ability of agencies to monitor CSPs and subcontractors with access to government data.[124] Depending on the service or categorization of data, breaches could have serious

---

119. Taylor, *supra* note 38, at 297 (although it relies on the NIST definition, FedRAMP does not designate specific services as cloud. That determination is up to the individual agency). When properly defined, many of the agencies failed to provide an adequate inventory). *See also* FRIEDMAN, *supra* note 111, at 2.

120. FRIEDMAN, *supra* note 111, at 1.

121. *Id.*

122. *See id.* (auditors found the oversight "especially concerning" in the Office of Science section where the majority of the DOE's efforts were focused, but yet reported no cloud usage).

123. OFFICE OF INSPECTOR GEN. UNITED STATES DEP'T AGRIC., *Audit Report 50501-0005-12: USDA's Implementation of Cloud Computing Services* 3 (2014) [hereinafter "USDA"] (listing only 17 of its 31 cloud systems for auditors), http://www.usda.gov/oig/webdocs/50501-0005-12.pdf.

124. CIGIE, *supra* note 58, at 7.

consequences for government users and result in civil or criminal liability for providers.[125]

Agency implementation problems did not end with failing to classify services. Agencies also failed to include service level agreements (SLAs), the right to audit CSPs and subcontractors, preservation and electronic discovery responsibilities, and retention and deletion of government data, among other provisions.[126] These omissions, according to CIGIE auditors, have the potential to put the security of the federal government's data stored in the cloud at risk.[127] I evaluate these omissions and discuss their potential effect in the subsequent sections.

B. Absence of Non-Disclosure Agreements (NDAs) and Consequences for Federal Agencies

Just like any commercial actor, protecting confidentiality is important for agencies moving their data to cloud computing. The purpose of an NDA is to keep private information, whether it is user data or trade secrets, confidential.[128] Non-disclosure agreements are often entered during pre-contractual negotiations and remain in force until after the parties' relationship is terminated. The advantage of entering the agreement early is that if the parties part ways without coming to an ultimate agreement, they have some assurance that the information they have disclosed will remain protected—or at least damages will be recoverable in the case of a breach of the agreement.

Federal agencies often require private contractors, including CSPs, to enter into NDAs.[129] In some cases, private federal data will be visible or accessible by CSPs. In addition to keeping non-public data private, disclosure of certain types of information could impact data security. In the best practice guide issued by FedRAMP, particular weight was placed on the ability of the federal agency to enforce NDAs against CSPs, in addition to

---

125. JOINT TASK FORCE TRANSFORMATION INITIATIVE, NAT'L INST. OF STANDARDS & TECH., SPECIAL PUB. 800-53 REV. 5, SECURITY AND PRIVACY CONTROLS FOR FEDERAL INFORMATION SYSTEMS AND ORGANIZATIONS 28 (2011), http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

126. CIGIE, *supra* note 58, at 7 (in the sample of 77 contracts, 42 contracts with a combined value of 317 million USDs did not contain SLAs).

127. *Id.* at 10.

128. CIO COUNCIL, *supra* note 21, at 7 (providing that federal agencies should include NDAs protecting non-public information that is procurement-sensitive, information that impacts physical security, among other sensitive information).

129. *Id.*

clearly defining expectations in the agreements.[130] This requirement was not consistently met. In the CIGIE audit, 33 of the 77 contracts did not have an NDA in place.[131] This oversight may also be in conflict with the requirements of the Acquisition Regulations—which require that contractors keep certain information private regarding security or safeguards.[132]

Even in cases where the NDA requirement was not wholly disregarded, NDAs were not applied throughout the infrastructure. In the case of the EPA, an NDA was in place between the primary contractor CSP and the agency.[133] However, pursuant to the contract, a subcontractor hosts the cloud application containing the EPA's data. The EPA did not enter into an NDA with the subcontractor and the "service agreement" between the primary contractor and the subcontractor hosting EPA data did not appropriately flow-down the NDA agreement.[134] By not providing a clear NDA that was enforceable throughout the CSP's contracting chain the EPA's private information was arguably less protected when handled by the CSP's subcontractor.[135] Similarly, the USDA failed to include an NDA in two of its contracts.[136] Where the USDA did include NDAs, it failed to provide any method for monitoring compliance with the agreements.[137]

As was noted in DoD reports, failing to provide an NDA with a contractor may have additional consequences for a federal agency.[138] More specifically, under the "release to one release to

130. *Id.*

131. CIGIE, *supra* note 58, at 8–9.

132. FAR 52.239-1(a)–(c) (1996) (requiring "(a) The Contractor shall not publish or disclose in any manner, without the Contracting Officer's written consent, the details of any safeguards either designed or developed by the Contractor under this contract or otherwise provided by the Government. (b) To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of Government data, the Contractor shall afford the Government access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases.").

133. U.S. ENV'T PROT. AGENCY OFF. OF INSPECTOR GEN, REPORT NO. 14-P-0323, EPA IS NOT FULLY AWARE OF THE EXTENT OF ITS USE OF CLOUD COMPUTING TECHNOLOGIES 7 (2014).

134. *Id.* at 7 (Instead of an NDA, a service agreement with the primary contractor was in place providing that the subcontractor hosting the PMOS application "does not warrant that the services and/or any information obtained thereby shall be complete, accurate, uninterrupted, secure or error free.").

135. *Id.*

136. USDA, *supra* note 123, at 8.

137. *Id.*

138. DISA, *supra* note 65, at 8.

all" rule, if a government agency releases information to a contractor without an NDA, it cannot later deny the public access to that information under the Freedom of Information Act (FOIA).[139] Therefore, although there may never be a data beach or other security failure, federal agencies that fail to include NDAs risk that information they intended to keep private will become public through citizen FOIA requests.[140]

C. Missing SLAs in Agency Cloud Contracts

SLAs are used to measure and ultimately regulate and define the level of service, by way of specifications and metrics, being provided to the agency.[141] SLAs play an important role in defining the expectations and responsibilities of parties, including quality of the service, and privacy requirements.[142] Typically, SLAs will specify technical and performance requirements that must be fulfilled by a CSP and define remedies if those requirements are not met.[143] For instance, SLAs often provide that a service will be available for a certain amount of time on a monthly basis. Guaranteed access or "uptime" generally ranges from 99.0% to 100% each month.[144] Customers that require a service with few

---

139. DEP'T OF DEF., *DoD Cloud Computing Contracts Issues Matrix* 3 (Dec. 16, 2013), http://www.disa.mil/services/dod-cloud-broker/~/media/files/disa/services/cloud-broker/pdcio%20signed%20supplemental%20guidance%20memo%20with%20attachment.pdf.

140. NARA v. Favish, 541 U.S. 157 (2003).

141. Niamh Gleeson & Ian Walden, *'It's A Jungle Out There'?: Cloud Computing, Standards and the Law*, 1–2, 20 (May 23, 2014), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2441182 (explaining that SLAs may also include technical details like backup schedules, recovery time guarantees, software update schedules etc.).

142. *European Commission Directorate General Communications Networks, Content and Technology Unit E2 – Software and Services*, *Cloud Computing Service Level Agreements: Exploitation of Research Results* iv. (2013), https://ec.europa.eu/digital-agenda/en/news/cloud-computing-service-level-agreements-exploitation-research-results (2013) [hereinafter "European Commission"]. *See also* DLA PIPER U.K. LLP ET AL., *supra* note 29, at 22 (providing that SLAs play an important part in defining when the service is conforming based on the agreed upon contract terms).

143. LEE BADGER, ET AL., NAT'L INST. OF STANDARDS AND TECH., SPECIAL PUB. 800-146 CLOUD COMPUTING SYNOPSIS AND RECOMMENDATIONS: RECOMMENDATIONS OF THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY 800-146 3.1, 3.2 (2012). *See also* European Commission, *supra* note 142.

144. In addition to planned or force majeure downtime, for a service to be considered "down" or "unavailable," it may have to be unavailable for a significant amount of time to qualify for a service credit. *See* Millard, *supra* note

interruptions may pay a premium amount to reach a level closer to 100% availability.[145] If service levels are not met, the CSP may be required to provide service credits, provide a full or partial refund, or pay other agreed upon damages.[146]

SLAs are not new to cloud computing and are commonly used in other technology contracts including software, hosting, and traditional IT outsourcing.[147] Unlike the more general or "boilerplate" terms offered on a broader basis, SLAs ought to provide specific measurable or quantifiable outcomes including performance levels. Although SLAs are common, they vary considerably among providers.[148] In both the U.S. and the EU, calls for standardized or model SLAs have been prevalent.[149] In addition to different standards used by providers, interpretation of

---

22, at 83–84 (explaining SLAs contained in negotiated contracts). For example, in a contract provided pursuant to a FOIA request, NASA required an uptime of 99.995%, defining availability as "24 hours a day for every day of the year." The agreement further provides that outages must be scheduled 72 hours in advance. Contract between NASA and eTouch Systems Corp., Contract number NNH05CC35D, 2.2.4 (2005) [hereinafter "NASA contract"].

145. How uptime is calculated may not be as straightforward. SLAs will generally contain exception from the uptime guarantee for things like routine maintenance, emergency maintenance, and situations outside of the providers control including loss of network connection or force majeure situations. *See* Dan Pepper, *Ignoring That Harmless Looking "Force Majeure" Clause in Your Cloud Services Provider Agreement?* CLOUDAVE (Apr. 15, 2013), http://www.cloudave.com/27723/ignoring-that-harmless-looking-force-majeure-clause-in-your-cloud-services-provider-agreement/.

146. Daniel Carmeli, *Keep an I on the Sky: E-discovery Risks Forecasted for Apple's iCloud*, B.C. INTELL. PROP. & TECH. F. 2013, at 1, 11 (the City of Los Angeles was able to negotiate with Google on issues of provider liability. Although the standard cap provided by Google was $1,000, the City of Los Angeles was able to negotiate a much higher amount).

147. Mark Vincent et al., CLOUD COMPUTING CONTRACTS WHITE PAPER: A SURVEY OF TERMS AND CONDITIONS (2011), http://www.ficpi.org.au/articles/White_Paper_June2011.pdf.

148. LEE BADGER, ET AL., NAT'L INST. STANDARDS & TECH., *Special Pub. 500-293, US Government Cloud Computing Technology Roadmap Volume II Release 1.0* (2011) (providing that "Customers are faced with evaluating different SLAs with cloud providers defining reliability using different terms (uptime, resilience, or availability), covering different resources (servers, HVAC systems, customer support), covering different time periods (hours, days, years), and using different guarantees (response time versus resolution time). SLA ambiguities leave the customer at risk.").

149. European Commission, *supra* note 142. *See, e.g.*, SLALOM: Legal & Open Model Terms for Cloud SLA and Contracts, http://slalom-project.eu/ (European project creating a legal model which codifies "fair terms and conditions" for cloud services).

the terms used in the agreements is not necessarily uniform.[150] For example, to define reliability, CSPs use different terms including "uptime, resilience, or availability" which may not have equivalent meanings.[151] A perceived lack of standards in SLAs has created a lack of confidence among cloud adopters.[152] If SLAs are well defined, they may help to limit misunderstandings and also allow cloud adopters to compare services.[153]

A federal "best practice" guide on cloud computing provides that "SLAs should clearly define how performance is guaranteed (such as response time resolution/mitigation time, availability, etc.) and require CSPs to monitor their service levels, provide timely notification of a failure to meet the SLAs, and evidence that problems have been resolved or mitigated."[154] An additional layer of this problem is brought to the forefront in this advice: even where the guarantees are provided, how can the agency effectively measure SLA performance? Even supposing cloud adopters are able to negotiate terms they find to be acceptable in an SLA, monitoring and discovering breaches of the SLA can be very challenging in the cloud environment.[155]

Pursuant to agency theory, if monitoring is adequate, adequate contractor performance should follow.[156] However, as noted by Epstein, adequate monitoring rarely takes place in public-private contracting.[157] In the opaque structure of cloud, such monitoring poses additional challenges. Unlike tangible goods, where a government auditor can drop by a site and check the number or quality of a product being produced by a private provider (e.g., physical check that the number of storage units paid for have been provided), IT outsourcing, and particularly cloud computing, requires a high level of technical expertise and provider cooperation to monitor and ensure performance. A CSP has little

150. BADGER, ET AL., *supra* note 148, at 17.

151. *Id.*

152. T. Noble Foster, *Navigating Through the Fog Of Cloud Computing Contracts*, 30 J. MARSHALL J. INFO. TECH. & PRIVACY L.13, 19–20 (2013).

153. BADGER ET AL., *supra* note 148, at 17.

154. CIO Council, *supra* note 21, at 8.

155. U.S. Department of Commerce, Bureau of Census and Technology Solutions Provider, Inc., Contract No. YA1323-12-CN-0009, 36, Section J "service levels" (2011) (in a contract obtained by FOIA request, a DOC contract contained clear requirements for SLAs and provided a methodology for monitoring performance including the means and technology to be employed in testing service levels).

156. Epstein, *supra* note 33, at 2249.

157. *Id.*

economic interest in informing a federal agency that is has not met service levels—particularly if this has gone unnoticed by the agency itself. To keep the CSP accountable, the government agency must have adequate controls in place.

In the case of the CIGIE audit, there is a very different situation for many of the federal agencies evaluated. It is not that the SLAs provided vague or ambiguous terms or failed to provide adequate monitoring tools, SLAs were simply *absent* from many of the agreements. In fact, of the 77 contracts evaluated, totaling approximately $317 million, 42 contracts failed to include how CSPs performance would be monitored or measured.[158] Overall, 64 of the cloud contracts lacked adequate SLAs, even if some performance measuring aspects were provided.[159] Without any objective standard to measure the services being supplied, agencies have few tools to determine if the services being provided are delivered adequately—or at all. Removing this contractual method of oversight increases the chance of agency overspending or using government funds ineffectively.[160] In the case of a dispute over service, the SLA is important for determining whether a contract breach occurred as well as measuring the service provided.

In individual audit reports provide by agencies, the Environmental Protection Agency (EPA) and the Department of Energy both lacked SLAs. Although the EPA contracts did include "performance of work" statements, the contracts did not provide specific service levels that contractors were required to uphold in providing the service.[161] Essentially, the contract only obligated the CSP to host the application—but required no specific standard of performance to be met.[162] Similarly, the Department of Energy entered into a contract with a CSP that provided some service requirements, but failed to specify uptime percentages, service outages, and remedies for failing to meet service requirements in the contract.[163] This does not mean that the EPA or the Department of Energy's CSPs can act in bad faith.[164] However, it

158. CIGIE, *supra* note 58, at 7.

159. *Id.* at 8.

160. *Id.* at 7.

161. U.S. ENV'T PROT. AGENCY OFF. OF INSPECTOR GEN, *supra* note 133, at 8.

162. *Id.*

163. FRIEDMAN, *supra* note 111, at 2.

164. Andrea M. Matwyshyn, *Privacy the Hacker Way*, 87 S. CAL. L. REV., 54–56 (2013) (providing that performance may be considered "bad faith" in a wide variety of circumstances including inaction). Conduct considered to be in "bad-faith" may be that which violates the written contract directly or actions

would be difficult to argue that a CSP providing a 90% uptime[165] was not acting in good faith even if the EPA was anticipating (and paying for) an uptime closer to 99%.[166] Moreover, if a CSP fails to provide a service at the level agreed, there is often a service credit or other discount available to the user. If the agency has no practical means to measure performance, knowing when the agency is eligible for service credits or discounts is very difficult. In addition, without the means to measure a breach of contract, terminations of contract provisions under the acquisition regulations are also difficult to enforce.[167]

Contracts negotiated with CSPs at other agencies contained aspects of SLAs, but missed important parts. For example, the Consumer Financial Protection Bureau entered into contracts with Amazon Web Services and Deloitte for cloud services which included specific clauses for security responsibilities and requirements for meeting service expectations.[168] However, the contracts did not include terms allowing for forensic audits for criminal and civil investigations or e-discovery procedures as required in the acquisition regulations.[169] Although the USDA included SLAs, they were not specific enough to protect government investment—totaling almost $7 million in the contracts surveyed.[170] For example, of the six contracts reviewed, two did not contain any uptime percentages required of the CSP.[171] Of the

---

that violate the implied covenant of good faith and fair dealing more generally. *Id.* at 55, n.239.

165. JANSEN & GRANCE, *supra* note 4, at 3-1 (uptime is the common measure of cloud service's availability or time that a system is functioning).

166. However, considering that price is often based on availability the government could well be paying for 99% uptime while receiving much less. *See, e.g.*, Millard et al., *supra* note 22, at 83–84.

167. 48 C.F.R. § 49.402-3(d) (1989) (providing procedure for default by a contract officer). HTTP://SLALOM-PROJECT.EU; ENV'T PROT. AGENCY OFF. OF INSPECTOR GEN, REPORT NO.14-P-0332: CLOUD OVERSIGHT RESULTED IN UNSUBSTANTIATED AND MISSED OPPORTUNITIES FOR SAVINGS, UNUSED AND UNDELIVERED SERVICES, AND INCOMPLETE POLICIES 7 (AUG. 15, 2014) (finding that the EPA paid full price for cloud services that were not delivered).

168. CONSUMER FIN. PROT. BUREAU, OFF OF THE INSPECTOR GEN., AUDIT REPORT 2014-IT-C-016: AUDIT OF THE CFPB'S ACQUISITION AND CONTRACT MANAGEMENT OF SELECT CLOUD COMPUTING SERVICES 6 (2014).

169. *Id.* at 6–7. *See* 48 C.F.R. § 52.203-13 (2010) (requiring contractors to cooperate with law enforcement investigations by disclosing certain information); 48 C.F.R. § 52.239-1 (1997) (allowing an agency access to a CSP's facilities); 48 C.F.R. § 52-215-2 (2010) (allowing the office or the inspector general to accesses the contractors' facilities and personal, among other sources, for audit).

170. USDA, *supra* note 123, at 7.

171. *Id.* at 7.

four USDA contracts that did contain a specific percentage of uptime, only three provided how uptime would be calculated—making any enforcement for non-performance against the CSP difficult.[172]

The terms of the contracts may have provided a statement of work (SOW) or other terms providing the "what" that had to be accomplished. However, the SLA describing the "how" or "how well" it had to be accomplished was often missing. This is a significant oversight for federal agencies. It also raises questions about the efficacy of the U.S. government's plan to invest billions of dollars in cloud computing. Without a good measuring stick, federal agencies are at the mercy of the CSP to determine whether a service is being performed adequately. In this determination, CSPs are not a neutral party. Consequently, the CIGIE audit recommends that all agencies should have an SLA with "clearly defined terms, definitions, and penalties for failure to meet SLA performance measures."[173] The FedRAMP issued "best practice" guide for contracting onto the cloud provides that penalties for failing to meet SLA requirements should be included in the contract with the CSP to provide "a credible consequence" for failure to meet the agreed upon service level.[174] Without these "credible consequences," CSPs risk little with sub-par performance.

D. Roles and Responsibilities of Partners and Subcontractors

In the CIGIE audit, several agencies failed to meet established best practices in their contracts regarding the use of subcontractors. The dynamic structure of cloud allows for outsourcing of critical parts of the service infrastructure, resulting in a multilayered service.[175] As a result, the connections between prime and subcontractors in cloud computing may be more tenuous than other types of IT outsourcing commonly used by government agencies.[176] Contracting CSPs often use third parties to increase

172. *Id.* (with no means to measure noncompliance, it is also difficult for the USDA to make claims for service credits).

173. CIGIE, *supra* note 58, at 7.

174. CIO COUNCIL, *supra* note 21, at 8. *See also Report of the European Union Agency for Network and Information Security on Survey and analysis of security parameters in cloud SLAs across the European public sector*, 6 (2011) [hereinafter "ENISA"] (finding service levels linked with penalties in only 44% of cases).

175. Millard, *supra* note 22, at 123–24.

176. Didier Bigo et al., *Report of Directorate-General for Internal Policies on Fighting Cybercrime and Protecting Privacy in the Cloud,* EUR. PARLIAMENT, 12 (Oct. 15, 2012), http://www.europarl.europa.eu/RegData/etudes/etudes/join/

capability and offerings or even provide their core service.[177] CSPs also take advantage of cloud by using third parties to provide aspects of their service.[178]

The result is often that major aspects of the cloud service are not visible to end-users and are performed by third-party subcontractors.[179] Because subcontractors are not employees of the primary contractor, the primary contractor may have a reduced level of control over subcontractors and the agency may have limited means to hold the subcontractor liable, depending on the terms of the agreement.[180] This is particularly true in cases where the subcontractors are working on a contract that is separate from or predates the contract between the federal agency and the CSP providing the cloud service. For example, if a Software as a Service (SaaS) provider has a long-standing or pre-existing contract with an infrastructure provider such as AWS or Google, the SaaS CSP must make adjustments in that agreement to make certain the terms governing the infrastructure being used are subject to the terms of the acquisition regulations, among others.[181]

2012/462509/IPOL-LIBE_ET(2012)462509_EN.pdf (providing that "complex mesh of contracts that are primarily concerned with abstracting the details of where and how processing actually takes place, in the interest of economic efficiency.").

177. DEP'T OF DEF., *supra* note 139, at 13. *See also* David Krebs, *Regulating the Cloud: A Comparative Analysis of the Current and Proposed Privacy Frameworks in Canada and the European Union*, 10 CANADIAN J. OF L. AND TECH. 29, 32–33 (2012).

178. DISA, *supra* note 65, at 7 (this can include "placing certain servers or equipment in third party facilities such as data centers, carrier hotels /collocation facilities, and Internet Network Access Points (NAPs)"). *See also* Millard, *supra* note 22, at 125 (discussing uncertainty and challenges in defining and applying requirements for subcontractors in the UK's G-Cloud program).

179. Primavera De Filippi & Smari McCarthy, *Cloud Computing: Centralization and Data Sovereignty*, 3 Eur. J. L. & Tech., no. 2, at 11 (2012).

180. Daniele Catteddu, *European Network and Information Security Agency*, *Report on Security & Resilience in Governmental Clouds- Making an Informed Decision*, 45 (2011) (arguing that "[s]ituations in which a CSP subcontracts the relevant services to a third party should be avoided or, at least, representations and warranties on possible sub-contractors should be included in the service agreement."). DLA Piper U.K. LLP et al., *supra* note 29, at 49 (finding that although CSPs can generally subcontract their actives, in the EU some variation among member states on whether prior approval is necessary).

181. DISA, *supra* note 65, at 7. *See also* Millard, *supra* note 22, at 15–17 (further discussing layers of cloud computing services wherein a SaaS CSP uses the services of an IaaS CSP to deliver its final product). WEITZENBÖCK, *supra* note 112, at 290–91 (providing different forms for organizing dispersed contractual networks).

An additional aspect of this dispersed structure is what has been deemed the "principal-agent problem."[182] In providing a cloud service, the incentives of the CSP (agent) may not be aligned with the Federal agency (principal).[183] The CSP and the Federal agency lack common goals outside of their stated contractual terms.[184] As a result, it can be difficult to control and evaluate a CSP's effort towards providing adequate service, security, and privacy protections.[185] Further, a CSP's interest in reporting an underperforming service potentially puts the CSP's profit interest in direct conflict with Federal agency's interest in obtaining value for its dollar. A secure system depends not only on the strength of the individual parts, but their interactions.[186] The longer the chain of providers, and the less aligned the interests of the providers are, the greater the potential the system has for weak links. For example, in cases where the subcontractors used have interests which are marginally aligned with either the CSP or the agency.

Adding to the principal-agent dilemma is whether the interests of subcontractors or sub-providers are aligned with either the CSP or the agency. Although the principal-agent problem existed prior to cloud computing in IT outsourcing, in addition to many non-IT applications, changing aspects such as shorter contract terms and limited opportunities for negotiation may have expanded the problem.[187] In traditional IT outsourcing, contracts were used to play a vital role in managing risks of the party outsourcing as well as to align the interests of the partners driving the service.[188]

---

182. JANSEN & GRANCE, *supra* note 4, at 40. *See also* George S. Geis, *Business Outsourcing and the Agency Cost Problem*, 82 NOTRE DAME L. REV., 955, 874–75 (2007).

183. To meet this problem in IT outsourcing, operating level agreements (OLA) among the parties are sometimes used to balance the success of one party on participation and cooperation with the others. Brito, *supra* note 32, at 8.

184. JANSEN & GRANCE, *supra* note 4.

185. *Id.*

186. *Id.* at 11.

187. Trevor W. Nagel, *Structuring Multi-Supplier IT Environments*, in INSIDE THE MINDS: BEST PRACTICES FOR MANAGING OUTSOURCING TRANSACTIONS, at 97–98 (Thomson Reuters, 2014) (stating that contracts entered into under these models are often long-term—lasting for periods as long as five to ten years). GEORGE KIMBALL, OUTSOURCING AGREEMENTS : A PRACTICAL GUIDE 11 (Oxford University Press 2010) (providing that in IT outsourcing, parties make a substantial investment of time and effort at the front end, and negotiation may take place over a period of a year or more).

188. Petter Gottschalk & Hans Solli-Sæther, *Critical Success Factors from IT Outsourcing Theories: an Empirical Study*, 105 INDUS. MGMT & DATA SYS. 685, 687–88 (2005) ("appropriate contractual arrangements can attenuate the leeway

In the case of federal agency cloud adoption, the EPA failed to negotiate appropriate contract terms allowing the agency to audit—or seek damages from—subcontractors used to provide the service.[189] In moving its Permit Management Oversight System (PMOS) to the cloud, the EPA entered into a contract with a CSP (primary contractor) that met many of the requirements of FedRAMP.[190] However, the agreement did not appropriately restrain or place limits on the use of subcontractors through "back-to-back" or "flow-down" clauses.[191] The primary contractor will employ the services of a subcontractor CSP to host the PMOS cloud application to be used by the EPA. In the contract the primary CSP has with the EPA, its subcontractor—the CSP actually hosting the PMOS system for the EPA—includes a disclaimer that could limit or block any agency recourse in the event of a malfunction, loss of data, or even for failing to provide basic functionality.[192] Specifically the contract term provides:

> You acknowledge and agree that your use of the services is solely at your own risk, and that except as expressly provided herein the services are provided on an 'as is' and 'as available' basis. [The subcontractor hosting the PMOS

---

for opportunism, prohibit moral hazards in a cooperative relationship, and protect each party's proprietary knowledge.").

189. De Filippi & McCarthy, *supra* note 179, at 11. "The dynamic character of the Cloud is such that any service provider could decide at any given time to out-source part of its infrastructure and operations to third-party providers, without ultimately informing the other parties to the contract."

190. U.S. ENV'T PROT. AGENCY OFF. OF INSPECTOR GEN., *supra* note 133, at 5.

191. Jörn Zons, *The Minefield of Back-to-Back Subcontracts*, 5 CONSTRUCTION L. INT'L 11, 1 (2010) (defining back-to-back agreements as "an agreement by which a main (or general/head) contractor (or another contractor down the line) aims to pass through its obligations and liabilities under its contract with the employer ('main contract') to one or several subcontractor(s)."). In government contracting, a "flow-down" clause refers to a mandatory clause that must be included in all primary as well as subcontracts. FELDMAN ET AL., *supra* note 102, at 569–70. *See* Ralph C. Thomas III, *A Primer for Negotiating Subcontracts for High-Tech Small Businesses*, 52 FED. LAW. 22, 22 (2005) (stating that "[f]ederal contracts include some provisions that the prime contractor *must* flow down certain clauses and requirements of the contract to its subcontractors." Flow down requirements originate from a number of sources including "statute, executive order, federal acquisition regulations (FARs), or the terms of a clause in the applicable prime contract.").

192. U.S. ENV'T PROT. AGENCY OFF. OF INSPECTOR GEN., *supra* note 133, at 5.

> application] expressly disclaims any and all warranties and conditions of any kind, express, implied, or statutory, including, without limitation, the implied warranties of title, non-infringement, merchantability, and fitness for a particular purpose and any warranties arising from a course of dealing, usage or trade practice.[193]

Remedies an agency has against parties, including subcontractors, where it is not in direct privity of contract remain unclear.[194] Stated differently, will the agency be able to recover losses from a subcontractor of the CSP's misuse of agency data?[195] Lack of certainty in these situations is problematic for federal agencies because they need to have accountability throughout the entire structure.[196] As noted in FedRAMP best practice guide on contracting:

---

193. *Id.* at 5.

194. Daniel J. Solove & Woodrow Hartzog, No. 2014-28, *The FTC and Privacy and Security Duties for the Cloud*, 13 BNA PRIVACY & SECURITY L. REP., 1 (2014) (discussing the unclear obligations CSPs have to protect the data of individuals with whom they have no contractual relationship). *See* De Filippi & McCarthy, *supra* note 179, at 11; WEITZENBÖCK, *supra* note 112, at 303–04 (providing that in many legal systems the freedom of contract allows parties to choose to link themselves to some actors while excluding themselves from others).

195. Sebastian Zimmeck, *The Information Privacy Law of Web Applications and Cloud Computing*, 29 SANTA CLARA COMPUTER & HIGH TECH. L. J., 453 (2012) (stating that "from a formal perspective, a privacy contract binds only the contract parties. However, because court decisions and regulatory enforcement actions can establish precedents and approved practices, privacy contracts can become relevant for third parties as well. Generally, cloud service providers and users can agree to any privacy arrangement they want."). *See also* Solove & Hartzog, *supra* note 194, at 1 (arguing that "[w]hile many companies that directly collect data from consumers are bound by the promises they make to individuals in their privacy policies, cloud service providers are usually not a part of this arrangement. It is not entirely clear what, if any, obligations cloud service providers have to protect the data of individuals with whom they have no contractual relationship. This problem is especially acute because many institutions sharing personal data with cloud service providers fail to include significant privacy and security protections in the contracts that govern the exchanges. Individuals can thus be placed at the mercy of contracts that they did not negotiate and that offer insufficient protection of their data."). McGillivray, *supra* note 16, at 238 (maintaining that in the EU, privacy rights are considered as fundamental—and thus mandatory—and the responsibilities for meeting privacy requirements cannot be easily contracted away).

196. WEITZENBÖCK, *supra* note 112, at 310 (in evaluating the application of the doctrine of privity of contract, the author finds that the contracts are a "major stumbling block" in allow members of virtual networks to hold other members (suppliers etc.) accountable).

> Generally, CSPs take ownership of their environment but not the data placed in their environment. As a best practice, cloud contracts should not *permit a CSP to deny responsibility* if there is a data breach within its environment. Federal agencies should make explicit in cloud computing contracts that CSPs indemnify Federal agencies if a breach should occur and the CSP should be required to provide adequate capital and/or insurance to support their indemnity.[197]

In the case of the PMOS application, the contract terms specifically limit the liability of the subcontractor hosting the application. If the CSP has also included a similar clause, limiting their liability for acts of subcontractors, then the EPA will have very little recourse in the case of a malfunction or even a service that does not perform or meet the needs of the agency.[198] Given this contract term, the EPA has done little to provide "credible consequences" for subcontractors mishandling or misusing important agency data.[199] If the PMOS application malfunctions or a data breach occurs, what type of damages can the EPA claim from a service provided on an "as is" basis?

Although wide disclaimers might be appropriate for free services, for the EPA, the service was not without cost. In fact, the audit found the EPA paid $2.3 million for services that were not fully delivered or did not comply with federal requirements removing many of the core risk-management points.[200] Given the EPA's purchasing power and mandate, the contract should have been negotiated and the disclaimer removed. Under this agreement, the EPA has contracted for a service that has no guarantee of being fit for the purposes stated and will be used on an "as is" basis. Although wide disclaimers are common in cloud computing, the EPA should not have accepted this term.

Requiring "flow-down" terms with subcontractors prevents accountability from being lost in the long list of parties supplying a service.[201] A primary contractor cannot dispense of its responsibilities under the Privacy Act, or other legislation, by

---

197. CIO COUNCIL, *supra* note 21, at 14. (emphasis added).

198. *See id.* (pursuant to the best practices guide, federal agencies are further required to ensure that "contracts with CSPs include CSP liability for data security.").

199. *Id.* at 8. *See also* European Union Agency for Network and Information Security (ENISA), *supra* note 174, at 6.

200. U.S. ENV'T PROT. AGENCY OFF. OF INSPECTOR GEN, *supra* note 133.

201. *See* Thomas III, *supra* note 191, at 22–23.

utilizing a web of subcontractors. However, implementing "flow-down" or "back-to-back" clauses has been problematic when applied in practice for specific agencies, as is expanded on in the following sections. Given the cloud model of offering services and contracts on a standard basis, this adjustment may be difficult for many CSPs to provide. Nevertheless, if a system of records storing PII on individuals is used to accomplish an executive agency function, certain requirements are placed on the system and its operators.[202] Specifically, where PII is stored in the system, contract clauses pertaining to the privacy requirements for keeping those records must be included in the contract between the CSP and the federal agency.[203]

E. Terms of Service—What Requirements Are Placed on the Federal User?

Terms of Service (TOS) agreements in cloud computing contracts are used to define the roles and responsibilities of the end-user of the service.[204] TOS agreements are prevalent in standard contracts and may be posted and updated on a CSP's webpage. The structure of CSP contracts vary, but TOS agreements often contain terms regarding access to data, warranties and indemnification, choice of law and forum, and rights and liabilities at the termination of the service.[205] There is however, no clear standard. As noted by one author, "[t]he nomenclature is somewhat bewildering, especially as it is often used imprecisely and interchangeably."[206] In addition to the terms presented directly in the contract, federal agencies may be bound with additional terms referenced, but not specifically listed in the agreement.[207]

---

202. 48 C.F.R. § 24.103(b)(1) (2005).

203. 48 C.F.R. § 24.104(a)–(b) (2005) (including the "Privacy Act Notification" in 48 C.F.R. § 52.224-1 and the "Privacy Act" in 48 C.F.R. § 52.224-2, respectively, in *supra* note 100).

204. CIO COUNCIL, *supra* note 21, at 6–7. What is actually included in the definition of TOS varies. In a study of standard terms and conditions offered by CSPs to end-users, researchers included acceptable user policies and privacy policies among other terms, as a TOS agreement. MILLARD ET AL, *supra* note 22, at 43–45.

205. CIO COUNCIL, *supra* note 21, at 6–7.

206. BYGRAVE, *supra* note 35, at 38 (referring specifically to Terms of Service (ToS) in light of many other categories such as End-User License Agreements (EULAs), Terms of Use (ToUs), and "Statements of Rights and Responsibilities.")

207. *Id.* at 6 (if that is the case, the best practices guide recommends that the TOS should be negotiated and agreed to prior to the contract award); *see also* DLA PIPER U.K. LLP ET AL., *supra* note 29, at 30 (Global study of cloud

Although standard TOS agreements may be a normal aspect of the cloud business model, some TOS terms are at odds with federal regulations.[208] In particular, if the TOS are not made part of the contract, or remain subject to change or variation/modification at the CSP's sole discretion, it is unlikely that the agreement is suitable for federal agencies.[209] The point of departure for federal agencies is that the roles and expectations of the parties should be clearly defined in the agreement. If the CSP retains wide latitude, or the ability to act unilaterally regarding changes to the contract, the federal agency may lose control over data and even have a difficult time assessing security aspects of the cloud service.[210]

The EPA also accepted a contract clause allowing the subcontracting CSP hosting the service to unilaterally change the contract.[211] Although the EPA's agreement with the primary contractor contained a clause requiring that "[c]hanges in the terms and conditions of this contract may be made only by written agreement of the parties," this term was not imposed on the CSP actually hosting the service.[212] Therefore, the service agreement between the prime contractor and the subcontractor (the supplier hosting the application) allows the subcontractor to make "unilateral changes to the terms of the service agreement by posting to the subcontractor's website."[213] By agreeing to this variation or modification clause, the EPA potentially loses a great

---

computing contracts finding that references to terms on a website are generally considered acceptable by courts if sufficient notice of changes is provided).

208. CIO COUNCIL, *supra* note 21, at 6.

209. Hoofnagle & Whittington, *supra* note 62, at 611. Service providers often update or change products, along with modifications to their privacy policies, which may have an impact on the way user data is collected and used.

210. DLA PIPER U.K. LLP ET AL., *supra* note 29, at 54–55 (finding that in their standard terms, many CSPs reserve the right to unilaterally amend contract terms). However, the study notes that in many European jurisdictions, these amendments are limited to actions that are "reasonable" or no "surprising or substantially unfair" based on the original agreement. *Id.* at 55–56.

211. U.S. ENV'T PROT. AGENCY OFF. OF INSPECTOR GEN, *supra* note 133, at 10.

212. *Id.* at 10.

213. *Id.* This was not the case in all federal cloud agreements. *U.S. Department of Commerce, Bureau of Census and Technology Solutions Provider, Inc.*, Contract No. YA1323-12-CN-0009, 36 (H.8 "subcontracting") (2011) (in a contract obtained by FOIA request, the following terms regarding subcontractors was provided "[s]ubcontracting will be permitted under this contract, only with the written consent of the Contracting Officer. Acceptance of an offer with subcontracting proposed shall constitute consent to such subcontracting.").

deal of control over the terms governing federal data stored by the provider.[214] Moreover, the variation clause in the contract does not even require that explicit notice of changes be provided to the EPA.[215] The types of changes a CSP might make are extremely variable. For example, the CSP might simply implement new software that has no appreciable impact on the functionality or security of the cloud service. However, even changes that may seem minor could have an impact on the EPA's ability to meet compliance requirements under FedRAMP or overall security.

It is not uncommon for CSPs to reserve the right to modify the terms of the agreement unilaterally in "free" services or those accepted on standard terms.[216] Nonetheless, it seems unnecessary for a party with significant bargaining power, such as an U.S. federal agency, to accept such terms.[217] In the CIGIE audit of federal agencies use of TOCs, auditors found that 22 contracts did not contain TOS provisions adequately defining responsibilities.[218] As a result, the roles of CSPs and agencies were not clearly provided.[219]

---

214. G. CORDERO-MOSS, INTERNATIONAL COMMERCIAL CONTRACTS: APPLICABLE SOURCES AND ENFORCEABILITY 20 (Cambridge University Press. 2014) (providing a typical contract clause preventing these types of amendments as "[n]o amendment or variation to this Agreement shall take effect unless it is in writing, signed by authorized representatives of each of the Parties.").

215. U.S. ENV'T PROT. AGENCY OFF. OF INSPECTOR GEN *supra* note 133, at 10. *See also* Krebs, *supra* note 177, at 37 (arguing that "if terms, such as where data is stored, change without notice compliance with privacy laws vanish.").

216. JANSEN & GRANCE, *supra* note 4, at 8. *See also* William Jeremy Robison, *Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act*, 98 GEO. L.J. 1195, 1214 (2010) (arguing many cloud adopters in effect pay for the service with their privacy); MILLARD ET AL, *supra* note 22, at 50–55 (finding in a 2013 study of contract terms that of the providers surveyed only one (Akamai) did not contain a variation clause).

217. *Cf.* Dan Jerker B. Svantesson, *Data Protection in Cloud Computing – The Swedish Perspective*, 28 COMPUTER L. & SEC. REV. 476, 477 (2012) (in evaluating the case of a Swedish municipality contracting with Google, Svantesson provides that "few contractual clauses so strongly indicate a power-imbalance as do clauses allowing one party to unilaterally change the terms of the contract. Indeed, on a general level, it is questionable whether a governmental actor, such as the municipality, ever should enter into a contract containing such a clause.").

218. CIGIE, *supra* note 58, at 9.

219. *See, e.g.*, USDA, *supra* note 123, at 8 (In the case of the USDA, an audit uncovered that six contracts for cloud services did not contain TOS defining roles and conduct of the CSP or agency.).

F. Access to Information: Terms Allowing the Agency to Access its Own Data

Federal agencies can expect to be sued. For federal agencies, contract disputes, challenges of procurement awards, and requests under the Freedom of Information Act (FOIA) are commonplace.[220] This reality—unavoidable litigation—means that federal agencies must be able to meet the discovery demands that litigation entails when using cloud computing. Specifically, federal agencies must be able to find, preserve, and possibly produce electronically stored information (ESI) and metadata stored with CSPs when so ordered.[221] In addition to discovery requirements, federal agencies must be able to obtain data from CSPs and subcontractors for audits, and should consider portability barriers that might inhibit the agency from obtaining their data after a service has ended.[222] In the following section these challenges are evaluated in light of agency cloud usage.

1. Federal Agencies and e-Discovery

The Federal Rules of Civil Procedure (FRCP) require the party being sued to make certain records available.[223] Pursuant to the FRCP, ESI must be provided in both civil and criminal cases where that information is in the "possession, custody, or control" of the party from whom data is sought.[224] ESI includes data from a variety of sources beyond email and final agency documents.[225]

---

220. CIO COUNCIL, *supra* note 21, at 24.

221. *See* Cindy Pham, *E-Discovery in the Cloud Era: What's a Litigant to Do?*, 5 HASTINGS SCI. & TECH. L.J. 139, 157 (2013) (maintaining that "federal courts have adopted the Rule 37(e) comments to hold a party's preservation duty attaches when the party reasonably anticipates litigation."). Metadata is "data about data." National Information Standards Organization, *Understanding Metadata* 1 (2004), *available at* http://www.niso.org/publications/press/UnderstandingMetadata.pdf.

222. *See* Robert H. Carpenter, Jr., *Walking From Cloud To Cloud: The Portability Issue In Cloud Computing*, 6 WASH. J.L. TECH. & ARTS 1, 12–14 (2010).

223. *See* CIO COUNCIL, *supra* note 21, at 23–25, 24 n.53. (explaining e-discovery requirements and citing Fed. R. Civ. P.: Rule 16, Rule 26(f), Rule 26 (b)(2) on Inaccessible ESI, Rule 33 on ESI Interrogatories, and Rule 34(b) on Form ESI).

224. Fed. R. Civ. P. 26(a)(1)(A)(ii).

225. USPS, *supra* note 77, at 34 ("ESI includes not only electronic mail, attachments, and other data objects stored on a computer system or storage media, but also any associated metadata, such as dates of object creation or modification, and non-rendered file content (i.e., data that is not explicitly displayed for consumers).").

Limits to production exist, including instances where producing the ESI has an "undue burden or cost." However, even if agency data is under the control of a CSP (or a CSP's subcontractor) the agency is still required to produce the ESI.[226] The general standard applied for being able to produce ESI is control over the document, not the location, domestic or foreign, of the data storage.

Once an agency has notice of litigation, or if litigation can be reasonably anticipated, the agency is required to take steps to preserve information.[227] If an agency fails to do so, they risk sanctions for spoliation of evidence.[228] If the agency fails to produce or preserve ESI as ordered, severe penalties may result.[229] For federal agencies, this requires that they are able to identify and preserve information they store with CSPs.[230] Where agency information is stored on infrastructure not owned or operated by the agency; obtaining the necessary ESI to be transferred to a third party requires cooperation with the CSP.[231] Complying with agency discovery requests may be cumbersome from the perspective of the CSP. More concretely, identifying and locating, separating, and saving ESI for discovery purposes may disrupt operations or impact CSP data retention schedules.[232] This is particularly problematic in the cloud model. If many users of the infrastructure are making these types of requests, the CSP may have difficulty meeting all the requests while also operating its infrastructure in an efficient manner–ultimately impacting the effectiveness and quality of the service. When complying with

---

226. Pham, *supra* note 221, at 156–57.

227. *See* Carmeli, *supra* note 146, at 7 (citing *Cyntegra, Inc. v. IDEXX Labs.*, No. CV 06-4170 PSG (CTx) 2007 WL 5193736, at *5 (C.D. Cal. Sept. 21, 2007)).

228. *Id.* at 7 (citing *Cyntegra, Inc. v. IDEXX Labs.*, No. CV 06-4170 PSG (CTx) 2007 WL 5193736, at *6 (C.D. Cal. Sept. 21, 2007)).

229. *See* Fed. R. Civ. P. 37(e); Fed. R. Civ. P. 37(e) advisory committee notes.

230. Pham, *supra* note 221, at 156–57.

231. Carmeli, *supra* note 146, at 2. *See also* M. James Daley, Steven C. Bennett & Natascha Gerlach, *Storm Clouds Gathering for Cross-Border Discovery and Data Privacy: Cloud Computing Meets the U.S.A. Patriot Act*, 13 SEDONA CONFERENCE J. 235, 238 (2012) (stating that "U.S. courts have, on many occasions, ordered the production of information in the possession of foreign entities, where the court has jurisdiction over a related entity in a U.S. proceeding.").

232. Pham, *supra* note 221, at 172. Preserving ESI also detracts from the CSPs ability to effectively use its resources, raising costs. Araiza, *supra* note 22, at ¶¶ 31–32.

discovery requests, the CSP further risks disruption of the service and inadvertent disclosure of data stored on the service by other customers.[233]

Even if data management is outsourced, the federal agency remains responsible for meeting discovery requirements.[234] At a minimum, this requires that data is stored for sufficient time periods to allow agency access to such data over a matter of years. Equally important, proper systems must be in place to make certain that data stored by a CSP (and their subcontractors) is accessible to the agency. The acquisition regulations also require that certain records be kept for the purposes of audit.[235] In the case of a CSP provider, this requires that the agency being audited grants access to the Office of Inspector General (OIG) for the purposes of examining transactions related to the contract between the CSP and the executive agency. This could be for the purposes of e-discovery, criminal or civil forensic investigations, among other reasons. The right to inspect records is not limited to the primary contract but also to relevant subcontracts.[236] In addition to the right to inspection, the acquisition regulations also require that that the primary contractor retains relevant information until 3 years after final payment of the contract.[237]

Given the results of CIGIE and individual agency audits, federal agencies have done little to secure access to their information in the event of litigation. Many agencies have failed to meet the threshold required by the Acquisition Regulations and the FedRAMP program. For example, in reviewing NASA's contracts, none of the agreements contained specific requirements for meeting e-discovery requirements.[238] Similarly, five of the six contracts the USDA had with various cloud providers did not include any data preservation requirements.[239] In addition to

233. Araiza, *supra* note 22, at ¶ 26.

234. Pham, *supra* note 221, at 160.

235. 48 C.F.R. § 52.215-2(d)–(f) (2015).

236. 48 C.F.R. § 52.215-2(d)(1) (2015) (requiring that the "Comptroller General of the United States, or an authorized representative, shall have access to and the right to examine any of the Contractor's directly pertinent records involving transactions related to this contract or a subcontract hereunder and to interview any current employee regarding such transactions.").

237. 48 C.F.R. § 52.215-2(f) (2015). Meeting these requirements has been difficult in practice. In its recent cloud adoption, the Consumer Financial Protection Bureau failed to obtain terms allowing access to contractor records pursuant to 48 C.F.R. § 52.215-2. *See* CONSUMER FIN. PROTECTION BUREAU, *supra* note 168, at 6.

238. NASA Office of the Inspector General (OIG), *supra* note 20, at tbl. 12.

239. USDA, *supra* note 123, at 7.

violating acquisition regulations and federal computing standards, this oversight could result court ordered sanctions (monetary and otherwise) for failure to comply with discovery requirements.

2. Accessing Data after Service Termination: A Plan for Walking Away

Federal agencies should make certain that when they leave the cloud service, they are able to obtain their data in a format they can access.[240] By making the contract explicit on this point, and providing that the agency is the owner of the data they store with the CSP, the agency can mitigate transmission delays.[241] If removal of agency data is subject to a "data hostage clause," requiring that the agency pay all debts or settle all disputes before data can be removed, the agency may find itself paying for services that were not preformed adequately just to keep operations running.[242]

For the Federal government, the problem of retaining data after the end of a service has not been purely a hypothetical one. In 2010, the Department of Labor (DOL) entered into a contract with Global Computer Enterprises (Global Computer) to provide a cloud computing service for financial management.[243] While providing cloud computing services for several agencies, Global Computer was under investigation by the U.S. Department of Justice and its offices were raided by the Federal Bureau of Investigation.[244] Federal law enforcement agencies asserted that

---

240. Portability challenges may come from different sources. On the one hand, Cloud adopters may have a limited ability to move to a new provider as a result of reliance on a specific CSP. Cloud adopters may become dependent one CSP's proprietary technology to the point that moving to another CSP would negatively impact business processes.

241. CIO COUNCIL, *supra* note 21, at 26 (providing that federal agencies should have contract terms requiring detailed ESI storage processes including specifying who will pay for searches and identification of ESI, and procedures for the ESI "chain of custody.").

242. Carpenter, Jr., *supra* note 222, at 3–4, 12–14.

243. Debtor's Motion, Memorandum and Affidavit at ¶ 7. In re: Global Computer Enterprises, Inc., No. 14-13290-RGM, 2014 WL 4700821 (Bnkr. E.D. Va. 2014). *See also* Jason Miller, *Labor, GSA Forced to Buy Systems from Bankrupt Vendor,* FED. NEWS RADIO (Sept. 8, 2014, 4:05 AM), http://federalnewsradio.com/management/2014/09/labor-gsa-forced-to-buy-systems-from-bankrupt-vendor/.

244. *Id. See* Debtor's Motion, Memorandum and Affidavit at ¶ 13, *In re Global Computer Enterprises, Inc.*, No. 14-13290-RGM, 2014 WL 4700821 (Bnkr. E.D. Va. 2014) (providing details on the Department of Justice investigation and legal expenses). *See also* Miller, *supra* note 243 (noting that Global Computer spent more than $4.6 million on legal fees, significantly

Global Computer was employing personnel prohibited from handling federal data due to their citizenship or immigration status.[245] Legal expenses resulting from federal charges played a central role in the Global Computer eventually declaring bankruptcy, leaving the DOL with uncertain access to its data.[246]

At the time it filed for bankruptcy, Global Computer was processing over $170 billion worth of DOL transactions with its cloud application.[247] In a DOL report evaluating the risks of Global Computer's control over agency data, the DOL Inspector General noted that the DOL had not developed a recovery plan in the case of disruption of access to its financial data, which could result in "serious consequences."[248] In other words, the DOL had become overly dependent or "locked-in" to its CSP.[249] Specifically, the DOL failed to "include language in its contract that required [Global Computer] to create a data extract process and return the data to the DOL in a machine-readable form."[250] Because the service was so customized, the agency was extremely dependent on Global Computer. The DOL determined that without access to Global Computer's employees, licenses, and other intellectual property owned by Global computer, any transition to a new provider would fail.[251]

---

inhibiting its ability to operate); Adam Mazmanian, *Cloud Contractor to Pay U.S. $9M to Settle False Claims Charges,* WASHINGTON TECH., (May 8, 2015), http://washingtontechnology.com/articles/2015/05/08/gce-false-claims.aspx (stating that GCE settled the case against it for $9 million—money that would come out of its Chapter 11 proceedings).

245. Miller, *supra* note 243.

246. Debtor's Motion, Memorandum and Affidavit at ¶¶ 13–15, *In re Global Computer Enterprises, Inc.,* No. 14-13290-RGM, 2014 WL 4700821 (Bnkr. E.D. Va. 2014) (Global Computer petitioned the bankruptcy court to sell its assets to the DOL including interfaces, software licenses, system documentation, and servers necessary to keep the DOL's application running.).

247. *Id.* at ¶ 11.

248. Memorandum from Scott S. Dahl, Inspector Gen., U.S. Dep't of Labor, to Christopher P. Lu, Deputy Sec'y, Dep't of Labor at 2 (Aug. 15 2014), *available at* http://www.oig.dol.gov/public/reports/oa/2014/22-14-007-01-001.pdf.

249. *See* USPS, *supra* note 77, at 10–13 (discussing agency "lock-in" risks on various cloud platforms including Software as a Service (SaaS), Platform as a Service (PasS), and Infrastructure as a Service (IaaS)).

250. Bart Perkins, *Lessons to Be Learned from a Project Nightmare*, COMPUTERWORLD (Mar. 11, 2015, 11:00 PM), http://www.computerworld.com/article/2895066/lessons-to-be-learned-from-a-project-nightmare.html.

251. Debtor's Motion, Memorandum and Affidavit at ¶¶ 33–36, *In re Global Computer Enterprises, Inc.*, No. 14-13290-RGM, 2014 WL 4700821 (Bnkr. E.D. Va. 2014) (explaining the contract with the DOL to provide servers, licenses, and other support to transition the service).

As the DOL learned the hard way, unclear contract terms regarding data ownership can cause difficulties for an agency trying to obtain its data if the CSP providing its services goes bankrupt.[252] In the case of the DOL, the Software as a Service contract terms with it CSP were unclear on whether data must be returned after termination of the service.[253] In its public notice justifying the contract to buy assets held by Global Computer, the agency provided:

> As such, all applications and data are hosted by the contractor at its site, and the government does not have access to the 'back end' of the system. Since June 5, 2012, the government has been seeking access to the full DOL dataset hosted by GCE to no avail, therefore at this point in time GCE is the only source available to perform this service.[254]

Based on the above assessment, DOL did not have the ability to obtain its data or keep the system running without purchasing Global Computer's data—which also happened to be the agencies. To obtain its data, and keep services running, the DOL (and other agencies) spent over $23.5 million.[255]

III. FEDRAMP COMPLIANCE: ROOM FOR AGENCY IMPROVEMENT

Although federal agencies procured cloud computing under the FedRAMP program, many either failed to include terms required under the program or failed to obtain program compliant contracts by program deadlines.[256] In addition to failing to apply

---

252. Jill R. Aitoro, *The Mysterious Bankruptcy Case of Global Computer Enterprises*, WASHINGTON BUSINESS JOURNAL (Sept. 12, 2014, 2:36 PM), http://www.bizjournals.com/washington/blog/fedbiz_daily/2014/09/the-mysterious-bankruptcy-case-of-government.html (last updated Sept. 17, 2014, 5:55 PM).

253. Jason Miller, *Inside the Reporter's Notebook: Labor Pinched by Poor Cloud Contracting; Financial Shared Services Progresses*, FED. NEWS RADIO (Dec. 9, 2013, 6:47 AM), http://www.federalnewsradio.com/?nid=533&sid=3521104.

254. Public Notice, Office of the Chief Financial Officer, Department of Labor, *Justification for Other than Full and Open Competition Financial Data Warehouse (FDW) Data Feed Solicitation Number: 132-1494-791*, at 2 (2013).

255. Miller, *supra* note 243.

256. Friedman, *supra* note 111, at 2 (quoting Memorandum from Gregory H. Friedman, Inspector Gen., Dep't of Energy on the Audit Report of "The Department of Energy's Management of Cloud Computing Activities" to the Secretary of the Dep't of Energy (Sept. 19, 2014) (noting that OMB required that agencies utilize cloud service providers that met the cybersecurity requirements

specific FedRAMP standards, noncompliance with federal acquisition regulations was also widespread among agencies. Like FedRAMP, compliance with the acquisition regulations are mandatory for federal agencies using cloud computing. The regulations provide that "[c]ontracting officers are responsible for . . . necessary actions for effective contracting, ensuring compliance with the terms of the contract, and safeguarding the interests of the United States in its contractual relationships."[257]

Although the omissions of provisions allowing agencies to inspect or audit CSPs were particularly widespread, most agencies failed to negotiate other key elements in their cloud agreements. For example, it was determined that the Department of Energy lacked a "majority" of key terms in its contracts with CSPs.[258] In addition to non-compliance with general acquisition regulation standards, many agencies failed to meet the cloud specific security and organization requirements mandated by the FedRAMP program.[259] Based on the CIGIE audit, one of the most visible agency shortcomings found in the audit—arguably the most woeful case—was that of the EPA. In addition to deficiencies in meeting acquisition regulations and FedRAMP requirements, EPA contracts were missing SLA agreements, omitted NDAs, and contained contract terms inconsistent with federal best practices. The EPA failed to use an authorized CSP and did not complete an audit from a Third-Party Assessment Organization (3PAO).[260] An examination of USDA contracts revealed that only four of the six met FedRAMP compliance requirements by the deadline.[261] In the case of the Department of Energy, contracting officials were of the opinion that "they were not required to comply with FedRAMP."[262] As a result, many of the FedRAMP requirements were not evaluated or incorporated.

---

of FedRAMP by June 2014, however, the Department of Energy, among others, failed to meet this deadline)).

257. 48 C.F.R. § 1.602-2 (2015).

258. Friedman, *supra* note 111, at 2.

259. *See, e.g.*, EPA, OFFICE OF INSPECTOR GEN., *supra* note 133, at 18–21 (evaluating non-compliance by the EPA).

260. *Id.* at 20.

261. Office of Inspector General USDA, *supra* note 123, at 11. This was largely due to the failure of the agency to properly define the systems as cloud and plan accordingly.

262. Friedman, *supra* note 111, at 4–5. As a result of this misinformation, DOE contracting officials were not working with cloud providers to update contracts.

In some cases, the contracting agencies negotiated terms that complied with Acquisition Regulations in their agreement with the primary contractor, but failed to impose mandatory contract requirements on other parties accessing or processing federal data. Missing mandatory requirements in the areas of access, audit, and preservation of federal data were particularly prevalent.[263] Even in areas where agreements were in place with primary contractors, they were not adequately imposed on subcontractors/third parties actually hosting federal data. To expand further on the example of the EPA PMOS application discussed above, the EPA failed to secure contractual guarantees throughout the chain of suppliers providing the service. In addition to limitations on liability, the agreement only allows the EPA to access the facilities of the prime contractor, but not the facilities of the subcontractor actually hosting the application.[264] As a result, a crucial part of any audit would be restricted. In its contract, the EPA failed to make certain that acquisition regulations requirements relating to audit and access "flowed-down" to subcontractors, limiting forensic investigations.[265]

Other agencies, including those with sensitive missions, placed low and moderate impact services on cloud computing services, without providing proper protections. For example, the OIG found that "none of" the five contracts the National Aeronautics and Space Administration's (NASA) entered into "came close to meeting recommended best practices."[266] Among other shortcomings, NASA did not negotiate contract terms with providers and instead accepted standard contract terms.[267] These standard agreements failed to meet cornerstone requirements of FedRAMP including federal record management, privacy, and security requirements.[268] Considering these points, the audit

263. VanRoekel, *supra* note 64, at 5 (requiring that "[e]ach Executive department or agency shall . . . (iii) [e]nsure applicable contracts appropriately require CSPs to comply with FedRAMP security authorization requirements.").

264. EPA, OFF. OF INSPECTOR GEN. *supra* note 133, at 12–14.

265. *Id.* at 12–13. EPA contracts do not apply 48 C.F.R. § 52.203-13 or 48 C.F.R. § 52.239-1 to subcontractors, even if terms are contained in the agreement with the primary contractor. Further, the EPA has not included 48 C.F.R. § 52.215-2 with the primary or subcontractor; *see also* CIO COUNCIL, *supra* note 21, at 15 (providing that agency contracts should allow for forensic investigations).

266. OFF. OF AUDITS, OFF. OF THE INSPECTOR GEN., NASA, *supra* note 20, at 12.

267. *Id.* at iv.

268. *Id.*

determined that NASA's contracting missteps had the potential to cause serious disruptions to agency operations.[269]

There were also some brighter spots in the audit. The Consumer Financial Protection Bureau contracts with the CSP Amazon Web Services, which used Deloitte's Compliance Analysis Toolkit to monitor contracts and cloud computing for compliance, met FedRAMP requirements in a variety of areas including SLAs, security, and other federally mandated requirements.[270] The Consumer Financial Protection Bureau audit found the contracts included clauses covering important aspect of the parties' relationship including security and service expectations.[271] However, deficiencies were still present. First, the contracts did not include penalties if the CSP failed to meet terms in the SLA.[272] Second, the contracts omitted important clauses required for investigative purposes, e-discovery, and federal records requirements.[273]

Based on the audits, and considering the missing terms, federal agencies have a ways to go in properly implementing cloud computing. Although agencies may not have focused on contracts sufficiently when the program was rolled out, FedRAMP has released new contract terms. These terms, and their ability to meet the contracting deficiencies enumerated in the recent audits discussed above are evaluated in the next section.

IV. STANDARD AND REVISED CONTRACT TERMS USED IN FEDRAMP: A WAY FORWARD?

Acknowledging that adopting cloud computing technology requires a great deal of technical expertise, the federal government, through NIST, has generated and imposed technical standards on its agencies to meet security challenges. A point that appears to have received less attention, at least in early federal cloud adoption and the FedRAMP program, is the role of contracts in managing security risks for federal agencies.[274]

---

269. *Id.* at iii (finding that on five occasions NASA failed to address business and security risks in its cloud computing agreements).

270. CONSUMER FIN. PROTECTION BUREAU, *supra* note 168, at 2. At the time of the audit, agency contracts were valued at $185 million.

271. *Id.* at 3.

272. *Id.* at 6.

273. *Id.*

274. VanRoekel, *supra* note 64, at 3–4. However, this need was envisioned in the authoritative OMB memorandum mandating FedRAMP compliance for federal agencies in 2011, which provided that the General Services

Guidance provided has been very general. Therefore, many agencies failed to negotiate contract terms as anticipated in the "cloud first strategy" and required by the FedRAMP program.[275] Based on contracts obtained by the author through FOIA requests, many of the contract precedents used predate cloud computing and are geared much more toward outsourcing or other long-term IT hosting agreements.

When it comes to procuring cloud computing, many potential users find themselves presented with a complex contract that they must evaluate for compliance based on limited guidance and resources. Even with some guidance on what the legal requirements are, understanding how these requirements are represented and must be applied in the CSPs infrastructure, is beyond the knowledge of many users.[276] However, unlike federal agencies, most consumers, SMEs, and municipalities do not have full-time legally trained staff with decades of experience in IT system procurement to examine their agreements. Even given the available guidance for federal agencies in the form of a "best practices guide" for contracting, major oversights occurred.[277] Although the guide may have provided some assistance, it did not contain specific or mandatory standard clauses that must (or could) simply be added to the contract with a CSP. In the following section, I evaluate aspects of the "FedRAMP Standard Contract Language" issued in 2012 and the more recently-released Control Specific Contract terms provided by the FedRAMP program in 2014.[278] I consider whether the new "control specific" terms might increase compliance and lessen some of the problems made apparent the 2014 agency audits.

Administration (GSA) would "[d]evelop and make available to Executive departments and agencies templates that can satisfy FedRAMP security authorization requirements through standard contract language and service level agreements (SLAs) for use in the acquisition of cloud services."

275. *See, e.g.*, Kundra, *supra* note 2.

276. Svantesson, *supra* note 217, at 477 (stating that a contract between a Swedish municipality and Google was effectively so complex that it "constituted a breach of the applicable [Swedish] law.").

277. CIO COUNCIL, *supra* note 21. In the best practices guide, contract terms were discussed broadly and may have been difficult to match or apply to the standard contracts being offered to the agencies by CSPs.

278. FedRAMP Standard Contract Language (June 27, 2012), https://www.fedramp.gov/files/2015/03/FedRAMP_Standard_Contractual_Clauses_062712_0.pdf; *see also* GENERAL SERVICES ADMINISTRATION, *FedRAMP Control Specific Contract Clauses: Version 2.0* (June 6, 2014), http://www.gsa.gov/graphics/staffoffices/FedRAMP_Control_Specific_Clauses_062712.pdf.

The "standard" FedRAMP contract terms issued in 2012 focused largely on technical aspects of the FedRAMP program that should be included in cloud computing agreements. The contract template provides assistance to agencies procuring cloud computing, but is not a complete or standalone agreement. The template requires that agency legal counsel evaluate and add necessary terms and conditions specific to their agency's mission. Consequently, the standard clauses were limited to basic security requirements for privacy and security of government data in addition to more specific areas of the FedRAMP program including security assessments. To meet security requirements, the terms focus on the roles of the agency and the provider. However, the terms are incomplete and do not cover many of the aspects in the FedRAMP best practices contracting guide.

On the other hand, the terms issued in 2014 are very specific in certain areas. Particularly, in requiring that government data is owned by the agency and that specific protections must be in place to protect personal data and other sensitive data. For example, the terms for "FedRAMP Privacy Requirements" provide:

> (a) The Contractor shall not publish or disclose in any manner, without the Contracting Officer's written consent, the details of any safeguards either designed or developed by the Contractor under this contract or otherwise provided by the Government.[279]

Although the terms are much more specific and provide some references to NIST standards, there is a level of interpretation and layer of specificity that must be added to obtain optimal protection. The terms also require that the CSP go outside of the contract document. For example, a term on "FedRAMP Security Compliance Requirements" provides that:

> The contractor shall implement the controls contained within the FedRAMP Cloud Computing Security Requirements Baseline and FedRAMP Continuous Monitoring Requirements for low and moderate impact system (as defined in FIPS 199). These documents define requirements for compliance to meet minimum Federal information security and privacy requirements for both low and moderate impact systems. While the FedRAMP

279. *Id.* at 3–4 ("Privacy or Security Safeguards").

> baseline controls are based on NIST Special Publication 800-53, Revision 3.[280]

The control specific contract terms were released in 2014 as a template—not a set of mandatory terms. Therefore, agencies may modify or deviate from the terms.[281] However, unlike the best practices guide previously provided by the CIO, the template provides specific clauses that agencies may insert directly into agency contracts rather than providing a general list of principles.

The revised terms also provide much more detailed security requirements including the standards that the CSP hosting agency data must comply with in the areas of encryption, access, and authentication. The security requirements are tailored depending on where the data resides in the usage or cloud consumption life cycle providing specific requirements to address risks and other legal requirements.[282] The template contract terms also focus specifically on agents of the CSP handling data including contract terms providing for specific background checks and other security requirements.

In addition to providing terms with specific technical requirements, the template also provides clauses requiring that data, both at rest and in transition, must be guaranteed to reside within a specific jurisdiction.[283] This may address a problem common in the CIGIE audit—that is, many of the contracts did not provide any specific location for the storage of government data.[284]

---

280. GENERAL SERVICES ADMINISTRATION, *supra* note 278, at 6 ("The contractor shall generally, substantially, and in good faith follow FedRAMP guidelines and Security guidance. In situations where there are no procedural guides, the contractor shall use generally accepted industry best practices for IT security.").

281. GENERAL SERVICES ADMINISTRATION, *supra* note 278 (providing guidance "that might be used for FedRAMP cloud computing projects.").

282. *Id.* at 2 (for example, audit retention requirements).

283. *Id.* at 1; *see also* CIO COUNCIL, *supra* note 21, at 22 (providing that federal agencies need to understand the CSP's infrastructure (including subcontractors) to determine the risks of jurisdictional exposure resulting from the laws of other countries that are potentially applicable when federal data in motion, at rest, or is stored outside of the U.S.).

284. Michael A. Magalski, *Management Advisory Report: Cloud Computing Contract Clauses: Report Number SM-MA-14-005* ii (Apr. 30, 2014), https://www.uspsoig.gov/sites/default/files/document-library-files/2014/sm-ma-14-005.pdf (stating that initially the USPS failed to include location or require data location in its contracts with CSPs). The Postal Service's internal rules require that all servers, including backup servers, reside in the contiguous U.S. for the reason that "data stored outside of the U.S. cannot be protected under the Privacy Act . . . ." USPS, *supra* note 77, at 39.

As the terms focus on the data flow, rather than the location of the contracting CSP, it will likely also apply to subcontractor CSPs. The terms do not require that the CSP provide the location or names of all providers, which could hinder the CSPs ability to subcontract or outsource services. Rather, it simply requires that all storage, including storage by subcontractors, must take place within a specific zone provided in the contract.[285]

In addition to securing the level of encryption and location of data, the model terms also provide for specific retention periods of ESI. As discussed above, e-discovery and other audit requirements specify that data must be available in the case of litigation as well as other purposes like FOIA requests and archive requirements.[286] Certain records are to be transferred to the National Archives and Records Administration for archive purposes while others are deleted according to federal retention schedules.[287] In addition to protecting data stored and transferred, the template terms also focus on very specific aspects of incident reporting, particularly where personal information is involved. For example, the template term requires that "[a]ny incident that involves compromised PII must be reported to the United States Computer Emergency Readiness Team within 1 hour of detection regardless of the incident category reporting timeframe."[288]

If the terms provided in the template are included in future agency contracts with CSPs, the standard for compliance will be more attainable. Rather than standard terms providing vague standards like "best efforts" or "industry standards," the model terms provide specific and measurable requirements (e.g., FIPS 140-2 level 2).[289] However, considering both the 2012 and 2014 terms, several problems are apparent. Although the goal of the FedRAMP program is to provide a standardized process that can

---

285. Millard, *supra* note 22, at 99–103 (In a study of contract terms, researchers noted the trend of larger CSPs to offer "'regional zones' in which a customer may be assured that data will remain.").

286. *See* 36 C.F.R. § 1236.20–1236.22 (preserving electronic records).

287. NATIONAL ARCHIVES AND RECORDS ADMINISTRATION (NARA), *Bulletin 2010-05: Guidance on Managing Records in Cloud Computing Environments* ref. 8 (Sept. 08, 2010), http://www.archives.gov/records-mgmt/bulletins/2010/2010-05.html.

288. GENERAL SERVICES ADMINISTRATION, *supra* note 278, at 3.

289. *Id.* at 1–2 (citing NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST), SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES: FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION 140–142 (FIPS PUB 140–42) (2001), http://csrc.nist.gov/publications/fips/fips140-2/fips1402.

be used many times by agencies, the template or model contract provided on the FedRAMP website is only partial. Standard "complete" contracts are not provided. When approaching a CSP, the agency has the difficult task of first determining which of the terms "should" be included and which "must" be included from the standard template based on the FedRAMP program and their internal agency requirements. The agency must then assess how the FedRAMP terms ought to fit into the standard contracts offered by CSPs and which aspects must be changed if compliance with FedRAMP, and federal law, is to be achieved. Based on agency audits, some have failed to complete this analysis and simply accepted standard terms offered by the CSP.

By not providing contracts or contract clauses that can be incorporated into any contract with a CSP, the FedRAMP program risks losing some of its ability to standardize. If all agencies in a sense must pick and choose, the cost of contracting and evaluating cloud computing services will likely go up—and instances of compliance with the complex legal landscape will remain uneven. It will also require that all agencies have a high level of competence in the legal requirements of cloud computing. In addition to patchy compliance, the benefits offered by standard cloud offerings may be reduced. The FedRAMP program may well benefit from a modified "write once use many times" approach to contracting as well as security authorizations.

At the same time, an overly standardized approach may be unrealistic—and even undesirable—when applied to the cloud computing market. After all, one of the most desirable aspects of contract is its "flexibility, simplicity, and predictability, not least relative to statute."[290] Although standardized agreements provide some certainty through uniformity and reduced transaction costs, overly rigid agreements would limit the flexibility of the federal government to take advantage of diverse cloud offerings. Agencies contracting for cloud also need a measure of flexibility to address the evolution of cloud technology in addition to changing needs within agencies. Even the best planned procurement system and accompanying contracts are unable to predict the needs of parties on all sides.[291] This is particularly true if cloud computing services

290. BYGRAVE, *supra* note 35, at 136. However, the author also notes limits to contract when the structure becomes "so complex and hierarchical that it suffers from some of the weaknesses typically attributed to legislation."

291. MILLARD ET AL., *Cloud Contracts: Looking At Clouds From Both Sides Now*, *supra* note 22, at 109–12. G-cloud provides for a standard "framework" contract between the government and CSPs providing different

are employed by agencies over many years as the technology and needs of the users will likely change. If FedRAMP terms become inflexible, they may have the unwanted result of limiting the uptake of cloud computing or significantly reducing the advantages of cloud.[292]

The security standards provided in FedRAMP may be state of the art and have the potential to provide the federal government with the potential to access the cloud. However, to be effective, they must be consistently applied and followed. In the case of the agencies reviewed in the audit, the gap between procedure and execution in contracts was surprisingly wide. This suggests that if cloud computing is to become a central aspect of the U.S. government's IT consumption plan, it must be implemented consistently. In the next section, some potential patches and a way forward are examined.

A. Agency Specific Approaches—Individual Contracts on a Standard Basis?

In addition to the terms provided for the FedRAMP program above, individual agencies are adding additional layers of contract terms applicable to their use of cloud computing. For example, the DoD and the United States Postal Service (Postal Service) have released terms containing specific clauses on areas not included in either the FedRAMP control specific terms or the best practices guide. The Postal Service has drafted additional standard terms aimed at protecting agency data from being repurposed and used for behavioral advertising or behavioral targeting.[293] Under these

---

cloud services (IaaS etc.). *Digital Marketplace guidance:* https://www.digitalmarketplace.service.gov.uk/g-cloud/framework#the-g-cloud-framework (last visited Feb. 23, 2016). If services are procured under this agreement, buyers and suppliers still need to sign a 'call-off contract' for each service procured through a framework. *Id.* Although the contract terms are much more detailed than available FedRAMP templates, they can be adapted and allow for some room for specification.

292. *See* KUNDRA, *supra* note 2 at 7 (discussing government savings based on cloud adoption).

293. FED. TRADE COMM'N, FTC STAFF REPORT: SELF-REGULATOR PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING 42 (2009), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf (behavioral advertising is defined by the FTC as "[t]he tracking of a consumer's online activities over time, including the searches the consumer has conducted, the web pages visited, and the content viewed in order to deliver advertising targeted to the individual consumer's interests."). *See also Opinion of the Data Protection Working Party on Online Behavioural*

terms, the Postal Service requires that "[t]he Contractor shall use Government related data only to manage the operational environment that supports the government data and for no other purpose unless otherwise permitted with the prior written approval of the Contracting Officer."[294] The term further provides that "The CP [CSP] must not analyze Postal Service data anonymously and use it for their purposes or share it with third parties."[295] Here, the Postal Service makes the point that even if a CSP makes the data "anonymous," it cannot be used for advertising or other purposes.[296]

In addition to the terms above, the Postal Service provides additional criteria in the form of a cloud computing guide that must be met by a CSP storing Postal Service data. In addition to requiring that the CSP's headquarters and infrastructure are located in the U.S., if the CSP "uses other companies to provide services (i.e., subcontracted out or outsourced), the infrastructure associated with those services must be located in the contiguous United States."[297] The guide includes other important aspects including requiring back-to-back contract terms.[298]

In 2015, the DoD also updated selected contract terms in a "Class Deviation" providing terms that must be included in any cloud computing contract.[299] In addition to being obligatory, the terms generally require a more restrictive use of government data than the "control specific" contract terms provided in the FedRAMP template.[300] DoD terms include an expanded definition of government data to "any information, document, media, or machine readable material, regardless of physical form or

---

Advertising; (June 22, 2010) (WP-171), available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf (providing overview of concept and regulation in the EU); *see generally* Yuen Yi Chung, *Goodbye PII: Contextual Regulations for Online Behavioral Targeting*, 14 J. HIGH TECH. L. (2014).

294. DEP'T OF DEF., *Class Deviation—Contracting for Cloud Services* 4 (DEPART. OF DEFENSE ED., 2015).

295. USPS, *supra* note 77, at 39.

296. *See, e.g.*, Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010) (discussing the difficulty of effectively anonymizing data).

297. USPS, *supra* note 77, at 41. *But see* Sasha Segall, *supra* note 50, at 1138–39 (discussing challenges to the GSA policy of limiting data centers to the U.S. and arbitrarily limiting expansion in countries with robust cloud sectors such as India).

298. USPS, *supra* note 77, at 42.

299. DEP'T OF DEF., *supra* note 294, at 3–5.

300. *Id.* at 3–5.

characteristics, that is created or obtained in the course of official Government business."[301] After broadly defining data, the term specifically limits use of government data to manage "the operational environment that supports the government data and *for no other purpose* unless otherwise permitted with the prior written approval of the Contracting Officer."[302] Like the term added by the Postal Service, federal agencies are concerned that their data may be repurposed and used for other objectives.[303] These may include targeted advertising among other commercial uses.[304]

Like the Postal Service guide, the DoD terms not only focus on limiting use to primary contractors, but also ensuring that other suppliers with access are bound by the same terms. Specifically, a DoD term under the heading "Subcontracts" provides that "[t]he Contractor shall include the substance of this clause, including this paragraph (g), in all subcontracts, including subcontracts for commercial items."[305] The remit of this clause is to ensure that back-to-back contract terms are in place that will create a chain of clear obligations for security. Moreover, it provides for a clear line of liability if a partner or supplier misuses DoD data. This term, if it can be bargained for and included as required, will limit oversights such as the broad exclusions for CSP subcontractors accepted by the EPA discussed above. The DoD has acknowledged the need for privity of contract with CSP hosting the data elsewhere and provides that if subcontracting occurs, the agency should ensure that the prime contractor retains "operation configuration and control of DoD data."[306]

Additional terms like those offered by the Postal Service and the DoD may increase security. However, requiring CSPs to take

---

301. *Id.* at 3.

302. *Id.* at 4 (for example, data loss or spillage, often discussed technically, was given the following contractual language: "means an unauthorized transfer of classified data or controlled unclassified information to an information system that is not accredited for the applicable security level of the data or information.").

303. Hayes, Kesan & Bashir, *supra* note 85, at 244 (evaluating secondary use and repurposing of data).

304. Parker, *supra* note 100, at 407–08 (citing the federal government's failure to obtain contract terms prohibiting CSPs from using PII stored on the services for commercial purposes).

305. DEP'T OF DEF., *supra* note 294.

306. DISA, *supra* note 65, at 24. *See also* GREGORY KLASS, CONTRACT LAW IN THE UNITED STATES 161 (Kluwer Law International 2nd ed. 2012) (stating generally that a contract confers legal rights and imposes legal obligations only on individuals who are parties to the contract).

into account detailed changes required by each federal agency may have the effect of reducing the cost savings and flexibility the government is trying to achieve in its cloud first strategy. In particular, the efforts placed on making the FedRAMP strategy flexible and reusable will be diluted if each agency requires significant changes after the CSP meets the initial FedRAMP hurdle. Stated differently, agency individualization runs the risk of moving the program from a "do once, use many times" to simply a "do many times" authorization and contracting process.

This is not to say that one contract must be developed and applied to all transactions. Any standardization must recognize that agency missions differ. Some agencies deal with extremely sensitive data while others do not. In some cases, although it may be confidential, the data the agency stores is not PII. Therefore, a more clearly defined baseline, or catalog of several agreements based on sensitivity or presence PII could go a long way in reducing the customization needed by each agency. Raising the floor and providing specific minimum terms—even if within a range—for all CSPs taking part in FedRAMP is a starting point. Providing core terms that are more specific than the CIO's best practices guide, but that remain focused on principles, has the potential to reduce agency oversights as seen in many of the contracts evaluated in the CIGIE audit. After all, the data being placed on the cloud by governments is extremely valuable and the risk of loss has great monetary and privacy implications. But the risks are variable among agencies, and the terms of standard contracts should reflect this.

V. CONCLUSION

Accounting for all aspects of the cloud lifecycle contractually requires careful planning. As early as the pre-contractual phase, federal agencies must consider the eventual dissolution or termination of the cloud computing service they are using. Whether the termination is a result of contract expiration, bankruptcy of a CSP, or even non-performance or breach of contract, the agreement must provide the terms necessary to make a smooth transition of government data back in-house or to another CSP. Vague or missing terms of cloud computing agreements might make a smooth transition, or any transition, difficult. Not only is attempting to address overlooked contractual and security issues retroactively difficult and less effective, it also brings extra risk and expense.

In the audits of federal agencies, the central question evaluated was whether the contracts agencies entered into contained adequate controls to meet agency needs in the areas of data privacy, data security, and access while at the same time protecting federal investment. The answer for most agencies was a clear "no." The audits showed that the vast majority of agencies using cloud computing lacked necessary contractual mechanisms for monitoring agreements and assessing the delivery of the service. The range of missing terms, and the laws that certain terms conflicted with, was surprising in the audit. From the failure to define services as cloud computing to incomplete inventories of services; the organizational and general communication of the "cloud first" strategy was problematic. This begs the question, what improvements or changes ought to be made in order to increase compliance?

As a starting point, providing more concrete advice to agencies, including standardized contract terms, has the potential to greatly increase agency compliance and reduce the patchwork of implementation seen in the initial adoption. Providing individual agencies with less discretion might also prove an effective tool for negotiation and obtaining more compliant contract terms from CSPs. If agencies are able to offer their terms to CSPs on a take-it-or-leave-it basis, they have a much greater opportunity to influence the market. The current agency reliance on "best practices guides" or other sets of general principles—instead of mandatory or prepared clauses—appears to have resulted in uneven compliance. By clearly defining roles and responsibilities in the contracts, and giving agencies less discretion over the terms they will waive or the variances from FedRAMP they will accept, the program will likely achieve more consistent compliance results.

Whether the 800-pound gorilla is able to tame the cloud remains to be seen. Although the initial round of cloud computing adoption was bumpy, there is room for optimism. Many of the contracts initially adopted by federal agencies were for relatively short terms, giving agencies the ability to renegotiate their agreements and obtain more compliant services. By focusing contract terms on the roles of the parties, where they are established, the chain of custody over federal data is much clearer. In this regard, the revised terms by the DoD and the Postal Service might provide a way forward for other agencies. Unlike the best practice guide, DoD terms focused specifically on the people, security methods, and location of CSP servers used by agencies. As agencies become more accustomed to contracting for cloud

computing, and have better tools to obtain compliant contracts and clearer FedRAMP requirements, the oversights noted in the initial adoption are less likely. If such oversights continue, resulting in data breaches or other damages, leveraging the civil and criminal penalties describe above should be used as a further incentive to obtain compliance.

Finally, new technologies are often shiny and enticing, but nonetheless merit careful examination. When it comes to governments adopting cloud, the concern is beyond the typical dichotomies that are often expressed when deploying a new technology or service model. That is, although the typical states *versus* private enterprise or technology *versus* law contentions are present in cloud, they are not the center of the dangers facing citizens when their governments adopt cloud. Rather, in public cloud procurement, states and CSPs are acting much more in concert, even as partners, in the move for cloud computing adoption. This is a source of concern for citizens as the choices governments make in adopting cloud impact privacy and security. Governments need to stay objective in their approach to cloud and not stand too closely to CSPs on one side of the "*v*," leaving citizens and their right to privacy, along with government accountability, on the other. Governments have a strong hand to play when negotiating with CSPs. However, without a critical eye, in addition to adequate systems for procurement, states will fail to obtain contract terms—and ultimately cloud computing services—that meet their needs and those of the citizens they represent.