PROTECTING "CROWN JEWEL" TRADE SECRETS IN THE CLOUD THROUGH VOLUNTARY INDUSTRY-GOVERNMENT COLLABORATIONS AND FEDERAL LEGISLATION

Alexis Salerno[1]

ABSTRACT

This Comment advances a novel and comprehensive path to federal regulation of cloud computing in the U.S., designed to protect the interests of small and mid-size enterprises (SMEs) and business clients generally. Slated to grow from an industry valued in the tens of billions to one valued in the hundreds of billions of dollars in the next few years, U.S. public cloud computing requires greater safeguards and oversight initiated by providers and the government. Due to the unequal bargaining power wielded by cloud services providers relative to their SME clients, there is little room for such clients to negotiate contracts that provide adequate protections for their trade secrets. And, thus a critical threat to trade secrets remains unaddressed by current federal law and cloud computing policy in the U.S.—the use of subcontractors by cloud service providers. Subcontractors pose a significant and often insidious risk to SME clients because cloud service providers are under no obligation to indicate their use of subcontractors nor are they under an obligation to guarantee that the subcontractors will protect their clients' data to the same extent the providers, themselves, protect their clients' information.

Since the U.S. lacks unified data privacy law related to cloud computing and most cloud computing oversight focuses on data encryption, SMEs are left to rely on trade secret law, state or federal, and contract law to bring actions against cloud service providers for breach of trade secret protections. Such suits are both costly and likely to fail because the clients did not adequately protect their trade secrets. The EU's new General Data Protection Regulation (GDPR) recognizes subcontracting risks in cloud

1. JD 2018, University of Pennsylvania Law School. Email: asalerno@*pennlaw.upenn.edu.* The author wishes to thank Professor Polk Wagner for his advisement and mentorship on this Comment.

computing by requiring cloud service agreements to indicate when subcontractors are used and holds cloud services providers liable when they fail to impose the same data protection obligations on their subcontractors as agreed upon between the client and cloud service provider. More broadly, the GDPR provides a generous definition of personal data that protects most, though not all trade secrets, and imposes steep pecuniary penalties on violators of such regulation.

As the EU and other Asian countries develop cloud computing laws that protect their citizens' data, the U.S. should recognize the economic imperative of devising its own safeguards for its citizens' data, namely trade secrets. As a starting point, the National Institute of Standards and Technology (NIST), the U.S.'s central cloud computing authority, should adopt the GDPR's definition of personal data along with the DTSA's definition of trade secrets in its best practices guidance. Beyond raising awareness about best practices in cloud computing, NIST should collaborate with the Cloud Service Alliance (CSA) to create a single, certification scheme to evaluate and monitor cloud service providers' subcontracting, trade secret, personal data, and security practices. Such a program would provide SMEs with a low-cost method to compare offerings. Additionally, a "red flag" warning system posted on the certification scheme's website for each participant, where a provider's data breaches would be detailed, would increase transparency in the industry and incentivize providers to maximize protection for clients' data.

To boost development of domestic cloud service providers, the U.S. should offer subsidies to providers willing to both conduct their operations and domicile in the U.S. Critically, a voluntary Cloud Code of Conduct, created by industry leaders, small business associations, and academics, should serve as a means of self-regulation in the industry. Cloud service providers would pledge to adhere to policies such as disclosing use of subcontractors and assuming liability for subcontractors' failure to protect client data to the level agreed to between the cloud service provider and client. Given the prevalence of harsh regulation in cloud computing overseas, namely the GDPR in the EU, industry providers will likely be incentivized to voluntarily join the Cloud Code of Conduct to shape the framework for future cloud computing law. Though lawmakers could impose regulations on cloud computing providers without using a voluntary code of conduct as a basis for the law, the disadvantages are significant. Primarily, using the Cloud Code of Conduct as a foundation for federal policy would enable the government to develop nuanced standards based on the voluntary Code's performance in the marketplace. Finally, the Cloud Code of Conduct could transition to an advisory role as a think-tank for new

policy ideas and industry education initiatives, ensuring the timeliness of the proposed remedies.

INTRODUCTION

Public Cloud Computing is a growing market worldwide that is expected to increase from $59 billion in 2014 to $205 billion in 2020.[2] Services include public cloud- SaaS, public cloud- PaaS, and public cloud- IaaS.[3] Cloud-enabled SaaS resources such as Enterprise Resource Planning (ERP) allow businesses to manage central tasks such as inventory tracking and payment processing along with data analytic capabilities such as financial forecasting.[4] Leading vendors for midmarket and small to medium size enterprises include Oracle, NetSuite, Workday, SAP S/4HANA Cloud, Microsoft, Acumatica, and FinancialForce.[5] Midmarket and Small and Medium-Sized businesses surveyed in a 2016 IDC survey indicated 8.9% of Small Businesses use ERP cloud services and 25.2% of Medium-Sized Businesses use ERP cloud services.[6]

In the U.S. alone, public IT cloud services revenue is expected to grow from $38 billion in 2014 to $124 billion in 2020, consisting of public cloud- SaaS, public cloud- PaaS, and public cloud- IaaS.[7] Lack of transparency and trust are sighted as major barriers to cloud adoption by businesses, particularly small and medium-size enterprises (SMEs).[8] Most policy and regulation related to cloud computing in the United States targets data encryption standards, with the intent of increasing safety and confidence in the industry.[9]

However, a significant issue for small and medium-size enterprises remains unaddressed.[10] Namely, the concern that cloud service providers'

---

2. *See* Frank Gens, WORLDWIDE AND REGIONAL PUBLIC IT CLOUD SERVICES FORECAST, 2016-2020, Table 1 (IDC, Doc. US40739016, 2016) (on file with author) (referencing Table 1 sourced from IDC Worldwide Semiannual Public Cloud Services Tracker, 1H16 forecast release, November 2016).

3. *Id.*

4. *Enterprise Resource Planning (ERP) Security Working Group*, CLOUD SECURITY ALLIANCE, (Mar. 7, 2018, 6:53 PM), https://cloudsecurityalliance.org/group/enterprise-resource-planning/#_overview [https://perma.cc/5HNP-ZHGD].

5. Mickey North Rizza & Eric Newmark, *IDC MarketScape IDC MarketScape: Worldwide SaaS and Cloud-Enabled Midmarket ERP Applications 2017 Vendor Assessment*, 1 (2017).

6. *Id.* at 4 (referencing Table 1).

7. *See* Gens, *supra* note 2, at Table 9 (citing IDC Worldwide Semiannual Public Cloud Services Tracker, 1H16 forecast release, November 2016).

8. Portfolio 515: Privacy and Security Issues in Cloud Computing, C. Privacy Risks in the Cloud, BNA 3 (2017).

9. Bob Gourley, Jane Melia, *FedRAMP Does Not Guarantee Data Security*, AFCEA THE CYBER EDGE, (Mar. 7, 2018 6:49 PM), https://www.afcea.org/content/fedramp-does-not-guarantee-data-security [https://perma.cc/JH5H-A474].

10. Janet A Stiven, *Technology Transactions: A Practical Guide to Drafting and*

use of subcontractors jeopardizes SMEs' trade secrets.[11] As the law exists in the U.S., there is no legal requirement for cloud service providers to disclose their use of subcontractors in their agreements with clients.[12] Since no privity exists between the client and the subcontracting party or parties hired by the provider, the client's legal recourse against the subcontractor is severely limited.[13] A client must rely on his agreement with the cloud service provider to protect his trade secrets, and personal data more broadly, even when a provider shares the client's data with subcontractors.[14] For SME clients, their cloud service providers typically wield more bargaining leverage, leading SMEs to accept unfavorable service agreements without adjusting the terms.[15] Therefore, trust in the cloud computing space is not high amongst small and mid-size enterprises and business clients overall in the U.S.[16]

Currently, most firms decide not to store their indispensable trade secrets, i.e. "crown jewels," in the cloud.[17] Instead, they typically store less vital components of their trade secrets in the cloud.[18] This Comment seeks to provide a series of feasible solutions, targeting subcontracting, to improve trade secret protections in cloud computing sufficiently for SMEs to place a significant portion of their important trade secrets, if not all of their "crown jewels," in the cloud. This Comment will first discuss how traditional means of trade secret protection, both contract and trade secret law, fail to adequately protect clients' trade secrets when data is shared between providers and subcontractors.

Next, ways the U.S. can protect businesses' trade secrets in the cloud by looking to the European Union's General Data Protection Regulation (GDPR) for guidance and relying on NIST to establish and disseminate trade secret protection guidelines for cloud computing will follow. The EU Commission's GDPR recognizes the damaging effects subcontracting can have on a small to mid-size enterprises if left unregulated and imposes obligations and liability on cloud service providers who use subcontractors.[19]

Negotiating Commercial Agreements, Cloud Computing Agreements, in PRAC. L. INST. 4-13 (Mark G. Malven ed., 2015).

11. *Id.* at 8.

12. Portfolio 515, *supra* note 8, at 3.

13. *Id.* at 3.

14. *Id.*

15. *See* Stiven, *supra* note 10.

16. *Id.*

17. Eric Savitz, *Is It Safe To Store Your Trade Secrets In The Cloud?*, FORBES (Apr. 6, 2018, 2:30pm), https://www.forbes.com/sites/ciocentral/2012/02/22/is-it-safe-to-store-your-trade-secrets-in-the-cloud/#5dc64fd24cb3 [https://perma.cc/M4PM-9JD9].

18. *Id.*

19. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and

The question arises, whether cloud service providers and market participants can be incentivized to voluntarily adopt NIST best practices, including those targeting trade secrets, without imposing federal regulation on cloud computing. An explanation of the trade protective measures NIST should recommend for trade secrets will follow. Then, a discussion of ways to motivate industry-wide compliance with NIST's solutions and other cloud computing reform will be provided, comprising of voluntary government-industry initiatives, mandatory regulation of cloud computing, or a combination of both.

I. EXISTING LEGAL PROTECTIONS FOR TRADE SECRETS IN THE U.S.

A. Contract Law

Regardless of the type of agreement, clickwrap or standard contract, there are no regulations or standards for disclosures related to a cloud service provider's use of subcontractors.[20] Consequently, contract terms generally fail to specify use of subcontractors and include disclaimers of responsibility for actions taken by third party services.[21] The general trend for cloud service providers not to disclose their use of subcontractors in service agreements exposes a client's trade secrets to tremendous risk.[22] This lack of transparency prohibits the client from adequately assessing the full scope of service it is consenting to use.[23] As a result, clients are left with the option to either assume this sizable risk or opt not to utilize cloud computing services and instead develop in-house programs.[24]

Aside from disclaimers, which clearly abscond the cloud service provider of responsibility, weak contractual commitments reduce the cloud service provider's risk of liability.[25] This in turn, serves as a disincentive for providers to negotiate adequate protections for a client's data in the

---

on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), 2016, O.J. (L 119) [hereinafter referred to as "Regulation (EU) 2016/679 General Data Protection Regulation"].

20. BSA THE SOFTWARE ALLIANCE, 2016 BSA GLOBAL CLOUD COMPUTING SCORECARD (2016) 6; Stiven, *supra* note 10, at 8; Portfolio 515, *supra* note 8, at 3.

21. Stiven, *supra* note 10.

22. *Id.*; Portfolio 515, *supra* note 8, at 3.

23. *Id.*

24. *See* Rizza and Newmark, *supra* note 5, at 4 (referencing on-premises as being akin to in-house).

25. Stiven *supra* note 10, at 4-18.

provider's separate agreement with a subcontractor.[26] In both scenarios, a client, especially a SME, has unequal bargaining power with a large cloud service provider to argue for improved safeguards for its data.[27] In some cases, unequal bargaining power may serve as a valid claim, but litigation is costly for a SME and is not a likely avenue to be pursued unless necessary.[28] Additionally, the client will likely have a hard time succeeding when the industry practices are slanted in favor of the provider—no requirement to disclose subcontracting parties and disclaimers.[29]

B. Trade Secret Law

Claimants may bring trade secret claims under the Uniform Trade Secrets Act (UTSA), which applies in 47 states and the District of Columbia,[30] or the Defend Trade Secrets Act (DTSA), which permits civil trade secret to be heard in federal court (does not preempt state trade secret law).[31] A trade secret according to USTA is:

> [I]nformation, including a formula, pattern, compilation, program, device, method, technique, or process that: Derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use; and is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.[32]

The three elements of a trade secret claim are: (1) the subject matter must be eligible for trade secret protection, (2) the holder of the subject matter must demonstrate that reasonable precautions were taken to prevent its disclosure, and (3) the trade secret holder must prove the information was taken wrongfully or misappropriated.[33] Generally, use of another's trade secret is not considered misappropriation and therefore illegal unless it is (a)

---

26. *Id.*
27. *Id.*
28. Portfolio 515, *supra* note 8, at 3.
29. *Id.*
30. *Trade Secret*, LII (Mar. 7, 2018, 8:29 AM), https://www.law.cornell.edu/wex/trade_secret [https://perma.cc/98A6-55GN].
31. Mark. L. Krotoski, *The Landmark Defend Trade Secrets Act of 2016*, MORGAN LEWIS 1, 8 (2016), https://www.morganlewis.com/-/media/files/publication/morgan-lewis-title/white-paper/the-landmark-defend-trade-secrets-act-of-2016-may2016.ashx [https://perma.cc/MV9D-46GK].
32. *See Trade Secret*, *supra* note 30 (summarizing USTA's definition of a trade secret).
33. *See id.* (paraphrasing the elements of a trade secret claim generally).

obtained through improper means or (b) entails a breach of confidence.[34]

In the case of a cloud service agreement between a business client and cloud service provider, trade secrets obtained by a subcontractor may be considered an inadvertent disclosure due to the trade secret holder's failure to reasonably protect the subject matter.[35] Clients are likely disadvantaged because standard cloud service agreements in the U.S. do not disclose subcontractor use and small and mid-size enterprises rarely have the resources to seek disclosure from large cloud service providers.[36] Yet, the subcontractor can argue it obtained and used the client's trade secrets legally because the client failed to establish sufficient protections in its contract with the cloud service provider.[37] In the rare case where the client succeeds in its trade secret claim against a subcontractor, remedies such as injunction and damages[38] fail to address the root issue—SME's confidence in cloud computing and trust in cloud service providers' reliability as business partners.

II. U.S. DATA PRIVACY LAW RELATED TO CLOUD COMPUTING DOES NOT ADDRESS SUBCONTRACTING

Beyond claims for breach of contract and trade secret violations, cloud clients have little to no recourse under data privacy law for trade secret disclosures caused by a cloud service provider's use of a subcontractor.[39] Generally, no unified privacy law exists in the U.S., instead, there are specific sectoral laws in areas such as health care and finance.[40] As of yet, there are no "laws or enforceable codes containing general security requirements for digital data hosting and cloud service providers" according to a BSA evaluation. [41] Instead, highly specified regulations exist, such as requirements in California to encrypt databases containing personal information.[42]

Where regulation does exist, it is primarily focused on encryption

34. *Id.*

35. *See id.* (indicating trade secrets may be obtained legally through independent discovery and reverse engineering additionally).

36. Portfolio 515, *supra* note 8, at 3.

37. Stiven, *supra* note 10, at 4-14.

38. Portfolio 43:-3rd: Trade Secrets: Protection and Remedies, Remedies for Unauthorized Use and/or Disclosure, B. Civil Actions, BNA 3 (2017).

39. *See* BSA, *supra* note 20, at 1-2 (discussing privacy policy in question 1 and cloud service provider specific law in question 3).

40. *See id.* at 1 (referencing questions 1 and 2).

41. *Id.* at 2.

42. *Id.*

safeguards,[43] such as FedRAMP, which is the government's cloud assessment, authorization and monitoring system for services used by federal agencies.[44] Enforcement actions by the FTC typically focus on encryption breaches or failure to design standard data protection measures.[45] The FTC under Section 5 of the FTC Act has the authority to investigate companies that fail to provide reasonable protections for consumers' personal information,[46] and the FTC can conduct special reports such as wide range economic studies.[47]

Additionally, the National Information Assurance Partnership (NIAP), which is managed by NSA, provides certification for technology products and is primarily focused on security issues.[48] Its evaluation process involves detailed protection profiles but does not include cloud service providers on its list.[49] The National Institute of Standards and Technology (NIST), a non-regulatory U.S. agency, develops standards for cloud computing and the digital economy in the United States.[50] Its standards are accredited by the American National Standards Institute (ANSI), a nonprofit organization.[51] In its seminal guides on cloud computing including *NIST's Roadmap 2013*[52] and *Framework for Improving Critical Infrastructure Cybersecurity (Framework)*, NIST does not have a broad definition of personal data that encompasses a sufficient range of trade secrets.[53] Specifically, NIST limits

43. Stiven, *supra* note 10, at 4-24.

44. *About Us*, FEDRAMP (Mar. 7, 2018 9:05 AM), https://www.fedramp.gov/about/.

45. *Start with Security: A Guide for Business*, FED. TRADE COMMISSION (Mar. 7 2018, 9:09 AM), https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business [https://perma.cc/5MFN-XQGF].

46. *A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority*, FED. TRADE COMMISSION (Mar. 7 2018, 9:10 AM), https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority [https://perma.cc/4RMD-SX4S].

47. *Id.*

48. *See What is NIAP/CCEVS?*, NIAP (Mar. 7 2018, 9:14 AM), https://www.niap-ccevs.org/Ref/What_is_NIAP.CCEVS.cfm (indicating the program includes the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) validation body).

49. *Approved Protection Profiles,* NIAP (Mar. 7 2018, 9:16 AM), https://www.niap-ccevs.org/Profile/PP.cfm [https://perma.cc/RN2M-CF3M]; *Protection Profile Development,* NIAP (Mar. 7 2018, 9:17 AM), https://www.niap-ccevs.org/Profile/InDraft.cfm [https://perma.cc/3AUB-SD5T].

50. *NIST Cloud Computing Program,* NIST (Mar. 7 2018, 9:19 AM), https://www.nist.gov/programs-projects/nist-cloud-computing-program-nccp [https://perma.cc/HVZ8-SRWR]; BSA, *supra* note 20, at 5.

51. BSA, *supra* note 20, at 5.

52. *NIST Cloud Computing Standards Roadmap Special Publication 500-291, Version 2*, NATL. INST. STAND. TECHNOL. (2013) 21, https://www.nist.gov/sites/default/files/documents/itl/cloud/NIST_SP-500-291_Version-2_2013_June18_FINAL.pdf [https://perma.cc/V7EQ-ZLYA].

53. NIST, *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1*,

its definition to personally identifiable information (PII), which is the following:

> [t]he information that can be used to distinguish or trace an individual's identity, such as name, social security number, biometric records, etc., alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.[54]

Therefore, a contact list with phone numbers would be protected but not data on a company's sales volume or distribution network.[55]

III. EUROPEAN UNION'S RESPONSE TO SUBCONTRACTING BY CLOUD SERVICE PROVIDERS

Under the European Union's new data privacy law, GDPR, effective on May 25, 2018, trade secrets are better protected by a broad definition of personal data,[56] encompassing any identifier including an identification number, location data, an online identifier (IP addresses, cookies, and RFID tags).[57] The definition essentially serves as a catchall for "all means reasonably likely to be used" to identify a natural person, and liability imposed on cloud service providers who use subcontractors.[58] Though broad in scope, it is important to note the GDPR's definition of personal data does not capture all trade secrets. This section will explain how the EU's GDPR addresses the major issues posed by cloud service providers' use of subcontractors. Primarily, the GDPR mandates contractual protections when cloud service providers utilize subcontractors, encourages third-parties to create cloud codes of conduct to enable providers to demonstrate adherence to the law, and promotes the adoption of certification schemes (either third-party or yet to be devised government initiatives) to assess service providers' policies and practices.[59]

NAT'L. INST. STANDARDS TECH. (April 16, 2018) 17, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf [https://perma.cc/QL5T-VBJN].

54. NIST, *supra* note 52, at 21.

55. *Id.* at 21.

56. Regulation (EU) 2016/679 General Data Protection Regulation, art. 28, 2016, O.J. (L 119).

57. *Id.* at recital 30.

58. *Id.* at recital 26.

59. *Id.* at art. 28, art. 40-43.

A. GDPR's Subcontracting Standards

The GDPR extends liability to service providers and includes rules aimed at increasing transparency and responsibility in subcontracting.[60] Specifically, a cloud service provider (processor) must receive consent from a customer (controller) to use subcontractors in its service agreement.[61] As stated in Article 28 (2), "The processor shall not engage another processor without prior specific or general written authorization of the controller."[62] Furthermore, if the cloud service provider changes its subcontractors it must notify the client. Stated in Article 28, "[. . .] the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes."[63]

Next, when a cloud service provider uses another processor (subcontractor) to perform specific processing activities for the controller (client), the CSP must pass on the "same data protection obligations as set out in the contract" between the controller and CSP processors.[64] Therefore, the CSP, processor, is liable to the client if the subcontractor fails to satisfy its obligations. The burden of carrying the "same" terms from the underlying agreement through to the one between the CSP and subcontracting party, has challenging practical implications.[65] Practitioner Webber points out that these terms may be impossible for large CSP processors to satisfy because they make different agreements with clients and then work with numerous subcontractors, including influential firms such as Amazon and Microsoft, for backend hosting services.[66] Consequently, the CSP processor will most likely "absorb" some of this contractual risk.[67] Webber further postulates such subcontracting requirement will "likely plague many legal teams,"[68] which evidence suggests is true from draft contractual language provided by

60. *Id.* at art. 28; *EU General Data Protection Regulation – Background*, DLA PIPER (Mar. 9 2018 10:21 AM) https://www.dlapiper.com/en/uk/focus/eu-data-protection-regulation/background/ [https://perma.cc/9UWT-4QW9].

61. Regulation (EU) 2016/679 General Data Protection Regulation, art. 28(2), 2016, O.J. (L 119).

62. *Id.* at art. 28(2).

63. *Id.*

64. *Id.* at art. 28(4); Mark Webber, *The GDPR's impact on the cloud service provider as a processor*, 16 J. PRIV. DATA PROT. 4 (2016) at 3, http://www.fieldfisher.com/media/3993765/the-gdprs-impact-on-the-cloud-service-provider-as-a-processor-mark-webber-privacy-data-protection.pdf [https://perma.cc/VQ8U-EVCS].

65. *Id.* at 3.

66. *Id.*

67. *Id.*

68. *Id.*

legal advisory firms such as DLA Piper.[69]

The GDPR's reach extends to personal data of EU citizens that is handled within the EU as well as transferred to third countries.[70] Specific requirements must be met for international data transfers to be permissible, including (a) previous vetting and approval by the Directive (prior law), (b) EU/US Privacy Shield, (c) binding corporate rules, and (d) one of two new measures: codes of conduct and certification.[71] Liability imposed by the GDPR is harsh, and in the case of transfer violations, the highest category of fines applies[72]—up to 20 million Euros or in the case of undertakings up to 4% of annual worldwide turnover.[73] This translates into increased responsibility for cloud service providers to protect personal data for EU citizens but does not incentivize increased protection for personal data of U.S. citizens.

More broadly, the sanctions imposed by the GDPR are amongst the highest, on a close footing with anti-bribery and anti-trust laws, for non-compliance.[74] Sanctions consist of two categories: (1) fines up to 20 million Euros or in the case of undertakings up to 4% of annual worldwide turnover[75] for breach of "the basic principles of processing," "data subjects' rights," "international transfer restrictions," "obligations imposed by Member State law for special cases," "certain orders of a supervisory authority," and (2) fines up to 10 million Euros or in the case of undertakings up to 2% of annual

69. *Example Data Protection Addendum Addressing Article 28 GDPR (Processor Terms) and Incorporating Standard Contractual Clauses for Controller to Processor Transfers of Personal Data from the EEA to a Third Country,* Version Date: 14 July 2017, DLA PIPER, CLIFFORD CHANCE, INTERNATIONAL REGULATORY STRATEGY GROUP, (Mar. 7 2018, 10:36 AM) https://www.DLAPIPER.com (Available for download in document form).

70. Regulation (EU) 2016/679 General Data Protection Regulation, art. 30, 2016, O.J. (L 119).

71. Caroline Krass, Jason N. Keinwaks, et al., *The General Data Protection Regulation: A Primer for U.S.-Bases Organizations That Handle EU Personal Data*, PROGRAM ON CORP. COMPLIANCE AND ENFORCEMENT AT NEW YORK UNIVERSITY SCHOOL OF LAW (Mar. 7, 2018) https://wp.nyu.edu/compliance_enforcement/2017/12/11/the-general-data-protection-regulation-a-primer-for-u-s-based-organizations-that-handle-eu-personal-data/ [https://perma.cc/R4DB-PNGV].

72. *EU General Data Protection Regulation – Key Changes,* DLA PIPER (Mar. 9 2018 10:48 AM) https://www.dlapiper.com/en/uk/focus/eu-data-protection-regulation/key-changes/ [https://perma.cc/L28B-7JRW].

73. *See Id.* (discussing GDPR fines); Regulation (EU) 2016/679 General Data Protection Regulation, art. 83(5), 2016, O.J. (L 119).

74. *Id.*; Regulation (EU) 2016/679 General Data Protection Regulation, art. 83(4)-(5), 2016, O.J. (L 119).

75. *EU General Data Protection Regulation – Key Changes*, DLA PIPER (Mar. 9 2018 10:48 AM) https://www.dlapiper.com/en/uk/focus/eu-data-protection-regulation/key-changes/ [https://perma.cc/9PG2-J5XX].

worldwide turnover for breach of "obligations of controllers and processors," "obligations of certification bodies," "obligations of monitoring bodies."[76] Furthermore, GDPR, per Article 58, grants supervisory authorities extensive investigative and corrective powers such as the authority to conduct on-site data protection audits and orders to perform specified remediation activities.[77] Finally, the GDPR significantly lowers the barrier for private claims against data controllers and processors—persons who have suffered "material or non-material damage" due to a breach of the GDPR have the right to seek compensation from the controller or processor.[78] To reiterate, the penalties imposed by GDPR are steep and incentivize cloud service providers and handlers generally to protect EU personal data, but do not address safeguarding U.S. personal data.

B. Cloud Code of Conduct

This section will analyze a measure created to support the GDPR's mission to protect EU personal data—Codes of Conduct with a specific eye towards subcontracting issues. Strengths and weaknesses of such codes will be discussed to show the potential actions industry and government in the U.S. could take to address subcontracting problems for U.S. personal data. The goal is to provide cloud service customers, namely SMEs, with an understanding of how members (cloud service providers) are protecting their customers' personal data. The GDPR, Articles 40 and 41, allow "associations and other bodies representing categories of controllers or processors"[79] to create codes of conduct monitored by independent bodies. A company's adherence to the code enables the firm to demonstrate compliance with many of the GDPR's requirements such as security and general processing obligations[80] and may demonstrate adequate safeguards for data transfers to third countries if commitments are binding and enforceable in the third country.[81] The Data Protection Board will gather approved codes of conduct in a register, available to the public.[82]

---

76. *Id.*

77. Regulation (EU) 2016/679 General Data Protection Regulation, art. 58(2), 2016, O.J. (L 119).

78. *Id.* at art. 82(1).

79. *Id.* at art. 40-41.

80. Webber *supra* note 64, at 3.

81. Krass, *supra* note 71.

82. Regulation (EU) 2016/679 General Data Protection Regulation, art. 40(11), 2016, O.J. (L 119).

C. *Example Cloud Code of Conduct: The European Cloud Code of Conduct (drafted with the guidance of the European Commission)*

This European Cloud Code of Conduct (EU Cloud CoC) is worth discussing because it contains language pledging protection for transfers of customers' personal data to third-party subcontractors.[83] It is significant to note the Code was designed to address the key "transparency" and "trust" issues "Small and Medium Enterprises (SMEs)" face when selecting a cloud service provider, and subcontracting is counted as one such problem.[84] Essentially, the Code is a voluntary device that allows a cloud service provider to evaluate and convey its adherence to the Code's requirements through self-assessment and self-declaration of compliance or third-party certification.[85] The Code's website provides a list of cloud providers that adhere to the Code, allowing cloud customers to verify their potential provider is in fact registered.[86] It is important to note, the Service Agreement between the cloud service provider and customer "determine[s] the terms under which the Cloud Service is delivered" and does not "replace a contract between the CSP and the Customer."[87] Beyond added transparency, the Code posits to provide an added safety net for cloud customers because cloud service providers must maintain a level of data protection aligned with the Code's standards at all times, not merely at signing.[88]

The Code's approval is less definite than suggested by the EU Cloud CoC's website but stands a high probability of approval because the Code, without its current name, underwent periodic reviews by and received drafting advice from the European Commission's working group on cloud-specific issues.[89] Founding members of the General Assembly include Alibaba Cloud, Fabasoft, IBM, Oracle, Salesforce, and SAP.[90] The EU Cloud Code of Conduct is managed and administered by an independent body, SCOPE EUROPE,[91] a think-tank supporting co-regulation measures

83. EU Cloud CoC, European Cloud Code of Conduct v 2.0, (May 2018), https://eucoc.cloud/en/contact/request-the-eu-cloud-code-of-conduct.html [https://perma.cc/K9S3-LUVW] [Referred to as the Code and EU Cloud CoC within the text of this article].

84. *See id.* at 3-4 (indicating the Code is designed primarily for business-to-business (B2B) cloud services).

85. *See id.* at 4 (allowing a cloud service provider to pledge one or all of its services to the Code).

86. *Id.*

87. *Id.* at 9.

88. *Id.*

89. *Id.* at 3-4.

90. *Id.* at 24.

91. SCOPE EUROPE, https://scope-europe.eu/en/our-scope/about-us.html [https://perm

in the digital economy. The Code is centered around independent Governance Bodies comprising of a General Assembly as a consultative body, Steering Board as an operational decision maker, Secretariat as administrative support, and Monitoring Bodies as monitor and enforcer of the code.[92] The Code outlines the approval process in broad terms, which includes a Declaration of Adherence and a self-assessment or certification performed by an external auditor.[93]

D. Subcontracting Specific Content

The EU Cloud CoC contains a section addressing subcontracting, the content echoes the policies conveyed in the GDPR without offering significant, new content, such as requirements that cloud service providers demonstrate effective monitoring of data protection practices and client data handling by their subcontractor(s).[94] For example, the Code permits a cloud service provider to delegate all or some of its processing activities delineated in the Service Agreement to third-party subcontractors with the customer's prior consent, which may be in the form of general consent at the onset of the Service Agreement (as stipulated in the GDPR).[95] No new or additional consent from a customer is required when a subcontractor is changed or added, but the customer must be informed of the change in subcontractors.[96] Though the Code holds the cloud service provider liable to the client for a subcontractor's failure to meet its data protection commitments, these standards are pulled directly from the GDPR.[97] In its current iteration, the Code does not provide cloud service providers with novel monitoring and diagnostic protocols to detect potential abuse of client data by their subcontractors.[98]

---

a.cc/MM3W-CFEP] (last visited Mar. 7, 2018 3:28 PM). This is a subsidiary of the German non-profit SRIW e.V. (Selbstregulierung Informationswirtschaft – Self Regulation Information Economy).

92. EU Cloud COC, *supra* note 83, at 23.
93. *Id.* at 7-8.
94. *Id.* at 10-11.
95. *Id.* at 10.
96. *Id.* at 10-11.
97. *Id.*
98. *Id.*

E. Evaluation of the EU Code of Conduct

Delving into the EU Cloud CoC's monitoring and enforcement policies reveals policies favoring cloud service providers.[99] This calls into the question the value of having industry practitioners spearhead a Code initiative that does not require the involvement of independent privacy experts and client advocates such as trade associations or guilds.[100] According to the Code, monitoring will be performed by a Competent Monitoring Body.[101] The first line of recourse for a customer concerned about a cloud service provider's compliance with the Code is to contact the cloud service provider, which places an unsophisticated SME client in an unequal bargaining position.[102] If the cloud service provider and client fail to reach a resolution, then the client may submit a complaint to the Monitoring Body, which will conduct fact-finding for a Complaints Panel. Such a Complaints Panel will be appointed by the Monitoring Body and will follow guidelines designated by the Steering Board.[103] Neither the rights of the client during the complaints process are described in the Code nor is it indicated that such content and additional resources will be provided to clients online.[104] Overall, the Code focuses on the perks of joining the Code and deemphasizes the responsibilities of member cloud service providers, suggesting the Code's creators primarily aim to attract additional industry leaders to the program at this stage.[105]

F. Certification

The GDPR also calls for voluntary certification schemes, which typically entails an audit of the cloud service provider's practices based on a detailed set of metrics and is conducted by a properly approved and trained third party.[106] Such a process is similar to a financial auditing process and is meant to provide cloud clients with additional confidence in cloud service

99. *Id.* at 33-34.

100. *Id.* at 26. Members on the Steering Board may elect to appoint an independent expert and/or trade organization representative as her representative on the Board.

101. *Id.* at 34.

102. *Id.* at 33-34.

103. *Id.* at 33.

104. *Id.*

105. *Id.*

106. *See* Marnix Dekker, Christoffer Karsberg et al., *Auditing Security Measures*, ENISA 34 (2013), https://www.enisa.europa.eu/publications/schemes-for-auditing-security-measures [https://perma.cc/DS8P-4E9E] (stating that some third-party auditors are governmental, and others are not).

providers' practices and policies as implemented.[107] The GDPR leaves the precise procedure for certification unclear, allows self-attestations, and instead states that certification may be granted by a certification body or competent supervisory authority based on criteria approved by either the competent supervisory authority or the Board.[108]

A general certification process, according to a 2013 study conducted by ENISA, involves the following:[109] (a) *implementation* of security requirements performed by the provider; (b) *audits* conducted by the auditor to see if the service or provider meets the security requirements; (c) *monitoring* conducted by a monitoring system that checks to see whether the requirements are met; (d) *certification* performed by the certification authority and certifies the service or provider, using audit reports and monitoring reports "from licensed auditors and validated monitoring tools"; (e) *licensing* of auditors by the certification authority, which may require auditors to pass exams evaluating their expertise or knowledge; (f) *validation* provided by the certification board for monitoring tools; (g) *accreditation* granted by the governing authority to the certification authorities that essentially asserts the soundness of the certification process.[110]

G. *Current Certification Related Actions Taken by the European Commission*

Actions currently taken by the European Commission to provide cloud customers with greater transparency and confidence in vendors include a collaboration between one of its subgroups, Certification Schemes from the Cloud Select Industry Group (C-SIG), and the European Union Network and Information Security Agency (ENISA).[111] Together they established the Cloud Certification Schemes List (CCSL).[112] The Cloud Certification Schemes List (CCSL) is meant to provide small to medium size enterprises, users with limited cloud expertise, with an overview of existing certification

107. *Id.* at 34.
108. *Id.*
109. *Id.*
110. *Id.*
111. *Cloud Computing Certification- CCSL and CCSM*, ENISA, (Mar. 7, 2018 4:13 PM), https://resilience.enisa.europa.eu/cloud-computing-certification [https://perma.cc/WVF8-AGDF].
112. *See id.* (stating on the website that, the Cloud Certification Schemes Metaframework (CCSM), "provide a neutral high-level mapping from the customer's Network and Information Security requirements to security objectives in existing cloud certification schemes . . . .").

schemes that could be "relevant for cloud computing customers."[113] CCSL identifies the "main characteristics" of the listed certification schemes including the underlying standards, certification issuing authority, auditing measures.[114] Underlying standards include questions about a cloud service provider's supply chain and whether it includes third-party agreements, compliance, and subcontracting arrangements.[115]

H. Evaluation of Certification Schemes

Regardless of whether a certification scheme is implemented by an independent party or the government, it provides a means to check the practices implemented by a cloud service provider. Self-assessments, as a standalone basis for certification, are a weak safeguard for cloud customers because the provider reports on its own performance and policies. Instead, self-assessment and an independent, third-party auditor provide greater assurances the cloud service provider is implementing personal data privacy measures. Furthermore, some legal practitioners' question whether receiving certification will provide the benefit of reduced regulatory scrutiny.[116] Such a benefit would strongly incentivize cloud service providers to enroll in a certification scheme. Arguably, the steep penalties imposed by a violation of the GDPR as well as the low bar for private actions, likely serve as sufficient motivation for cloud service providers to seek independent approval of their policies. From the cloud customers' perspective, an added layer of review provides additional assurance personal data will be protected adequately.

---

113. *Id.* Marnix Dekker, Dimitra Liveri, *Certification in the Eu Cloud strategy*, ENISA 6 (2014), https://resilience.enisa.europa.eu/cloud-computing-certification/certification-in-the-eu-cloud-strategy [https://perma.cc/AS2Y-ELKW].

114. *Id.*

115. *CSA Attestation – OCF Level 2,* ENISA, (Mar. 7, 2018 4:19 PM), https://resilience.enisa.europa.eu/cloud-computing-certification/list-of-cloud-certification-schemes/csa-attestation-ocf-level-2 [https://perma.cc/KM77-HRJV] (For example, the certifier CSA's profile has a tab labelled, "Part 5 Security Objectives: Supply Chain Management, Transparency and Accountability," which discusses third party assessments, audits and agreements. The schemes listed so far include: Certified Cloud Service-TUV Rheinland, CSA Attestation -OCF Level 2, CSA Certification -OCF Level 2, CSA Self Assessment – OCF Level 1, EuroCloud Self Assessment, EuroCloud Star Audit Certification, ISO/IEC 27001 Certification, Payment Card Industry Data Security Standard v3, Leet Security Rating Guide, Service Organization Control (SOC) 1, (SOC) 2, (SOC) 3, and Cloud Industry Forum Code of Practice.).

116. Webber, *supra* note 64, at 3.

IV. U.S. SOLUTION PROPOSALS

Using the EU initiatives discussed in the previous section as a framework, this section will propose potential actions the U.S. government and industry could take to provide greater safeguards for trade secrets when cloud service providers use subcontractors. Beginning with the recommendation that NIST expands its definition of personal data to mirror the one used in the GDPR, the conversation then moves to protective measures for trade secrets NIST should incorporate in its seminal publication, *Framework*. Next, a centralized certification scheme is advocated for as well as a Cloud Code of Conduct meant to serve as a self-regulating measure in the industry and subsequently a launching pad for regulation of cloud computing.

A. Establish Standard Definitions for Personal Data and Trade Secrets in Cloud Computing

As the standard setting authority for cloud computing in the U.S., NIST should harness its seminal publication, *Framework*, to inform the public about the threat subcontracting poses to trade secret protection.[117] Critically, the *Framework* should provide ways to mitigate subcontracting risks where possible and if not possible, note where potential gaps in protection may exist. To achieve these objectives, NIST should first replace its definition of personal information[118] with personal data as defined in the GDPR because it identifies a larger range of information afforded enhanced protection, such as data transmitted with an IP address or linked to an RFID.[119] This will provide a layer of protection for some trade secrets, including information about inventory tracked with an RFID monitored by a warehouse employee.

Second, NIST should incorporate the DTSA's definition of a trade secret in its Cloud Computing Guideline and Glossary. DTSA's definition of a trade secret is ideal because it is broad in scope, thereby protecting many of a businesses' activities.[120] The definition is as follows:

> [T]he term "*trade secret*" means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques,

117. NIST, *supra* note 53, at 18.

118. NIST Cloud Computing, *supra* note 52, at 21.

119. Regulation (EU) 2016/679 General Data Protection Regulation, recital 30, 2016, O.J. (L 119).

120. 18 U.S.C. § 1839(3).

> processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing . . . .[121]

Furthermore, NIST's use of the same definition as DTSA will increase consistency as to which components of a business are potentially protected under federal trade secret law and protected by cloud computing best practices.

B. Provide Protective Measures for Trade Secrets in NIST's Framework

Protective measures for trade secrets should be incorporated into the "Framework Core" and "Framework Profile" sections of NIST's *Framework*.[122] Since the "Framework Core" consists of five essential functions, "Identify, Protect, Detect, Respond, and Recover," methods to address trade secret threats should be contained in each[123]. Starting with "Function," the "Category: Asset Management" should include a "Subcategory" where assets are identified as trade secrets, then ranked in order of importance.[124] As mentioned, many SMEs identify "crown jewel" trade secrets as too valuable to place in the cloud and opt to store less critical information in the cloud.[125]

The next "Category: Business Environment" should include a "Subcategory" discussing which trade secrets drive the firm's market share and which competitors would be most interested in accessing the firm's trade secrets.[126] Importantly, "Category: Chain Risk Management" should include a "Subcontracting" category specifically for third-party, subcontractors in cloud computing.[127] Here, NIST would provide a Cloud Contracting Checklist to make it easy for small to mid-size businesses to compare the terms offered by their service providers to optimal terms related to trade secrets, other intellectual property, and personal data protections and obligations, the disclosure of subcontracting policies and allocation of liability.

The checklist would be modeled on key terms provided by the GDPR

121. *Id.*
122. NIST, *supra* note 53, at 3-4.
123. *Id.*
124. *Id.* at 24.
125. Savitz, *supra* note 17.
126. NIST, *supra* note 53, at 25.
127. *Id.* at 28.

along with several additions. This checklist would raise consumers' awareness of the terms offered to cloud clients' in other countries and potentially galvanize consumers to demand such terms from cloud service providers in the U.S. A Cloud Contracting Checklist would include the following—

General Contract Terms

 Contract specifies what is personal data, trade secrets, and other intellectual property.

 Contract specifies what obligations (including liability) and rights the client has, and the cloud service provider has in relation to the personal data, trade secrets, and other intellectual property.

 Personal data, trade secrets, and other intellectual property are not shared with third countries unless required under the law of the applicable jurisdiction, and when permissible by law, notification of such access will be provided to the client.

 Obligation to keep information confidential.

 *Discloses the jurisdiction in which it processes data.

 Obligation to protect data and ensure adequate safeguards are in place through monitoring continuously, documenting such monitoring, and conducting periodic audits. The client will have access to reports from such activities upon request.

Subcontracting Terms

 Includes a section disclosing whether subcontractors are used or not.

 *Discloses the name and location of the subcontractor, both where the business is incorporated and where it processes its data.

 Informs the client when it changes a subcontractor.

 Gives the client permission to withdraw from the agreement when a subcontractor changes.

 Holds the provider liable for subcontractor's failure to protect data to the level afforded by the contract between a client and cloud service provider.[128]

*This point is important because a firm should be wary of the jurisdiction in which a cloud service vendor operates as well as the jurisdiction in which its subcontractors operate because trade secrets, and data in general, will be at greater risk of exposure in countries with a reputation for cyber espionage, weak trade secret, and intellectual property protections, and/or lenient penalties for such actions.[129]

128. *See* Regulation (EU) 2016/679 General Data Protection Regulation, art. 28, 2016, O.J. (L 119) (using the GDPR terms as a basis for the Checklist).

129. *See generally* Portfolio 515, *supra* note 8, at 5 (discussing the range of diverse obligations and data privacy security issues associated with data being stored across multiple

Then, under the "Function: Protect," a category should be added for a cloud service provider certification scheme.[130] Such certification scheme would be created by CSA ideally, or a similar caliber organization, and would be endorsed and be subject to review by NIST. The decision to utilize a single certification scheme, when many exist in the marketplace, provides a consistent set of standards for clients to assess and compare cloud service providers. Such certification scheme would evaluate a provider's overall security protocol, monitoring and disclosure practices, and subcontracting protections.[131] This certification scheme would provide a ranking system based on the level of scrutiny a firm undergoes, further discussion to follow, and include a continuous monitoring system. The certification monitoring board would post a profile for each certified cloud provider on its registry website.

Essentially, a "red flag" monitoring program would be incorporated into the certification scheme, requiring a firm to self-report breach of personal data, trade secrets, or other intellectual property and permit clients to report such breaches to the certification monitoring board. Upon receiving notice of a breach, the certification monitoring board would post a "red flag" icon underneath the cloud provider's online profile with a description, thereby alerting clients. A threat ranking system could also be implemented, classifying threats as high, medium, or low based on the scope of the breach and provider's response time.

Next, under the "Function: Detect," a firm should develop its own in-house monitoring process, which should include monitoring its cloud service provider's certification profile to see if "red flags" have been posted.[132] The "red flag" monitoring system provides a low-cost method for SMEs to determine whether the breach impacted the company or will likely impact the firm in the future. NIST should also provide under the "Function: Respond" a separate "Subcategory" for an impact analysis.[133] In such analysis, a firm should evaluate the breach's impact on trade secrets and actions to mitigate the breach's impact (e.g. discontinuing the use of the cloud service provider).

If NIST adopts the aforementioned best practices, or similar practices, SMEs will have stronger grounds to file suit for trade secret violations in

jurisdictions).

130. NIST, *supra* note 53, at 29.

131. Star Certification, *About CSA Star Certification*, CSA (Mar. 7, 2018, 6:32am), https://cloudsecurityalliance.org/star/certification/#_overview [https://perma.cc/JMM6-2Q4T] *(*providing a basis for the proposed certification described here).

132. NIST, *supra* note 53, at 37.

133. *Id.* at 41.

state or federal court because both the cloud provider and subcontractor should know the data was not meant to be disclosed and the firm took adequate steps to safeguard its data.[134] Remedies may entail enjoining a cloud provider or subcontractor from conducting business or granting the client financial compensation.[135] Neither remedy will undo the harm of leaked trade secrets that may cause the firm to suffer significant loss and potentially cripple a SME. While individual actions may be insufficient to protect a firm from major trade secret losses, the goal is to reduce the frequency with which they occur sufficiently to motivate businesses to increasingly trust and use cloud computing. Raising market-wide awareness of the issue subcontracting poses to trade secrets, incentivizing cloud providers to provide fair and favorable terms, protecting a clients' data when subcontractors are used, and providing "red flag" warnings to the public when such breaches occur will make the market safer overall.

Finally, the "Function: Recover" may include stricter ways to monitor cloud service providers to better protect trade secrets in the future if the firm is still viable.[136] Again, individual firms will receive the greatest benefit and chance of recovering from a breach when cloud providers market-wide are incentivized to better protect trade secrets. A discussion below will evaluate whether such reform should be voluntary or mandatory.

Lastly, under the third segment of the *Framework,* "Framework Profiles,"[137] the certification scheme would be a useful tool for SMEs to evaluate and compare cloud vendors cheaply. According to NIST, such Framework Profiles are used by firms to assess target vendors and define mandatory protections the vendor must have in place before the vendor has access to the buying organization's systems.[138] Therefore, the results of a vendor's certification assessment could be included in such a cloud provider's Framework Profile, providing clients with an additional tool to select the optimal vendor.

---

134. *See Trade Secret*, *supra* note 30 (defining the three elements of a trade secret claim, including that reasonable precautions were taken to prevent the disclosure of the information); Krotoski, *supra* note 31, at 8 (noting that the Defend Trade Secrets Act grants remedies in either state or federal court).

135. Krotoski, *supra* note 31, at 10.

136. *See* NIST *supra* note 53, at 43 (describing how the Cybersecurity Framework would incorporate learned lessons into future activities).

137. *Id.* at 4.

138. *See id.* ("Profiles can be used to identify opportunities for improving cybersecurity posture by comparing a "Current" Profile (the "as is" state) with a "Target" Profile (the "to be" state).").

C. Certification Scheme

As referenced above, under the NIST Framework Function "Protect," a certification scheme endorsed by NIST and implemented by CSA, or a similar high-quality organization, would lower a SME's due diligence costs and increase the quality of information available to the SME. The NIST/CSA Certification Scheme's assessment rubrics used by auditors and responses for each participating provider would be reported in an online registry, enabling clients and potential clients to identify the strengths and weaknesses of each participating provider. Namely, the vendor's certification profile would provide SMEs with a low-cost way to evaluate the cloud service provider's organizational structure, security measures, service agreement terms, and the use of subcontractors. Additionally, the "red flag" monitoring program, as previously described, would require firms to self-report breach of personal data, trade secrets, or other intellectual property and would permit clients to report such breaches. The public's accessibility to provider certification audits and breach history would reduce the asymmetrical information hurdle faced by SMEs. With greater transparency in the marketplace, providers would likely be motivated to offer more secure and consumer-friendly services to avoid reputational damage and decline in customer demand.

The question remains unsettled whether such a certification scheme should be voluntary or mandatory. Reform may not happen quickly enough without federal regulation because it may take longer for the majority of providers in the industry to comply, which would in turn delay growth in consumer trust in cloud computing. On the other hand, coupling the certification scheme with an education campaign for consumers may motivate consumers to seek service providers that are CSA certified, thereby driving other providers to adapt to keep up with customer demand. The additional pressure from Europe and Asia, which have already implemented data privacy reforms,[139] may make cloud providers wary of similar legislation in the U.S. To delay such measures, cloud service providers may have a greater incentive to comply with NIST's voluntary certification scheme. This may be especially true given the harsh penalties imposed by the GDPR, as well as the low bar for personal claims.[140] If none of these

139. *GDPR Resource Center*, CLOUD SECURITY ALLIANCE https://gdpr.cloudsecurityalliance.org [https://perma.cc/4PMB-2HUJ] (last visited Mar. 7, 2018 6:13 PM).

140. *See EU General Data Protection Regulation – Key Changes*, DLA PIPER https://www.dlapiper.com/en/uk/focus/eu-data-protection-regulation/key-changes/ [https://perma.cc/M4C4-NV3X] (last visited Mar. 9, 2018 10:48 AM) (noting the low bar for personal data as any information that can reasonably be used to identify a natural person).

theories hold sufficiently true, then the government could initiate investigative actions by the FTC.[141] Such investigations, industry-wide or individual, could be used to marshal support for legislative reform that mandates certifications and imposes harsh penalties for failure to comply.

Structurally, Cloud Security Alliance's Security, Trust & Assurance Registry (CSA STAR) certification program is an ideal candidate to modify because it incorporates international standards such as SOC 2 and ISO and complies with EU law.[142] The scheme evaluates subcontracting generally and could be expanded to assess safeguards for trade secrets, personal data, and other intellectual property. CSA's STAR program consists of three levels: (1) self-assessment, (2) third-party assessment-based certification, and (3) continuous monitoring-based certification.[143] The "red flag" alert system should be incorporated into the level three continuous monitoring-based certification. Relying on a single scheme, as discussed earlier, as opposed to multiple schemes provides clients with a standard guideline to compare providers and allows NIST to better focus its attention and oversee the program. As a means to externally validate the program and monitor the criteria used in the scheme, such certification program could be reviewed by the NIAP under the protection profiles (PP) screening process.[144]

The first level of the NIST/CSA Certification Scheme would comprise of a self-reporting device, similar to the CSA STAR's Assessments Initiative Questionnaire (CAIQ), which asks a series of yes or no questions about data security, privacy, and disclosure policies a cloud service provider follows.[145] The CAIQ addresses subcontracting under the header, "Supply Chain Management, Transparency, and Accountability (Third Party Agreements)."[146] Two questions are directly pointed at subcontracting terms: Do you provide the client with a list and copies of all sub-processing agreements and keep this updated? (Check y/n). Do third-party agreements

141. *See* FEDERAL TRADE COMMISSION, *supra* note 45 ("The [Federal Trade] Commission may prosecute any inquiry necessary to its duties in any part of the United States and may gather and compile information concerning, and to investigate from time to time the organization, business, conduct, practices, and management of any person, partnership, or corporation engaged in or whose business affects commerce.").

142. CLOUD SECURITY ALLIANCE, *supra* note 139.

143. *Id.*

144. *See* NIAP, *supra* note 48 (defining a protection profile as "an implementation-independent set of security requirements for a particular technology that enables achievable, repeatable, and testable evaluation activities for each evaluation.").

145. *See CSA CAIQv.3.01, Section: Supply Chain Management, Transparency, and Accountability*, CLOUD SECURITY ALLIANCE (OCT. 12, 2017), https://cloudsecurityalliance.org /download/consensus-assessments-initiative-questionnaire-v3-0-1/ [https://perma.cc/NC89-R4VU] (referring to Third Party Agreements under ID STA-05 in excel format).

146. *Id.*

include provisions for the security and protection of information and assets?[147]

Here, the proposed certification scheme should incorporate the points from NIST's Subcontracting Checklist into a series of questions for providers to answer. Having cloud providers respond to the questions inspired by the Checklist will provide SMEs with critical information about providers' trade secret protection obligations, subcontracting practices, and data protection policies. Forcing providers to be more transparent about their responsibilities and practices will enable SMEs to evaluate whether a provider is worth trusting and whether providers market-wide should offer greater protections and better policies.

Key questions adopted from NIST's Subcontracting Checklist include—

General Contract Terms

 Does the contract specify what personal data, trade secrets, and other intellectual property is?

 Does the contract specify what obligations (including liability) and rights the client has and the cloud service provider has in relation to the personal data, trade secrets, and other intellectual property?

 Is personal data, trade secrets, and other intellectual property not shared with third countries unless required under the law of the applicable jurisdiction, and when permissible by law, notification of such access will be provided to the client?

 Is there an obligation to keep information confidential?

 Does the contract disclose the jurisdiction in which the firm processes data?

 Is there an obligation to protect data and ensure adequate safeguards are in place through monitoring continuously, documenting such monitoring, and conducting periodic audits? Does the client have access to reports from such activities upon request?

Subcontracting Terms

 Does the contract include a section disclosing whether subcontractors are used or not?

 Does the contract disclose the name and location of the subcontractor (both where the business is incorporated and where it processes its data)?

 Does the cloud service provider inform the client when it changes a subcontractor?

 Does the contract give the client permission to withdraw from the

147. *Id.*

agreement when a subcontractor changes?

 Does the contract hold the provider liable for subcontractor's failure to protect data to the level afforded by the contract between a client and cloud service provider?[148]

At this first level, the responses provided to the CAIQ and the proposed questions above, would be self-reported and therefore would not undergo an auditor's scrutiny. In the second level of the certification process, auditors would evaluate the same series of questions, making the disclosure more reliable than the self-reporting in the first level.[149]

The second level should mimic the CSA's third-party assessment-based certification process, which involves two independent, third-party evaluations: (1) CSA STAR Attestation and (2) CSA STAR Certification.[150] CSA STAR Attestation is a collaboration between CSA and AICPA, whereby specially trained accountants,[151] from firms such as Deloitte, Ernst & Young, and KPMG, conduct SOC 2 attestations and supplement with the Cloud Controls Matrix criteria.[152] Though SOC 2 is not designed with cloud services in mind, it asks critical questions that are directly applicable to subcontracting.[153] For example, C3.6.0, paraphrased, evaluates whether an "entity has procedures to obtain assurance or representation" that "confidentiality policies of third parties to whom information is transferred" conform with the firm's confidentiality and related security policies and the third party is in compliance with such policies.[154] In addition to evaluating firms using SOC 2, auditors should assess firms based on the CSA Cloud Controls Matrix, which addresses cloud specific issues.[155] Many of the questions in the Matrix parallel those in the CAIQ, from level one, and should incorporate the questions adopted from the NIST Subcontracting

148. *See* Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC, art. 28, 2016 O.J. (L 119) 1, 49-50 (listing the GDPR terms which have been used as a basis for the Checklist).

149. CLOUD SECURITY ALLIANCE, *supra* note 139.

150. *Id.*

151. *See CSA Corporate Members Providing CPA Attestation Services*, CSA, (Mar. 7, 2018, 6:27 PM), https://cloudsecurityalliance.org/star/attestation/#_auditors [https://perma.cc/2NZT-W6RD] (discussing cloud specific assessment training for CPAs certified in Cloud Security Knowledge (CCSK)).

152. *Id.*

153. *Cloud Controls Matrix Working Group*, CSA, (Mar. 7, 2018, 6:29 PM), https://cloudsecurityalliance.org/group/cloud-controls-matrix/#_overview [https://perma.cc/E5HB-J7YA].

154. *Id.*

155. *Id.*

Checklist.[156]

This second level of evaluation holds greater weight than the former because an independent third party assesses the cloud provider's reported practices, paralleling the auditing process required for a financial statement filed with the SEC.[157] The Matrix should be used because it carefully indicates which of the CSA's standards correspond with other standards, such as those from NIST, FedRAMP, and the EU Directive,[158] providing easy comparisons across frameworks and cloud provider profiles. The other independent third-party evaluation should closely follow the CSA STAR Certification, which assesses the cloud service provider's security and combines the requirements of ISO/IEC 27001:2005 management system standard with its CSA Cloud Controls Matrix.[159]

The third-level continuous monitoring-based certification, should be expanded beyond CSA's framework, which provides customers with information about cloud service providers' security practices in a clear format.[160] The "red flag" monitoring system, previously described, should be included. Overall, the NIST/CSA Certification Scheme would provide SMEs with free access to information about the security and quality of cloud service providers in the market-place. Lowering a SME's due diligence costs and increasing the quality of information available to the SME will enable the client to find the most suitable provider available. Furthermore, increased transparency will enable SMEs to collectively demand better policies and practices from cloud service providers.

D. Voluntary, Industry Initiated Cloud Code of Conduct

Drawing from the basic premise of the voluntary EU cloud code of conducts, a single voluntary Cloud Code of Conduct should be created in the U.S. The U.S. government should encourage industry practitioners to sponsor and develop a Code that would require providers to use consumer-oriented contracting terms, comply with NIST's Certification Scheme, and conduct business in countries with strong IP safeguards.

---

156. *Id.*

157. *Id.*

158. *See Cloud Controls Matrix v.3.0.1*, CSA (2017), https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3-0-1/ [https://perma.cc/46DQ-MDGY] (showing Matrix mapping along the top row of the excel file).

159. *See Star Certification*, CSA, (Mar. 7, 2018 6:32 PM), https://cloudsecurityalliance.org/star/certification/#_auditors [https://perma.cc/Y29X-FNNT] (indicating that auditors should be accredited to ISO 27006 and are from firms such as Coalfire ISO, Schellman & Company, LLC).

160. CLOUD SECURITY ALLIANCE, *supra* note 139.

Instead of serving as a compliment to an existing piece of legislation, as codes do in the EU, a voluntary Cloud Code of Conduct program could serve as the basis for future legislation. The possibility of future legislation should be dangled in front of the industry as both a carrot and a stick, so to speak. Essentially, the U.S. government could incentivize industry to voluntarily create a Cloud Code of Conduct, by reminding providers that creating such a code would allow them to establish the basic framework and standards used in future legislation. Contrastingly, failure to implement a feasible Code, with adequate safeguards and standards, could result in harsh regulation of the industry with steep penalties for data breaches and failure to protect personal data, trade secrets, and other intellectual property. Harsh penalties already or will soon exist in other parts of the world, such as the EU and Asia.[161] Therefore, the threat of unfavorable regulation in the U.S. is a legitimate risk and would likely motivate the industry to create a reasonable Cloud Code of Conduct.

Lessons should be learned from the EU Cloud Code of Conduct, the most publicized code that developed from an EU working group initiative.[162] Namely, the U.S. Cloud Code should have a decision-making board comprised of cloud service providers, academics, and trade association representatives representing small to mid-size businesses. A diverse board will likely drive more balanced solutions that do not weigh too heavily in favor of providers, as the EU Cloud Code of Conduct presently does. Pledgees should agree to adhere to NIST definitions and best practices from the *Framework*.

The main objectives of the Code's board should center, as mentioned, around requiring members to provide consumer-oriented contracting terms, comply with NIST's certification scheme, and identify countries with strong IP safeguards. To maintain consistency with NIST's *Framework* and NIST/CSA Certification Scheme, the terms set forth in the NIST Subcontracting Checklist should be used. Central to the terms, and inspired by the standards in the GDPR,[163] is the liability placed on cloud service providers if their subcontractors fail to provide the same level of protection (terms) for the client's data as originally agreed upon between the cloud service provider and client. Placing the responsibility on the cloud service

161. *Id.*

162. European Cloud Code of Conduct, *supra* note 83.

163. *See* Regulation (EU) 2016/679 General Data Protection Regulation, art. 28, 2016, O.J. (L 119) (requiring that controllers "shall use only processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject").

provider is essential because it incentivizes the provider to be more cautious and selective when using subcontractors.[164]

Additionally, there should be a condition that cloud service providers disclose their use of subcontractors, provide notification when subcontractors change, and include an option for clients to withdraw from the agreement if subcontractors change.[165] To demonstrate compliance with the Code, cloud providers could be instructed to create a notification system including a subcontractor registry accessible to clients. Providers will likely accept the cost of increased due diligence to select a reliable, quality subcontractor to reduce the risk of the subcontractor failing to protect the client's data to the same level stipulated between the provider and client.

Next, the board should require pledgees to comply with NIST's Certification Scheme, regardless of whether certification is required by law or voluntary. To facilitate better cooperation with NIST and the CSA, the Code board should designate liaisons to each organization. Additionally, the board should conduct meetings with NIST and the CSA regarding the certification process to learn about updates to the program, recent compliance issues, and data security concerns.

Another critical objective of the board would entail identifying countries with strong IP safeguards and developing a list of countries with favorable IP policies. Pledgees to the code should agree to only use subcontractors from such countries. Critically, this requirement makes it a condition that pledgees would themselves be from countries on the aforementioned list. Specifically, the board should evaluate whether a country has robust IP policies in place that disincentivize trade secret theft and allow for rights of action by foreign businesses/actors. Since trade secrets are often stolen through such espionage attacks, determining whether a country's government has a reputation for respecting data access and penalizing cyber espionage is critical. Additionally, where the U.S. has data privacy agreements and similar agreements in place, the board should determine whether the safeguards adequately protect IP and are being successfully enforced (as determined by self-reporting from both governments, independent third-party audits, and general industry consensus

164. *See* Mark Webber, *The GDPR's impact on the cloud service provider as a processor*, 16 J. PRIVACY & DATA PROTECTION 11, 13 (2016) http://www.fieldfisher.com/media/3993765/the-gdprs-impact-on-the-cloud-service-provider-as-a-processor-mark-webber-privacy-data-protection.pdf [https://perma.cc/82HW-EXCD] (discussing processors' and controllers' duties and responsibilities under the GDPR).

165. *See* Regulation (EU) 2016/679 General Data Protection Regulation, art. 28, 2016, O.J. (L 119) (stating that controllers "shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes").

surveying). Such a requirement will likely increase the cost of using subcontractors because clients will have to select higher quality third-parties. Consequently, providers may be more selective in choosing their subcontractors to justify the cost or carry-out these functions themselves, thereby reducing the risk of trade secret violations.

Monitoring and enforcement of the Code should aim to instruct more than punish.[166] Specifically, a separate Code committee should be responsible for monitoring pledgees' compliance with the code and NIST certification status.[167] Another committee responsible for enforcement of the Code should develop a warning system for minor first-time offenses and an education program for more significant offenses that can be corrected through training.[168] If the offense is significant and cannot be corrected or should not be corrected through training, then removal from the Code is warranted and notification will be provided in the program's public registry.[169]

E. Federal Initiative: Subsidies for U.S. Cloud Computing Infrastructure Development

The government should offer subsidies for cloud computing infrastructure development to encourage growth of domestic cloud computing providers and domestic subcontractors. The U.S. risks falling behind, as other countries continue to develop their own regulations and incentives for cloud computing that protect their citizens' data and favor their citizens' businesses.[170] Businesses contracting with providers in countries with both poor protections for IP and reputations for cyber espionage pose a critical threat to small and mid-size enterprises. According to a 2016 Verizon Data Breach Investigation Report, more than half of breaches were the result of cyber espionage in the manufacturing industry.[171] Development

166. *See* European Cloud Code of Conduct, *supra* 83, at 30 (contrasting the EU CoC's enforcement policies).

167. *See Id.* at 35 (paralleling the EU CoC's use of a separate monitoring body).

168. *See Id.* at 35-36 (implementing a warning system and education program for offenses committed by pledgees will provide constructive guidance for pledgees and improve consumer trust; neither proposal is included in the EU CoC).

169. *See Id.* (separating infractions into those that can be remedied without removal from the registry and those that cannot offers more specific guidance about acceptable behavior to pledgees than the EU CoC, which does not make this distinction).

170. *See* CLOUD SECURITY ALLIANCE, *supra* note 139 (discussing "[t]he new General Data Protection Regulation (GDPR)" and that "[t]he regulation will apply to all industries across the European Union.").

171. Frank M. Groom, Stephan S. Jones, *Enterprise Cloud Computing for Non-Engineers*, CRC PRESS, "Security Considerations" (2018), https://books.google.com/books?id=NGNRD

of a robust network of U.S. based cloud service providers and subcontractors could reduce the risk posed by reliance on foreign cloud service providers. Subsidies could be used to spur development of new providers and incentivize current providers to relocate to the U.S. Reducing the cost of operating a cloud service in the U.S. would allow firms to keep their prices competitive with foreign providers, enabling small to mid-size enterprises to choose a provider based on quality over cost.

F. Federal Regulation of Cloud Computing with Voluntary, Industry Initiatives

Federal law regulating cloud computing should codify NIST's *Framework* and glossary of terms, which include the proposed definitions for personal data and trade secrets. Assuming the industry creates a successful voluntary Cloud Code of Conduct, federal law would adopt most of the framework. The Code's central requirements for pledgees to provide consumer-oriented contracting terms, comply with NIST's Certification Scheme, and conduct business in countries with strong IP safeguards for U.S. clients will provide the foundation for the federal law. Because providers already underwent major reforms to comply with the Code, the burden of complying with the law will be significantly reduced. Though the process of adhering to the Code's standards would be costly and time-consuming, providers could have the option to make changes at their own pace and apply for membership when ready without the risk of facing financial penalties for failure to comply by a specified deadline.

The consumer-oriented contracting terms from the Code, adopted from NIST's Subcontracting Checklist, should be codified in this federal law. Penalties for violations should fall on a sliding scale, with fines up to $5 million dollars, or 1% of annual worldwide revenue, whichever is greater.[172] Fines would be higher for certain offenses, such as (1) failure to ensure subcontractors protect data to the same level as stipulated between client and provider, and (2) failure to provide and/or follow terms protecting trade secrets, personal data, or other intellectual property law. A private right of

---

wAAQBAJ&pg=SA2-PA50&lpg=SA2-PA50&dq=cloud+computing+trade+secret+threat+by+cyber+espionage&source=bl&ots=qhh3Hj5oLw&sig=zS9MGMa2ExCgCqDF5XJ5BfjIzSk&hl=en&sa=X&ved=0ahUKEwih8t6dqqbaAhXD31QKHWLJDkAQ6AEIPTAD#v=onepage&q=cloud%20computing%20trade%20secret%20threat%20by%20cyber%20espionage&f=false [https://perma.cc/35FF-EP7S].

172. *See* Regulation (EU) 2016/679 General Data Protection Regulation, art. 83, 2016, O.J. (L 119) (serving as the basis for fines in the proposed U.S. legislation, but penalties would be less severe in the U.S.).

action would also exist for economic losses.[173] The Code's structure bolsters a client's claim under the DTSA for trade secret violations because the nature of the agreement, as stipulated under the law, demonstrates the client took adequate measures to safeguard the trade secrets.[174] Additionally, a client would have separate right to a breach of contract claim.[175]

Compliance with the NIST/CSA Certification Scheme would also be mandatory under federal regulation, as in the Code. To screen the widest pool of market participants, certification should be mandatory for any cloud provider conducting business with the U.S. A penalty system should be imposed based on a stratified structure—$500 thousand to $1 million for failure to make an initial submission for certification, $500 thousand for failure to follow recommendations provided by the certification board, and $200 thousand to $2 million for repeated "red flag" offenses or a severe data breach that was willful, reckless, or negligent.[176]

Arguably, the most controversial condition of the Code would be included in the federal law—cloud service providers must conduct business in countries with strong IP safeguards for U.S. clients based on a pre-approved list. The criteria for the list would parallel the Code's, but would offer an appeals process[177] for providers willing to undergo an independent, third-party audit of their business practices and the infrastructure they have in place to protect trade secrets, personal data, and other IP. Violations of the law would result in financial penalties for both the client and provider unless the client was deceived into contracting with a non-approved vendor. Providers who deceive clients would incur financial penalties under this law and would likely face fraud charges as well.[178]

If and when the law is implemented, the Code should transition to an advisory "think-tank." The Code board would be responsible for hosting education initiatives in collaboration with the government and NIST to provide members with the most recent industry risks and best practices. The Code board would host member forums to discuss solutions to security

173. *Id.*

174. LII, *supra* note 30; Krotoski, *supra* note 31, at 8.

175. Gourley, *supra* note 9, at 4-13.

176. *See* Regulation (EU) 2016/679 General Data Protection Regulation, art. 83, 2016, O.J. (L 119) (serving as the basis for fines in the proposed U.S. legislation, but penalties would be less severe in the U.S.).

177. *See EU General Data Protection Regulation – Key Changes*, DLA PIPER (Mar. 9, 2018 10:48 AM), https://www.dlapiper.com/en/uk/focus/eu-data-protection-regulation/key-changes/ [https://perma.cc/NE4U-FPYV] (discussing the approval process for international data transfers; the proposal here is loosely inspired by the GDPR's strict data transfer measures).

178. 18 U.S. Code § 1341.

threats, and trade secret violations. Additionally, the board would propose initiatives for members to vote, by majority of those attending, to implement new standards to comply with to better protect trade secrets in the cloud. Both the board's forums and new standards would serve as a testing ground for new reforms and government legislation, thereby fostering continuous improvement of cloud computing regulation.

G. Federal Regulation of Cloud Computing Without Voluntary, Industry Initiatives

If federal laws were developed without implementing a voluntary Code of Conduct first, then the legislation may receive less support from the industry because market-participants would not have as much say in the law's framework. Critically, providers would not have the grace period the Code would afford to implement the required safeguards. Instead, providers may have to rush to implement costly protective measures or risk heavy penalties for failure to comply with the legislation's prescribed deadline. The development of the law itself may be more adversarial and risky for cloud service providers because the law may rely on FTC studies and enforcement actions[179] against providers to develop the foundation for the Code. Therefore, the Code may take a more punitive tone, with steeper financial penalties as in the GDPR, for violation of the law.[180]

The federal law would adopt the terms from NIST's Subcontracting Checklist, as above. Certification would also be mandatory, for the reasons previously discussed, as would a similar requirement that cloud providers conduct business in countries with adequate IP safeguards based on a pre-approved list. However, an appeals process would be unlikely because it would be too much of an added risk on an already untested piece of legislation. Without the Code of Conduct, the legislation would lack prior market screening and feedback, making nuanced solutions challenging in the first iteration of the law. Consequently, significant amendments may be required of the legislation. Additionally, there is a lost opportunity to transform an industry-created code into a think-tank and industry advisor to the government for future reform and legislation.

179. FED. TRADE COMMISSION, *supra* note 45.

180. *See* Regulation (EU) 2016/679 General Data Protection Regulation, art. 83, 2016, O.J. (L 119) (describing penalty structure.).

CONCLUSION

Adoption of cloud computing is growing, but client trust remains low. Trust is especially low amongst small to mid-size businesses, who stand to lose their "crown jewel" trade secrets and, ultimately, their business if their trade secrets are leaked. Neither contract law nor trade secret law provide adequate recourse for SMEs if their data is breached in the cloud, namely by a subcontractor. Furthermore, the U.S. lacks cloud computing regulation, which more generally places U.S. SMEs and U.S. business clients at a disadvantage because other countries have increasingly adopted cloud computing regulations that protects their citizens' interests, including subcontracting practices. To remain competitive in the cloud computing industry and protect U.S. clients' trade secrets, NIST should expand its definition of personal data to match the one provided in the GDPR and incorporate the DTSA's definition of trade secret in its seminal work, *Framework*. NIST should collaborate with CSA to create a certification scheme to evaluate and monitor cloud service providers' subcontracting, trade secret, personal data, and security practices. Subsidies should be offered to U.S. based providers by the government to incentivize growth of domestic cloud services. Optimally, a voluntary Cloud Code of Conduct should be established as a means of self-regulation in the industry. This Code should serve as the basis for cloud computing legislation, and transition to a think-tank function after legislation is passed to help the U.S. identify and respond to the latest issues in cloud computing.