White Paper on Cloud Computing: Overcoming Challenges of Integrating Robust Competition with Security

by

John W. Bagby

Abstract

Cloud computing is a growing service industry supplying an expanding portfolio of individual services rendered to end-user clients. Such services are roughly classified as remote data storage, user-access interface and data processing. Regulators around the world are scrutinizing the contracting practices, industrial organization and the resulting quality of service levels in cloud computing service markets. This white paper analyzes the cloud’s architecture as the essential underpinning to successful encouragement of security investment, standardization, cloud regulation, information governance, economic incentives and the cloud’s achievement of critical infrastructure importance.

Introduction

Competition is the primary impetus for cloud computing. Cloud computing offers and often delivers infrastructure cost savings, expertise, broad geographic accessibility, process automation, redundant data backup, scalability and rapid-standardized upgrades. Advocates of outsourcing frequently argue successfully that enterprises of all sizes should be encouraged to delegate certain information technology (IT) functions. Cloud services contracts generally transfer some in-house IT operations to independent service organizations, the separate entities that provide cloud computing services. Ideally, such delegations occur when the latter are capable of achieving economies of scale in functionality, expertise, software and hardware. This white paper reviews the alignment of such economic incentives to achieve an industrial organization.

---

1 Submission to Solicitation for Public Comments (RFI) on the Business Practices of Cloud Computing Providers, Federal Trade Commission, FTC Docket No. FTC-2023-0028 (Mar. 21, 2023) https://www.ftc.gov/system/files/ftc_gov/pdf/CloudComputingRFI.pdf This white paper is not directly organized to respond in the order of the FTC’s enumerated queries, but nevertheless, provides indirect replies through implication to the FTC’s specific queries.

2 Professor Emeritus, Smeal College of Business and College of Information Sciences and Technology, The Pennsylvania State University.
Cloud Competition & Security

(I/O) that results in outcomes beneficial to society. It is axiomatic that an enduring competitive environment will remain elusive in the quest for optimal societal results.  

Cloud Architecture has become a Key Element in the AI Information Supply Chain

Cloud computing has developed through various stages, initially as a conceptual design since the 1950s. However, development of the cloud’s “virtualization” functionality permits outsourcing and this has offered a significant reduction of in-house expense for IT hardware, software and personnel. This is the initial competitive advantage cloud computing offers. It has made cloud services a central storage phenomenon throughout business, non-governmental organizations (NGO) and government processes.

Projections for strong growth in cloud services strongly suggest cloud computing services was a once ephemerally-defined industry. Standard Industrial Classification (SIC) is a government taxonomy of industries used in many nations for various regulatory purposes. For example, the SEC still uses traditional SIC coding to classify registrants’ disclosure filings. While technology innovation and market transformation may require near-constant evolution in SIC classification schema, such coding remains useful to understand cloud computing services (work performed) as well as the industry’s structure (industrial organization), its contracting practices (terms of service (ToS) and end-user license agreements (EULA)), and the markets for work actually performed by the cloud’s primary end-users. Under traditional 4-digit SIC Codes, cloud computing services is likely embodied in, at least, several separate classes in the range of 7000-8999 – Services, more specifically: 7370 - Services-Computer Programming, Data Processing, Etc.  

4 General use computing capable of enabling hardware of a single computer or server (farm) to be divided or partitioned, thus simulating separate and independently operating “virtual computers.” See e.g., What is Virtualization, IBM https://www.ibm.com/topics/virtualization  
5 Consulting firms abound with general agreement on, at least, good medium-term prospects for cloud computing services, identifying the market-leading cloud service providers and projecting generally strong revenue growth, see e.g., 2023 State of the Cloud Report, FLEXERA (2023) https://resources.flexera.com/web/pdf/Flexera-State-of-the-Cloud-Report-2023.pdf  
6 Related 4-digit SIC codes implicating cloud computing services include: 7371 - Services-Computer Programming Services; 7372 - Services-Prepackaged Software; 7373 - Services-Computer Integrated Systems Design; 7374 - Services-Computer Processing & Data Preparation; 7370 - Services-Computer Programming, Data Processing, Etc.; 7371 - Services-Computer Programming Services; 7372 - Services-Prepackaged Software; 7373 - Services-Computer Integrated Systems Design; 7374 - Services-Computer Processing & Data Preparation.
In recent years, the cloud computing industry is becoming more precisely defined under the replacement regime for SIC coding, the NAICS.\textsuperscript{5} This is likely driven by


cloud computing services solidifying its core competences, while expanding into new markets by: (i) diversifying its service offerings,\textsuperscript{9} (ii) identifying and courting new, underserved end-user clientele industries,\textsuperscript{10} and (iii) penetrating into new world markets.\textsuperscript{6} Still, with negotiated, non-standard cloud contracting as a source of potentially higher transactions costs, expansion into these new markets could be less profitable for the cloud services industry. This projected reversal of historically “excessive returns” could, perhaps, incentivize further market segmentation. Such trends strongly suggest further development of automated negotiations, the proliferation of boiler-plate and smartcontracting\textsuperscript{7} in some specific EULA terms. Furthermore, some configurations are likely to involve blockchain, distributed ledger technology.\textsuperscript{8} Government would appear to be

Classification System (NAICS). Under the revised NAICS, cloud computing services are designated as No. 518210 Cloud Computing Services (excepting software publishing and computer systems design):

518210 Computing Infrastructure Providers, Data Processing, Web Hosting, and Related Services

This industry comprises organizations primarily engaged in providing computing infrastructure, data processing services, web hosting services (except software publishing), and related services, including streaming support services (except streaming distribution services). Data processing

\textsuperscript{5} In recent years, the U.S. Office of Management and Budget (OMB) has managed revision of the SIC coding system for Canada, the U.S. and Mexico into the North American Industry

\textsuperscript{6} Cloud services appears to have penetrated the North American market most successfully. Incursions into China, India and Australia appear to be the next-ranked geographic market penetration. Much of the EU and the developing world appear underserved by cloud computing. See, e.g., Cloud Computing Market Size, Key Players, Revenue, Share, Future Trends, Growth and Forecast 2031, MARKETWATCH (April 18, 2023) https://www.marketwatch.com/pressrelease/cloud-computing-market-size-key-players-revenue-share-future-trends-growth-and-forecast-2031-2023-04-18


establishments provide complete processing and specialized reports from data supplied by clients or provide automated data processing and data entry services.

https://www.census.gov/naics/?input=cloud+computing&year=2022&details=518210

9 Id. and see infra, discussion of NIST classification of cloud service models, IaaS, PaaS and SaaS. These general classifications can be further sub-divided into numerous particular functionalities, many not generally considered as cloud computing services, but instead, as end-user client industry functions among those which patronize cloud computing services, see id. 2022 NAICS No.518210 ostensibly includes such services as scanning, video streaming, cryptocurrency mining, video games, data entry, etc.


10 Financial services appear to lead cloud services as the top end-user industry client grouping. Large clients comprise over half of cloud computing service clients. This leaves most other industries as well as small to medium-sized businesses (SMB) as currently underserved by cloud computing, thus, holding promise for considerable growth in end-use of cloud computing services.

another, significantly underserved end-user client segment, but generally operating under hybrid contracting rules. 14

Cloud data repositories and remote data processing have grown most rapidly in the past decade. 15 Today, and for the foreseeable future, increasing amounts of record keeping, transaction processing, and big data availability, the latter particularly as feedstock for artificial intelligence (AI), will rely on cloud computing. While definitions differ for cloud computing, provisionally, here, consider the cloud as largely third-party services provided as electronic storage and processing of permanent records, intermediate storage of transaction communications, and data-minable repositories. The latter promises high-quality forensics in discovery of investigatory leads and analyses to base decision-making, theretofore obscured by complexity. 9 Clouds are classified in many ways including as to their industrial organization as a near utility with service or as private clouds tied to a limited range of clients. 10 Cloud computing is enabled by the once steadily decreasing costs of digital electronic data processing and storage (Moore’s
Cloud Competition & Security

Law) due to economies of scale achieved in dispersed, large-scale data center infrastructures.


Cloud Computing Service Models

There is developing a wide variety of extant and (near) imminent cloud computing service models. This alone evidences that cloud services are developing as leading and producing, or at least, responding to, a competitive environment. Consider there is emerging a proliferation of cloud service models, particularly as to complex and multi-service design architectures. These models address or promise functionality based on client experience, current demand and projections of future client needs. Factors include the devolution of many data storage and data processing functions while providing client options in (i) ownership and control over cloud hardware and services, as well as (ii) addressing the accommodation of variations in the physical location of cloud client users, (iii) variations in the physical location of cloud servers (as the foundational cloud computing hardware resource), (iv) variations in data formatting, (v) variations in user interfaces, and (vi) variations in applications program interfaces (API).

Cloud service providers appear ready to provide additional options that further segment their markets. While the history of cloud service development, as well as the current state of its competitive environment, are key matters in assessing cloud computing competition and security, predicting its future industrial organization is essential to any meaningful and durably efficacious regulatory intervention. For

---

Cloud Competition & Security


See generally, John W. Bagby & Nizan Geslevich Packin, *RegTech and Predictive Lawmaking: Closing the RegLag between Prospective Regulated Activity and Regulation*, 10 Mich.Bus. & Entrep. L.Rev. 127-177 (2021) [https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1118&context=mbel](https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1118&context=mbel) (arguing regulators can anticipate regulable activities by recognizing delays inherent in regulatory lag (RegLag) then by deploying various predictive regulatory tools of RegTech and big data).

Hereinafter, the term *industrial organization* is used in the micro-economics and antitrust economics sense. This means that, herein, the cloud computing services industry is subjected to analysis of its structure, ownership, supplier and customer relationships, market power, barriers to entry, transactions costs, and transparency/opacity of information. This industry architecture approach seems well-suited to reveal answers to the FTC’s RFI primary inquiries (FTC Docket No. FTC-2023-0028) on competition, market power, and business/contracting practices that likely impact the industry’s resulting levels of service. Thereby, evaluation of these conditions might thereby reveal particular potential points of failure, anticompetitive practices and how security risks are externalized to clients, customers and individuals’ data privacy interests. See generally, Joe S. Bain & P. David Qualls, *INDUSTRIAL ORGANIZATION: A TREATISE*, 2nd ed., (1987, JAI Press, Greenwich CN); Leonard W. Weiss, *StructureConduct-Performance Paradigm and Antitrust*, 127 U. Pa. L. Rev. 1104-1140 (1978) [https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=4870&context=penn_law_review](https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=4870&context=penn_law_review).

A deeper dive into industrial organization is now more readily available with big data inputs into the input-output modelling, first developed by Wassily Leontief, a technique for which he won the 1973 Nobel Prize “for the development of the input-output method and for its application to important economic problems,” [https://www.nobelprize.org/prizes/economic](https://www.nobelprize.org/prizes/economic). For example, cloud service providers generally supply at least primary data storage with the Infrastructure as a Service (IaaS) model making client data accessible to a variety of clients’ computing hardware. Some cloud services add Platform as a Service (PaaS) functionality to IaaS by including development tools and often constitute a form of host interface to access underlying data and/or content. Software as a Service (SaaS) adds data processing to IaaS and PaaS capabilities by adding software applications. SaaS is also sometimes known as Web Services, enabling remote and mobile terminals with network access to solve problems. SaaS also better enables Application Services Provider (ASP) contracting models that enable software pricing based on usage, subscription models or other departures from fixed-price software licensing schemes.

---


Cloud Competition & Security

There is likely a wide range between standardized, boiler-plate cloud computing service provider terms of service (ToS) and separately negotiated and significantly more flexible ToS in contracts with higher stakes. Costly negotiation of technically-oriented terms breeds boiler plate such as when low transactions costs drive contracting in an oligopoly. Thus, this condition breeds standardized form contracting with take-it-or-leave it ToS. When such boilerplate restricts access to the cloud as an essential service, particularly for small to medium sized businesses (SMB), the condition of adhesion contracting is strongly implicated.14

Industrial Organization of Cloud Computing Services

Despite the competitive discipline that inspired the advent of cloud services, as in many markets, other factors eventually emerge to reorganize the competitive environment. For example, such forces include actual contracting practices, contract dispute resolution experience, alternative products/services that may serve as substitutes, innovation and vicarious experiences that inspire coordination among other nations also struggling with results from extant industrial organization structure and performance.24

Cloud computing initially emerged as an outsourced activity.25 As with many domestic industries, outsourcing to other nations (offshore outsourcing),26 often remains a strong temptation, based on cost savings efficiencies and forum shopping to avoid litigation, regulation and other incidents of public policy influence. Arguably, offshore outsourcing potentially threatens national economic and defense security, such as when as cloud data repositories and data processing are offshored to antagonistic or disloyal and opportunistic foreign nations. When critical infrastructures27 are outsourced offshore, such practices raise threat levels to national economic security.28

---

https://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=4311&context=wlulr

24 While comprehensive assessment of all nations’ approaches to cloud services is well beyond the scope of this white paper, the European Union’s (EU) proposed “Data Act” represents an
Cloud Competition & Security

COUNCIL, No. 2022/0047 (COD) (Feb. 23, 2022) https://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:52022PC0068 (emphasizing, among other matters, the maintenance of EU values, interoperability, incentivizing EU onshore cloud services providers, regulatory compliance, and associated cybersecurity regulation)

Some commentators argue that strong omnibus privacy rights will inhibit the growth of AI in those regions where privacy regulatory compliance costs remain high, see generally, Bagby, John W. and Houser, Kimberly, Artificial Intelligence: The Critical Infrastructures (September 15, 2021). Available at SSRN: https://ssrn.com/abstract=3924512 or http://dx.doi.org/10.2139/ssrn.3924512 (arguing an information supply chain approach to AI reveals a generalized AI architecture susceptible to optimize industrial policy intervention, both by deploying government support and the imposition of various regulatory tools).

25 See e.g., Andrea Ovans, What Is Strategy, Again? HARV. BUS. REV. (May 12, 2015) https://hbr.org/2015/05/what-is-strategy-again (analyzing history of strategy literature recognizing outsourcing as a major tool of cost containment). The outsourcing literature recognizes an oscillating pendulum that swings between (i) strategies to trim costs and acquire critical mass in expertise and functionality from outside experts and (ii) insourcing to develop proprietary and dedicated internal expertise and service capacity adequacy.


Cloud Computing Services Accumulate into Critical Infrastructure

Cloud computing is becoming a major component of critical infrastructure. Cloud computing is pervasive and broadly impactful precisely because the cloud links (almost) all other critical infrastructures. Status as a critical infrastructure implicates strategic decisions involving industrial policy-making to maintain economic resilience and national security.15 There may be no turning back on cloud computing as an essential architectural element in most Internet commerce, intra-organizational

recordkeeping, process control and transaction processing. Thus, arguably cloud computing should be monitored for various performance metrics given its essentiality in critical infrastructure. Direct regulation and indirect discipline, achieved through industrial organization aspects, appear as two major external pressures to discipline cloud service providers to achieve overriding critical infrastructure goals.

As with many activities driven largely by promised financial benefits analyzed using cost-benefit/analyses (C-B/A), some threats are understated in this form of evaluation. This makes robust and reasonable assessment require better integration of financial C-B/A with predictive threat analysis inherent in risk-benefit/analysis (R-B/A).16

Cloud Situs Implicates Jurisdiction Limitations

Incorporation domicile, as well as the situs of major operations, have always posed industrial organization problems. Enterprises strategically locate particular installations (data centers, headquarters, financial institutional service providers, manufacturing, warehouses) into friendly forums. This is one of the latest incarnations of the classic “competition in laxity,”17 otherwise known as the “race to the bottom”18 in search of leniency. In a globalized economy, this implicates forum shopping resulting in barriers to regulation, limits on litigation’s jurisdictional reach, greater opacity in corporate records and communications, and labor relations most favorable to employers.19 The storage and processing of transactions and communications can also be a major venue selection criterion.34 It is theorized that businesses resort to havens to avoid taxation, regulation, litigation and visibility that the transparency of localized operations invites.35 The comforts, liberties and cost savings of havens likely serve to attract cloud computing services to locate servers and associated hardware into data havens that erect barriers to foreign legal processes.36

CLOUD Act

The Clarifying Lawful Overseas Use of Data Act a/k/a the CLOUD Act evidences recognition that cloud computing is an essential service, particularly to the operation of

government, government’s enforcement of federal law and the reach of various levels of regulation. Offshoring cloud computing services reinvigorates the quest for a stateless Internet, another chapter in the controversy over shielding operations from foreign nations’ jurisdiction in investigations, discovery, forensics, regulatory enforcement and litigation, both civil and criminal. The CLOUD Act was initially introduced in 2018 as H.R. 4943 but was later bootstrapped into the Consolidated Appropriations Act of 2018 as Division V. The CLOUD Act amends the Stored Communications Act of 1986 component of the Electronic Communications Privacy Act (ECPA) to enable extraterritorial reach of federal warrants when the data is located abroad.

---

41 The CLOUD Act was passed in response to Microsoft v. U.S. In that case, the FBI issued a warrant during the investigation of criminal drug charges. The warrant described emails stored on Microsoft’s offshore servers located in Ireland. Near the end of the five years of litigation, Congress passed the CLOUD Act rendering the original

warrant moot after the Supreme Court vacated the Second Circuit’s invalidation of the warrant.\textsuperscript{21} Prior to the CLOUD Act, only a more onerous procedure was available for U.S. warrants to access data contained on foreign servers and only under bi-lateral and multilateral mutual Legal Assistance Treaties (mLATs).\textsuperscript{22}

In the following sections, this white paper explores prospects for how economic incentives impacts cloud computing services, how this results in (un)acceptable levels of data security, the roll of contracting resulting in ToS/EULAs defining enforceable service level commitments (SLC) for cloud computing services and the monitoring of the industrial organization of cloud computing services.

The Political Economy of Security

The public policy of security implicates an analysis using both law and economics as well as the political economy perspectives.\textsuperscript{23} Security may be ripe for regulation because of market failure in security investments. Cloud computing services is an essential part of this calculus. While nations have historically invested significantly in national security,\textsuperscript{24} private-sector investment in security is much less robust. Some businesses have clear and immediate security needs. Consider how banking provides at least two good examples connecting law and regulation to security investment. The first example illustrates that strong policy incentives lead to effective security investments while the second example illustrates the need for policy incentives because of market

\begin{itemize}
  \item \textsuperscript{21} In re Warrant To Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., 829 F. 3d 197, 204–205 (2\textsuperscript{nd} Cir. 2016) https://casetext.com/case/microsoft-corp-v-unitedstates-in-re-a-warrant-to-search-a-certain-endashmail-account-controlled-maintained-bymicrosoft-corp
  \item \textsuperscript{24} This investment is often beyond optimal levels. Some argue President Reagan’s military buildup during the 1980s, alleged by some at the time as excessive military buildup, forced the Soviet Union to “over-invest” in their national security, eventually causing the U.S.S.R.’s downfall. See generally, Schweizer, Peter, VICTORY: THE REAGAN ADMINISTRATION’S SECRET STRATEGY THAT HASTENED THE COLLAPSE OF THE SOVIET UNION (Atlantic Monthly Press, 1996).
\end{itemize}
failures to incentivize adequate security. These both analogize immediately to cloud computing services.\(^{25}\)

First, the physical safety of bank assets, currency, negotiable instruments and safety deposit contents is required under contemporary banking regulation.\(^{26}\) Cloud hardware, servers, server physical locations and interconnectivity both wireline and wireless transceivers share such physical location security vulnerabilities. Such security investments in tangible personal and real property were clearly signaled to the banking industry by market forces long before comprehensive state banking regulation or national banking regulation was initiated. From the Wild West days through the Gangster-era, banks responded to their vulnerability for theft by investing in physical and administrative security controls. The result was innovation and widespread deployment of strong security: vaults, security sensor monitoring, administrative process, employee/insider controls (e.g., NCR) moral hazard minimization techniques, secure asset transportation (e.g., Wells Fargo & Brinks as transporters) and tracking technologies for both assets like coin, precious metals and currency as well as the negotiable instruments or other mandatory documentation that directly affects many banking transactions. These control mechanisms were initially seen as costly but eventually became fairly effective because they were so effective in lowering risks and thereby attracted and retained loyal customers through loss minimization.

Second, contrast the bank’s progress on physical safety against the rather lax current security provided by modern financial institutions to their individual retail customers over some electronic assets and their customer’s PII. Under law, banks have custodial responsibility over account information and payment card processing. While the CardSystems Solutions failure in the modern era\(^{27}\) prompted development and widespread deployment of the more effective PCI standard,\(^{28}\) hacking incidents continue to rise, betraying market failure of customer pressure to increase security investment.\(^{29}\) Some argue commercial and investment banks invest significantly more on security in

\(^{25}\) Parts of the following are adapted to cloud computing services from John W. Bagby, *Security Law, Regulation and Public Policy for Accounting Professionals*, No. ALSB2018_098, Academy of Legal Studies in Business, Portland OR (Aug.11, 2018).


\(^{27}\) See, Electronic Payment Systems, LLC v. Cardsystems Solutions, Inc., 1:06-cv-00626, (D. Colo.). The June 2005 security breach at CardSystems Solutions impacted 40 million payment cards. Allegedly, data was regularly transmitted unencrypted, ostensibly to avoid the resultant system sluggishness of robust security measures, such as encrypting data in transit.

\(^{28}\) See PCI Data Security Standard v.4.0 (Mar.2022) https://docs.prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf

\(^{29}\) It can be argued that some customers fail to appreciate the risks of PII misuse so they fail to apply adequate pressure for additional security investment. Arguably, this is irrational behavior. When such individuals exist in sufficient numbers, this becomes widespread ignorance and contributes to market failure by sending erroneous signals.
Cloud Competition & Security

matters directly impacting their wholesale contractual duties to major, commercial business customers than for the more numerous, dispersed and uncoordinated individual retail customers.\(^{51}\) Attention to a few big customers may be stronger than to the frequent but uncoordinated market demand signals from individual retail customers. While regulation may not yet fully address these problems, similar market failures in other realms will arguably benefit from standardization and regulatory intervention.\(^{52}\) Economic incentives affecting the cloud seems to be no different in principle but given the cloud is often a constituent component of these financial information systems, it is part of the architecture potentially suffering from under-investment.\(^{53}\)

Market Failure for Security Investments

For many years there has been recognition that markets for security investment protection fail in several ways.\(^{54}\) Some of these problems are inherent in the increasingly complex security and information supply chains that include cloud elements while other problems are classic applications of recurring market failures. Of even greater concern is that when these conditions combine with other market failure(s), they become quite stubborn, even “wicked problems.”\(^{55}\) Such problems negatively impact social welfare even more profoundly suggesting regulatory mechanisms likely will be designed and deployed to correct market failure in this special application area of security investment. It would seem that the cloud could only evade such public policy pressures if it were eliminated from the information supply chain architecture; almost an absurd contention.

Difficulties of Complex, Layered Supply Chains

Online, wireless and electronic commerce relationships are layered markets; actually, they are becoming quite complex supply chains. “Low friction” market structures, the cloud is a contemporary example, initially attract innovation and new business startups because they appear less costly. However, it is often argued that eCommerce techniques often result in the “winner’s curse,” most notably a problem in

\(^{51}\) It seems axiomatic that larger wholesale customers are more lucrative enabling them to enjoy better treatment in many ways when compared with the large number of small, low stakes accounts of retail customers.


\(^{54}\) Why the Security Market has Not Worked Well, Ch.6 appearing in COMPUTERS AT RISK: SAFE COMPUTING IN THE INFORMATION AGE, System Security Study Committee; Computer Science and
Cloud Competition & Security

Technology Board; Commission on Physical Sciences, Mathematics, and Applications; National Research Council (1991) https://www.nap.edu/read/1581/chapter/8

Camillus, John C., Strategy as a Wicked Problem, 86 HARV. BUS. REV. 98 (Reprint No. R0805G, May 2008) https://hbr.org/2008/05/strategy-as-a-wicked-problem (arguing wicked problems are difficult to solve due to incomplete information, a plethora of participants with diverse opinions, large economic stakes, and interrelations between wicked problems and other thorny problems).

Transaction costs are “bid to zero” and overpayment systematically recurs, resulting from excessive optimism and asymmetric information. Furthermore, complex transaction architectures permit independence of specialized function, enable nimble adaptability, and reduce the costs of maintaining slack overcapacity. Increasingly, network science now provides insights into such complexity, such as the identification of incentives to “disintegrate” supply chains: disintermediation. Furthermore, the less socially beneficial side effects, such as inter-dependency risk, are only now becoming clear.

Ultimate consumers, are generally called “end-users” in eCommerce and social media (SM) circles. Users have little direct contact with the peripheral suppliers that deliver goods and services to the retail businesses, with whom such end-using consumers data and query handling are actually handled. Indirect suppliers instead negotiate key contract terms such as “service level commitments” (SLC) and security problems).


60 Consider the complexity of “eHavioral” behavioral advertising on cell and mobile devices and the subset of this activity called Wireless Advertising Messaging (WAM). See generally FTC STAFF REPORT - PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS, FTC (March 2012) https://www.ftc.gov/reports/protecting-consumerprivacy-era-rapid-change-recommendations-businesses-policymakers

The “architecture” of these networks varies but all must include at least the following, generally separate independent entities:

(i) user or ultimate consumer,
(ii) wireless TelCo – the communications service provider,
(iii) other ISPs &/or OSPs connecting all the various participants,
advertisers, advertising agency which develops the ad program, and cloud computing services including the data aggregator, which supplies PII used in targeting ads to the user based on algorithm-driven analytics.

In the future, such networks are likely to add additional participants: other service providers, additional aggregators from which data and PII is harvested by the primary aggregator, and cloud service providers which store data. See generally Xu, Heng, John W. Bagby & Terence R. Melonas, Regulating Privacy in Wireless Advertising Messaging: FIPP Compliance by Policy or by Design? LNCS PROCEEDINGS Vol. 5672, Privacy Enhancing Technologies (PETS), 9th Int’l Symposium, pp. 19-36 (2009) https://link.springer.com/chapter/10.1007/978-3-642-03168-7_2 protections directly with only the service retailer, which serves as a “hub” for the consumer product or service. Thus, suppliers of system software, outsourcing “software as a service” (SaaS), outsourced cloud storage services, payment services, advertising and analytics service providers, PII aggregator(s), Internet Service Providers (ISPs), online service providers (OSPs) are, at best, only weakly disciplined by ultimate users. Telecommunications Companies (TelCos) and a growing additional array of interconnection intermediaries are increasingly involved.

The increasing number of intermediate suppliers in eCommerce supply chains are less responsive to the demands of ultimate users. They generally fail to respond adequately to almost any other signal sent by every entity, except for their immediate counter-party in these complex systems. Indeed, suppliers are traditionally responsive primarily to their immediate counter-parties. Responsiveness to other parties is derivative, only if asserted by their immediate counter-party. While cloud computing services are likely to accommodate end-user demand as feasible, the communication of these preferences is through, and not around, the end-user’s immediate counter-party.

Therefore, isolating ultimate users from the complex array of intermediaries attenuates the impact of user/consumer complaints, demands or even their approval and adoration. Instead, as one or more layers of intermediaries are interposed, it becomes predictable that delay will result with the attendant mis/re-interpretation or disregard of signals. This attenuates market pressures that users exert, which could have incentivized the security investments most effectively. Participants in complex supply chains must clearly be responsive to the risk management needs of their most immediate counter-party. Market discipline is most useful among direct contracting counter-parties. However, this discipline is diluted as it becomes indirect, delayed, distorted or ignored for all other participants who are more remote.

Clearly, complex, layered supply chains may result in various market failures. First, complexity raises the quantity of information relevant and necessary to any party’s rational selection. This condition naturally produces information asymmetries. Second, complexity imposes externalities as under-informed participants become overwhelmed and are further burdened by ineffective signaling, a market mechanism failure. This leads to rising costs of transaction monitoring, including recordkeeping, audit and confirmation, further compromising vindication of adequate performance.
Cloud Competition & Security

Discipline to render full performance on contracts is generally based on specific, voluntarily assumed duties (SLC), general duties of care, and in special cases of trust, even duties of loyalty. These duties are diluted as the probability of discovering breach of contract decreases or forensic costs rise in monitoring, audit, investigation, litigation, arbitration, or other rights preparations and vindication methods (settlement negotiations). Thus, complex supply chains inherently impose barriers to rights vindication, particularly for most remote parties. EULA or other ToS also make users particularly vulnerable because these contracts nearly uniformly limit rights or remedies, make unconscionable choices of law and forum and/or first require the exhaustion of non-litigation remedies.

Third, a “bounded rationality” results as the foundational assumptions for the “invisible guiding hand” of the perfect competition model are relaxed. Many economic actors fail to act “rationally.” For effective market regulation in the real world, this presence of significant bounded rationality undermines many of the assumptions of rational market participation. Fourth, security may be argued as form of public goods that should be provided by some form of intervention precisely because public goods are non-rival and non-excludable, but necessary. Business correctly perceives that robust returns on private investment in public goods remain speculative, even unlikely. Therefore, public goods are generally under-produced by the private sector, precisely the current state with security investments and other critical infrastructures. However, even if security investment were to remain under-produced, perhaps intervention from attest and consulting engagements that address security matters could enhance security protections.

Information Asymmetries Undermine Security Investments

The complex, layered supply chain discussed here exacerbates a classic market failure meriting regulatory intervention: asymmetric information. When buyers or sellers lack sufficient information to make rational choice, this produces bad results, the “adverse selection” problem. Ultimate consumers cannot effectively guard their own security in a complex, layered supply chain. Information is needed to make rational choices about the reliability of security protections for products they neither understand nor have authority to select from alternative, competitive vendors. This isolates and weakens the influence of end-users. The interposition of monitoring and auditable conditions, through contract and/or incentivized by regulation, should improve

31 See generally Simon, Herbert, Bounded Rationality and Organizational Learning, 2 ORG. SCI. 125 (1991) accessible with subscription at: https://www.jstor.org/stable/2634943?seq=1
asymmetries in the market for security in a manner similar to its improvement in the
market for investment securities.

Of course, there are two mechanisms that could offset the market failure of
information asymmetries. Pressures on intermediaries could force security investment.
Also, in a competitive market, ultimate consumers could simply defect to other sellers
and select different intermediaries who would then supply the desired levels of higher
security. Alternatively, the user could simply choose to discontinue using the products
altogether. However, ultimate consumers infrequently have much choice in the
intermediary vendors that are part of these network systems. A form of vertical
integration results preventing selection or variety. Outsourcing is the province,
sometimes the dire need of information services suppliers and seldom is a choice given
to the ultimate end-users. However, even with the introduction of some choice, many
end-users remain incompetent or unwilling to investigate the choice of intermediaries in
a complex information supply chain.

It should be recognized that transparency is often a double-edged sword.
Visibility of security vulnerabilities to supply-chain intermediaries, as well as to ultimate
consumers, enables market discipline. For example, transparency enables pressure to
replace insecure products, unreliable outsource “partners” or supply chain participants
and to retain monitoring and attest services to verify quality and reliability of security.
This is generally a good thing for competition because it enables user choice, efficiency
and arguably incentivizes security investment.

However, there is downside risk to transparency. Transparency can also invite
attack when it serves to signal attackers with key details, thereby enabling more effective
exploitation. As security vulnerabilities become more widely known, this informs
competitors. Nevertheless, confidential sharing of vulnerability information, when
confined to participants in critical infrastructure networks, can balance these two
difficulties. Still, information sharing has its own set of challenges, raises antitrust
 collusion concerns such as price and term visibility and is vigorously criticized.

35 See generally Bagby, John W., Evolving Institutional Structure and Public Policy Environment
of Critical Infrastructures, 9 SPEAKER’S J. PA. POL’Y. 187 (Spring 2010)

Information shared among private sector entities, particularly among competitors, is
generally presumed collusive without the imposition of (often inefficient) safeguards, such as
the rules regulating trade associations [e.g., no pricing discussions]. Furthermore, governments
and private sector entities have natural aversion to information sharing because the risks of
Clearly, if information asymmetries are significant and any intermediary has considerable market power, the impact of these offsets is limited. Of course, there are some counter examples. Following the various AT&T antitrust settlements alleging integration under the unlawful tying theory, long distance service provider choice and telephone instrument vendor choice was permitted. Similarly, the deregulation of electric power has also unbundled transmission from electricity generation, permitting some limited choices in a few states regarding their electricity generator. Many users may select from competing providers of mobile device “apps,” although such choices are much more widely available on the open source platform Droid than on Apple’s iPhone or RIM’s Blackberry devices. There is little evidence that social networking, wireless advertising messaging or any of the other free (advertising-based) services now proliferating provide much choice to users for the selection of intermediaries servicing the service provider as “partners.”

Externalities and Free Riders Disincentivize Security Investment

Security is arguably a benefit regularly and extensively provided by only a few. However, security is often an externality shared by many participants in some markets or among participants in some networks. When any member of such a group invests in security and other members recognize that they may also benefit, this positive externality creates a disincentive to further security investment by these other beneficiaries. Those benefiting but not investing become “free riders” on the security investment of the more active investors.36

In some network threat situations, security may actually be most effectively supplied by fewer than all participants. Sometimes the dominant participant’s security investment induces free riding by others. Service providers and software vendors often occupy this dominant position. Law and regulation should probably focus security investment incentives on these (presumably) “least cost provider(s).”37 In many situations, this outcome is also most efficient because the dominant provider enjoys a business model enabling it to pass on these security investments as costs to its endusers.

---

However, without such an effective cost pass-through, security investment will remain sub-optimally low.

***

Private sector information in government hands is generally viewed by the private sector to be insecure or vulnerable to acquisition by rivals or unwelcome use by regulators. Consider the government in the sunshine laws that inspired the federal Freedom of Information Act (FOIA) and the many state open records laws. While FIOA exemptions for CIP information apply to Protected Critical Infrastructure Information (PCII), similar exceptions under state open records laws remain unclear and inconsistent. Similar difficulties in CIP information sharing exist under the Federal Advisory Committee Act and the sometimes parallel state open meeting laws.

***

Many libertarians argue that cooperation and information sharing between government and business too often fails to serve the public interest. Therefore, public policy barriers to information sharing are formidable, suggesting that the design of information sharing mechanisms will continue to challenge critical infrastructure protection (CIP) efforts, may suffer initial failures and may grow unstable as self-interest becomes widely perceived as overpowering the public interest.

By contrast, in other, strongly interdependent situations, a network may be only as secure as its weakest link. This presents a coordination problem whenever insecure behavior by (almost) any participant heightens the risk to all. Consider the example of a botnet, an illegal, coordinated, denial of service attack using malicious malware secretly installed on mostly unwilling (zombie) computers. Botnets exemplify this weakest link situation, a derivation of the “Tragedy of the Commons.” Under this problem, participants have the strongest incentive to expand their uses (or costless


insecure behavior) without constraint (security under-investment) until the commons (network) is exhausted (suffers some significant damage).\(^\text{41}\) Security investment incentive changes, perhaps achieved through regulation and confirmed by professional attest, may be most effective when made pervasive by targeting all participants. In the cloud component of the information supply chain architecture, the tragedy is insubstantial investment into the data repository commons.

Thus, if law is to be an effective incentive, it must recognize which situations involve a stable, dominant, least-cost provider to target incentives for security investment. Furthermore, the role of monitoring and attest in system design, outsourcing validation and audit of security deficiencies cannot be understated. In other situations, the incentives may need to target all users. In either case, incentives may need to harness the network effect to select the most efficient security incentive mechanism. Of course, experience with attacks showing the failure of dominant players vs. the failure of weak links also informs the design of regulatory programs that better incentivize security investment.

**Direct Costs, Uncertain Benefits Complicate Security Investments**

Regulatory approaches to strengthen security incentives must recognize who bears the costs and risks of security failure and the extent of their ability to remediate. Next, these regulatory approaches must be politically acceptable. Some losses from under-investment in security are clear, immediate, significant and increasingly likely, such as the penetration of national defense or a critical infrastructure system. For example, hacking the electric power grid or a major control system (that could open the dam gates) would probably be immediate and result in catastrophic failure or mass destruction.

By contrast, the benefits of many security investments are manifest as the uncertain avoidance of unquantifiable future loss. Indeed, some benefits from enhanced security include losses that are hypothetical and remote; some may seem trivial. For example, identity theft can result in impersonation, credit-worthiness damage, and/or individual financial losses. This is clearly an increasing problem that may result in quantifiable money damages. However, these direct and immediate damages occur and are adequately vindicated in only a fraction of the reported security breach cases.\(^\text{42}\)

http://www.softcomputing.net/jias/rosenfeld.pdf

\(^{42}\) See e.g., Jay P. Kesan & Carol M. Hayes, *Liability for Data Injuries*, 2019 U. ILL. L. REV. 295  
https://www.jstor.org/stable/27171170
Investments are most compelling when they result in payoffs that are immediate or near term, the investment returns are high probability and the benefits can be easily converted into substantial cash inflows or prevent cash outflows. As with many corporate investments, “bang for the buck” is the most convincing justification for investment decisions. This is the main problem that underlies what may be the strongest disincentive to security investment. Uncertain and less tangible, future benefits make for a less compelling argument for present investments. Many security investments are far less compelling because they result in an uncertain avoidance of unquantifiable future loss. When security investments are compared with productive investments in the entity’s core businesses—those promising high, near term, positive cash flow results—then many security investments pale. Thus, security investments frequently fail to be authorized because they are regularly crowded out by more promising investments promising positive returns for core activities that pay off in the near term. Financial projections prepared and attested by professionals unfamiliar with the political economy of security are less convincing to motivate security investment.

Intruder Incentives Frustrate Security Investment Optimization

Hackers, intruders and other sources of threatening risk often have at least three alternative and separately sufficient incentives to conduct their intrusions. First, and axiomatically, there is the prospect for a payoff, such as by some theft that can be monetized by “fencing” the plunder or in the receipt of direct compensation from another party coordinating the hack. However, this incentive only partially explains hacking incidents. While intrusions by skilled hackers can be economically “rational” with positive payoffs and low penalty risks, their success rate appears exceedingly low.

Second, in national security and international competition, there may be an ideological or nationalistic cause that drives hacking activity. Third, many hackers also exhibit the “Styx Effect” because they are not gainfully nor full-time employed and “enjoy” a bit “too much time on their hands.” Under the “Styx Effect,” hacking is intrinsically motivating even when independent of other incentives, and becomes a more powerful incentive with combined with either or both the pecuniary and ideological incentive. This phenomenon is exacerbated with a near unlimited and growing supply of intruders and targets, the impact of Moore’s Law on direct hacking costs and the speed of interconnectivity.

Information Supply Chain Analysis Informs Security and Privacy Policymaking

A model of the basic structure of data management activities directly illustrates how and where privacy and security regulations can be focused.\textsuperscript{76} The privacy balance is reconciled with restrictions placed at several major choke points along the sequence of events typical to the data management process. Most of these regulatory approaches are ex ante security \textit{preventive}, they seek to deter intrusions. Thereafter, when prevention fails, damage suits are ex post \textit{curative} solution for past, unprevented privacy violations. Ex post rights vindication signals disincentives to under-invest in security.

No security or privacy regulation could long be effective without a clear technical perception of data management practices. New techniques could be developed to circumvent weak restrictions. Security and privacy regulation can encourage or limit particular activities at each or at multiple stages during data management. This is a supply chain focus for regulation of security and privacy to best model unique data flow regimes. Three basic steps generally comprise the data management of PII:

(1) collection,

(2) analysis, and

(3) use(s)

These steps can be further broken down into additional discrete segments as they are developed by the data industry. Consider the flow and processing of PII in Figure I.

\textbf{Figure I:}
Data Acquisition

Data collection, or data acquisition, is the first step in the information supply chain. This is the observation or sensing of some activity, usually followed by collecting and coding into an organized data storage. In network environments, much observed information is captured as it flows through telecommunications wires, along the airwaves, within networks or at particular servers or websites. Information capture generally refers to the interception and storage of data during its creation, entry, discovery, detection or transmission by an interception device installed somewhere, perhaps even at several points en route. For example, in traditional commerce, information is directly observed and captured as transactions are recorded on paper, at points of sale (PoS) or otherwise in computers. Vendors and delivery services must make reports of consumer purchases; loan payments or defaults must be recorded by lenders; an insured’s careful or risky acts are highly relevant data routinely gathered by insurers for underwriting; and employers must record and analyze employee activities as they accomplish job-related goals, productivity is metered or employees engage in misconduct. In the online world, websites are visited, links are clicked, queries are answered with data, cookie data is made available to servers from user’s devices as electronic probes read data files, and numerous other types of activities become more readily observable. This online data is captured when electronic records are made. Metadata provides forensic data about data useful as evidence in numerous situations.44


45 National security law limits the access to classified information and employment or outsource contracts may restrict access or transfer onward of particularized information.

Unless specifically constrained,45 the right to learn protects our direct perception and experience. This right generally permits us to observe, record and remember most
information. Although not expressly stated in the U.S. Constitution, the right to learn is the most direct inference from First Amendment rights of speech, press and association. While speakers generally enforce their own self-expression rights, these rights are not primarily for self-actualization. The First Amendment encourages the distribution and cognition of ideas needed for robust functioning of a democracy and a robust economy. Hence, learning is the intended result of First Amendment freedoms because it informs social, political, economic and ideological to serve democratic objectives. Furthermore, learning is more than a right, in many instances, learning is a duty from the obligation to attend school to various regulatory duties to collect, analyze, disclose and act upon business-related information. The right to learn is clearly critical to our growth and development because learning underlies nearly all progress.

From this perspective, privacy regulation intercedes only as an exception to learning when the balance favors individual privacy, commercial confidentiality or national security. Some privacy laws prohibit even the observation or recording of some data. For example, (i) a common law privacy right restricts outsider intrusion upon the seclusion of others, (ii) criminal and tortuous trespass laws forbid entry into the sanctity of another’s property, (iii) it is generally illegal for voyeurs or peeping Toms to use surreptitious means to visually observe others, (iv) some forms of employer monitoring are restricted, (v) wiretap laws prohibit listening to landline or wireless telephone transmissions, (vi) state laws prohibit cameras in restrooms or locker rooms, and (vii) it is generally illegal to intercept computerized telecommunications (e.g., e-mail, file attachments).

In the future, further prohibitions on direct observation seem likely. These may include restrictions on the monitoring of children’s activities, unauthorized decryption, prohibitions on taking human tissue samples for genetic testing and the unauthorized interception of financial transactions. In all these activities, public policy views the collection of this data as unduly intrusive when it violates intimacy, solitude and modesty or gives the observer an unfair advantage over the subject individual.

Information Analysis

The second step in the information supply chain is the organization and analysis of the data to create knowledge useful for some purpose(s). Before computerized telecommunications and storage, most data were transcribed by hand into paper databases. For example, the primary function of double-entry accounting systems is to create a reliable discipline for hand-written bookkeeping entries. The use of simultaneous debit and credit entries permitted systematic organization of accounting records. This reduced errors, permitted correct classification of items and allowed reconciliation – the subsequent inspection for quality control purposes. Similarly,

46 The right to learn is also a catchphrase for the claim of constitutional basis for positive reforms to free public education, see e.g., Darling-Hammond, Linda, THE RIGHT TO LEARN: A BLUEPRINT FOR CREATING SCHOOLS THAT WORK, (1997 Jossey-Bass, Inc. San Francisco).
analysis of PII should also follow systematic handling and pragmatic evaluation before valid conclusions should be drawn or decisive action taken thereon.

As data collection and organization has become mechanized, these activities are termed data warehousing. The impromptu analysis of this data in real time is often called data mining. This recognizes that innovative methods of analysis of huge databases can reveal important and useful relationships. Not all firms are capable of effective information analysis. Often the PII captured is disclosed to third party firms that specialize in gathering PII from several sources to provide analysis for clients. The verb aggregate (suffix pronounced: -gate) is often used to describe the process of combining PII about one or more individuals from multiple sources. An aggregator is a database manager, cloud service provider or data broker who usually combines partial bits of PII data about identified individuals from multiple sources. When collected and properly organized, these data can accumulate to a profile or dossier about that subject individual that is useful in making marketing, insurance, credit and employment decisions.

It is important to contrast this activity with the adjective form of the same word: aggregate (suffix pronounced: -git). When used to describe databases composed of PII about many individuals, the term “aggregate data” generally means that personal identifiers are not captured or provided to clients, they are stripped away, deleted or otherwise anonymized. This step helps to obscure the linking of PII to subject individuals from aggregate data.\(^\text{47}\) To illustrate the difference between aggregate (adj.) and aggregate (v.) consider the following example of traffic counts. Vehicle traffic can be counted using detector loops imbedded in the pavement without identifying drivers or their license plates. This “aggregate (-git, adj.) data” of traffic volume is used to know accurate traffic volume to plan for new traffic signals or to maintain highways. By contrast, this highway planning could also be based on data from highway video cameras which could identify each car’s license plate, as is done now at an increasing number of unmanned toll plazas. Thereby, an aggregator could combine this with PII data from wireless calls and credit card purchases made en route to profile the continuing whereabouts of each subject individual caught traveling on that highway.\(^\text{48}\)

Data analysts often “drill down” into large accumulations of “big data”\(^\text{49}\) to draw conclusions that are useful to their own decision-making or useful when further


\(^{48}\) See generally, John W. Bagby, Big Data and Intelligent Transportation Systems, LEGAL AND ETHICAL ISSUES IN PREDICTIVE DATA ANALYTICS, Indiana University, April 16, 2015.

disclosed to their clients. Key to these efforts is the evolving methods of data organization, structuring, filtering, aggregation, association and analysis. Nearly all conclusions are based on theories and conjecture or on generalizations from empirical testing. Clustering and association are among the analysis techniques.

Big data analysis is mostly not a true scientific method of inquiry. Why? Some forms of analysis are based on faulty assumptions, erroneous calculations or premature generalizations (e.g., junk science). For example, law enforcement is generally prohibited from interpreting lie detector evidence to disprove an alibi. In the future, other restrictions can be expected to prohibit the use of some data analysis methods. For example, employers and health care providers may be prohibited from using genetic testing of human tissue samples to infer predisposition to disease or criminal activities. Health insurers and employers resist extending coverage to individuals if they or their families have the potential to require high-cost medical treatment. Employers might try to avoid hiring persons or fire them if genetic propensity to disease or dishonesty is discovered. Privacy advocates believe that genetic testing should not be used in these ways until there is very strong and reliable scientific consensus connecting particular genetic markers with these undesirable predispositions. Big data used for healthcare underwriting or the determination of premiums, is apparently notwithstanding. Methods used in big data analytics increasingly depend on machine learning (ML), a component of AI in which algorithms are constantly updated and revised to vary the search, extraction, sensitivity and selection of relevant data.

Use of Knowledge

Data is collected and analyzed to give it value. This value is realized as the knowledge is used, largely in decision-making. This is the third stage in the information supply chain. Without the promise of some economic gain when resources are expended to collect data, analyze information and produce knowledge, then only intellectual curiosity would motive such activities. High quality information is presumed in economic theory, but it is only common sense that valuable and accurate knowledge is too often a scarce commodity. Most people have personal experience with an underinformed transaction confirming this. Data is collected and information produced for direct use by the data manager or for secondary use when sold to clients, “shared” with “partner” firms, bartered in return for other information or otherwise transferred onward.

This regulatory focus on the third stage of data management serves at least two important purposes. First, by prohibiting particular uses of information, use restriction

---


51 This can be simply stated as fact or it can be an ideological attack for those who insist they only do “real science.” Academics longing for acceptance into the community of (scientific) scholars are particularly vulnerable to anti-big data elitism inspired by the scientific method of falsification.
policies recognize that collection and analysis of PII is often inevitable and rightful. The greatest injury to the subject individual comes with use of PII. The incentive to improve decision-making with information is so strong that some firms inevitably learn PII despite restrictions on collection and analysis. Use restrictions are nearly the last resort because they are intended to prevent privacy intrusions from actually causing injury to the subject individual. A second reason to focus on use restrictions is that data management is similar to other industries. When information moves from acquisition, through analysis, to ultimate use(s) these activities are actually a chain of distribution. It illustrates that there is value in information; there is value added by intermediate services (e.g., compilation, selection, customization, interpretation) and there are markets for knowledge that is useful to information consumers.

However, if the “handlers” of PII are regulated under privacy law, this focus shifts from a supply chain to a chain of custody. Custody recognizes that subject individuals have rights in their own information and that privacy regulation constrains the activities of these PII handlers during the three basic stages of collection, analysis or use. This also implies that firms involved in data management have general custodial duties of reasonable care, security, safeguarding and sometimes even more specific statutory duties. A chain of custody approach suggests that privacy regulation could restrict the transfer, transmission, communication or receipt of PII. A focus on information handling recognizes the vulnerability of flowing data and reinforces the handler’s responsibilities to the subject individual regarding security. It could also be used to more directly control intermediaries and purchasers.

Privacy rights cast as use restrictions are also quite common. Consider some of the following examples: (1) underwriters for automobile insurance are sometimes prohibited from considering moving violations after the passage of some years; (2) potential creditors are forbidden from considering an individual’s former bankruptcy in making credit decisions after several years pass; (3) financial and health care privacy rules require the subject individual’s consent before the release or sale of protected healthcare information (PHI); and (4) law enforcement is generally prohibited from using a confession to prove guilt without Miranda warnings.

Standards Channel Security Guidance

Four methods of developing security duties predominate under current public policy. First, statutes, and regulations promulgated thereunder, can require safeguarding intangible information as well as the supporting tangible property deployed as integral architectural elements of cloud computing services. These provisions are particularly

52 There are substantial accumulations of international, federal and state laws and regulations applicable to information security, a catalog of which is beyond the scope of this work, see generally, Eric A. Fischer, Federal Laws Relating to Cybersecurity: Overview of Major Issues,
important given they enable end-users to comply with legal duties when using cloud computing services. Second, the courts and regulators can interpret these statutes, or develop common law doctrine that requires responsibility over security involved in the design, installation, operation and auditing of security systems involving cloud computing services.\textsuperscript{53} Third, contracts up-stream, down-stream or cross-stream can require immediate counter-parties, sometimes even remote counter-parties, throughout the information supply chain to pursue various security safeguards of data gathered by, residing in or supplied by cloud service providers.\textsuperscript{54} Fourth, standards occupy a middle

These provisions are generally referred to as cybersecurity regulations. Some federal laws are applicable primarily to operations and information repositories of the federal government and its agencies, see \textit{e.g.}, Federal Information Security Modernization Act of 2014, Pub.L.113-283 (Dec.18, 2014), Federal Privacy Act and Freedom of Information Act (FOIA) 5 U.S.C. §552. Other cybersecurity rules are part of sectoral regulatory programs applicable to industry sectors falling under each agency’s regulatory jurisdiction. These provisions impact cybersecurity duties for particular lines of business or business sectors outside government. For example, the security of PHI is regulated under the Health Insurance Portability and Accountability Act (HIPAA) security rule, \textit{HIPAA privacy, security, administrative data standards, and national identifiers}, 42 C.F.R. §403.812 \url{https://www.ecfr.gov/current/title-42/chapter-IV/subchapter-A/part403/subpart-H/section-403.812} Similarly, financial information security is required under the Gramm-Leach-Bliley (GLB) Act, 15 U.S.C. §§6801 - 6827, \url{https://www.law.cornell.edu/uscode/text/15/6801}

State privacy laws proliferate; six states have comprehensive privacy laws and dozens of other states regularly consider privacy law proposals. State legislatures now appear to shun the tradition of “uniformization” that deploys model acts or uniform laws. Instead, each state has taken a sui generis approach. Ununiform state privacy laws threaten inconsistency and complexity in security compliance. The six comprehensive states are California, Colorado, Connecticut, Iowa, Virginia and Utah. Proposals for federal pre-emption of such state laws are hotly debated. \textit{See e.g.}, Hayley Tsukayama, \textit{Federal Preemption of State Privacy Law Hurts Everyone}, \textit{Electronic Frontier Federation} (July 28, 2022) \url{https://www.eff.org/deeplinks/2022/07/federal-preemption-state-privacy-law-hurts-everyone} Generally, state privacy laws have provisions that expressly or impliedly impose information security duties on information repositories within their jurisdiction. Furthermore, many state legislatures are quite active in proposing, debating and otherwise considering privacy laws with cybersecurity provisions likely applicable to cloud computing


\textsuperscript{54} \textit{See generally}, Kimberly A. Houser & John W. Bagby, \textit{The Data Trust Solution to Data Sharing Problems}, 25 \textit{VANDERBILT J.ENTERTAIN. & TECH.L.} 113, 153-167 (2023) \url{https://scholarship.law.vanderbilt.edu/jetlaw/vol25/iss1/3} (developing the X-stream approach to classify the “bundles of contracts” with suppliers, customers and various service providers (such as cloud computing services) citing Ronald Coase, \textit{The Nature of the Firm}, 4 \textit{ECONOMICA} 386, 391–93 (1937)).
services. See generally, Data Privacy Laws by State: Comparison Charts, BLOOMBERG LAW (May 1, 2023)
https://pro.bloomberglaw.com/brief/data-privacy-laws-in-the-u-s/ In addition, there are substantial sources of formal and informal guidance from various federal and state agencies, opinions of attorneys general and legislative histories implicating some further detail concerning cybersecurity duties.

ground in which government actors play a less intrusive role in developing security regimes.

This section discusses how standards often underlie all methods of security duty formation. Standards can require safeguards and monitoring responses that reduce security threats as well as responses that remediate intrusions. In the first subsection, the nature of (security) standards is examined. This includes the aspirational, Fair Information Practice Principles (FIPP), which are vague standards that arguably underlie most privacy laws by including security safeguards. The third subsection illustrates how the traditional focus on internal control underlies financial information security. Later subsections discuss specific audit standards as well as more general (international) standards potentially applicable to all cloud security activities and constituencies.

The (Security) Standardization Taxonomy

Security standards follow a well-trod pattern established in professional, behavioral, technological and interoperability realms. Standards originate from various sources but are developed in three primary ways. First, de facto standards arise when a proprietary technology achieves broad market success. Second, de jure standards are generally imposed by judicial opinion, legislation or are developed and deployed by government regulatory agencies that are delegated authority to exercise their domain expertise. Third, voluntary consensus standards (VCS) arise increasingly in private-
standards through competitive success of their products. There are democratic process problems with proprietary and de facto standards because they lack political checks and balances before they are imposed ex ante. Furthermore, some de facto standards are also closed standards because they are neither transparent nor fully accessible permitting the owner to discriminate against users. As with other dominant standards, de facto standards generally impose high switching costs thus locking users into the standard and retarding future innovation. See generally, Bagby, John W., *Role of Standardization in Technology Development, Transfer, Diffusion and Management*, THE HANDBOOK OF TECHNOLOGY MANAGEMENT, Vol. 3, Hossein Bidgoli, ed. (2010, John Wiley & Sons, Hoboken, N.J).

sector venues known as standards development organizations (SDO). For example, accounting standards are developed and deployed by professional bodies with domain expertise in financial accounting practices. When these VCS standardization efforts are more limited, such as when they arise ad hoc and the SDO disbands when completed, they are generally called consortia. De jure standards generally constrain everyone while de facto, consortia, and VCS standards are voluntary for those who choose to participate. Audit professionals impliedly choose participation because they are intentionally certified and licensed or choose to supply consulting engagements that require their certification.

De jure standards are considered formal standards because they are created by law in legislation, regulations, or are set in tribunals such as by court precedents. These are principled standards imposing mandatory requirements with the force of command and are created by a legitimate authority. Typical examples include environmental and safety regulations as well as most standards of professional conduct. Professional standards are mostly behavioral, not technical. Professional standards are also formal standards when set by professional societies like that done in the accounting, legal or real estate professions. Furthermore, when government officially recognizes or adopts professional standards set by accredited nongovernmental bodies, these professional standards eventually become de jure standards. For example, building codes become governmental de jure when adopted by states or municipalities. Accounting and audit standards set by professional societies can be adopted by governmental bodies such as the SEC, the Federal Reserve or PCAOB. Government de jure standards are more appropriate if an enabling legislation requires regulatory decisions not solely influenced by direct pressure from the industry regulated.

57 Under rules of the U.S. Office of Management and Budget (OMB), regulatory agencies must exercise standards-setting judgment independent of regulated entities where the regulator must determine “the level of acceptable risk; setting the level of protection; and balancing risk, cost, and availability of technology in establishing regulatory standards.” See generally, Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities, OMB Circular A-119 https://www.gpo.gov/fdsys/pkg/FR-2016-0127/pdf/2016-01606.pdf A-119 policies were largely codified in National Technology Transfer
standardization processes into a hybrid form combining both de jure and de facto characteristics. Increasingly, VCS process rules include at least a minimum of political participation checks and balances. These are required in the U.S. and in some international standardization venues, such as the ISO. However, VCS rules face the practical problem of attracting major players into standardization. Excessively tough VCS rules might deter the major players who must intimately participate in standardization as a design process particularly if they share their expertise to assure success for the standardization effort, see generally, Weiss, Martin & Carl Cargill, Consortia In The Standards Development Process, 43 J.AM.SOC.INFO.SCI. 559–65 (1992) https://doi.org/10.1002/(SICI)1097-4571(199209)43:8<559::AID-ASI7>3.0.CO;2-P

Understanding security standards applicable to cloud computing services benefits from a standardization life cycle approach. This method of analysis is appropriate to analyze markets; particular products and services; the development of complex systems, processes and software; and many data matters. The insights derived from life cycle analysis permit holistic system assessment to avoid omissions, identify critical path efficiencies, monitor performances at each phase, assure functionality of all links connecting phases, and to optimize the SDA’s impact. This is particularly important because most all SDA share common sequences as applied to most fields of endeavor.58

The standardization life cycle approach to security standards proceeds to first identify a need for security standards. Legislative findings and judicial opinions sometimes provide a description of such an impetus. In the second stage, participants are attracted to the SDA which defines the scope of the standardization activity. For example, the National Institute of Standards and Technology (NIST) identifies that regulatory agencies and information science professionals can be critical participants in the design, installation, testing and remediation of security systems. Such recognition often prompts NIST, consultants and academia to conduct studies, establish task forces and working groups, then follow democratic policy development procedures to issue drafts and eventually adopt final standards. In these proceedings, experts develop regimes, political and advocacy activities test and refine the proposals and choices are ultimately made by consensus.

Alternatively, standardization economics suggests that first mover leadership might lead a whole industry to pursue one or more of the forms discussed above: de jure, de facto, consortia, and/or voluntary consensus. In contested standards areas, several venues might compete for the standardization activity. In extreme cases,

---

standards wars may be waged, a mild form continues today in the security standards arena.

In the third phase of the standardization life cycle, the actual standard develops. This is essentially a design exercise through a complex interplay among three forces: design, sense-making, and negotiation. Design, sense-making and negotiation, the DSN model, recognizes the complex and different roles played by various standards developers, such as: advocate, architect, bystander, critic, facilitator, guru, or procrastinator. During the SDO's development process, the participants engage in: setting the project scope, composing and making proposals and counter-proposals constituting an anticipatory design, analysis of draft standard impacts (sense-making), negotiating revisions, coalition building to attain consensus and final approval through various democratic processes (e.g., voting).

In the fourth phase, the standard is “reported out” and published, urging adoption either implicitly or explicitly. Professional standards, like security standards are now developing, are generally reported out as drafts initially and, when revised and adopted, they become binding regulation. During the fifth phase of technical standards, compliant products and processes are developed and produced; markets then arise for these products and processes.

Professional standards similarly create markets for professional services. Indeed, a critical part of the standardization life cycle is conformity assessment. Much of security standardization will ultimately mandate processes of conformity assessment, essentially an assurance process that can result in certification, monitoring, metrology and/or accreditation. Finally, as technology advances, the standard is reconsidered by evolving markets, SDOs, court cases addressing failure of standards or conformity assessment, or the review by regulatory response to pressures to consider or adopt or replace existing standards with alternative competitive designs. This reconsideration can force the revision or abandonment of incumbent standards as society's needs change, technology develops and markets force the eventual decline of mature processes compliant with the prior standard in question, perhaps even the development of superior substitutes.

59 See generally, McNichol, Tom. AC/DC: THE SAVAGE TALE OF THE FIRST STANDARDS WAR (John Wiley & Sons, 2011) and Shapiro, Carl, and Hal R. Varian, The Art Of Standards Wars 41 CAL.MGT.REV. 8-32 (1999) http://people.ischool.berkeley.edu/~hal/Papers/1999_CMW_Standards_Wars.pdf In the field of developing financial information security standards, there were several internal control environments that were initially competing to become the definitive standards, COSO (Treadway Commission), # Firms, CoBIT, NIST, ISO 27,000 series, FTC Security Standards, etc.

60 See generally, Mitra, Presenjit, Sandeep Puro, John W. Bagby, Karthik Umapathy & Sharoda Paul, An Empirical Analysis Of Development Processes For Anticipatory Standards (Oct. 2005) : http://www.netinst.org/Mitra.pdf and available at SSRN: https://ssrn.com/abstract=2115235 (interpreting empirical results of ICT standards design exercise in which technical specifications were developed to serve as rules, guidelines, or definitions of characteristics that ensure
Characteristics of (Security) Standards

The compliance tolerance of security standards is an important first characteristic. Compliance tolerance identifies the autonomy, specificity, and precision required. The permitted variance of a standard requires development of some measure(s) of the tolerances found in compliant systems. Tolerances are variations within certain limits and the determination of instances that fall outside these allowable limits. This characteristic of standards is measured by both functionality and by conformity assessment. Consider how some standards permit a wider tolerance for compliance than do other standards.⁶¹

The accounting profession is a useful example because many accounting and audit standards directly involve financial information security. Financial reporting standards have long recognized at least some variance in compliance tolerance, by establishing a three-part taxonomy. Some standards are intentionally vague, drafted more like general guidance, so they can still be successful if the system would not suffer immediate, obvious or catastrophic failure with minor noncompliance. Indeed, in some domains, the standards tolerate predictable variation in expected activities such as where strong public policy pressures force such standards to encourage innovation by allowing wider acceptable variations to encourage more effective or efficient compliance. Management process and financial disclosure standards are classic examples of standards satisfied by wide tolerance ranges.

⁶¹ Consider this electrical compatibility example. There are a nearly infinite variety of designs possible for consumer electrical devices. These devices in Japan and most of the Western Hemisphere work well within the 10 volt range of 110 volts to 120 volts. Some devices continue working above or below this range. For example, incandescent bulbs simply brighten or dim. These are more flexible standards because they have wider boundaries that envision a more forgiving range of variance. By contrast, some other electrical devices become inoperable or are damaged when supply voltages are outside the allowable range (e.g., florescent bulbs) illustrating that some standards require product compliance within a much narrower tolerance range. ¹⁰⁰ See e.g., Ng, Mike, The Future of Standards Setting, 7 C.P.A.J. 18–20 (Jan.2004), http://archives.cpajournal.com/2004/104/perspectives/nv9.htm.
Three broad categories of compliance variance exist in financial reporting: rules-based, principles-based and principles-only. Rules-based standards are the strictest in this spectrum of compliance variance - often expressed in precise language so they permit less flexibility. On the other end of this spectrum are principles-only standards for which compliance is arguably easiest because they are vaguely expressed. A middleground approach, known as principles-based standards, are behavioral standards that depend heavily on professional judgment. Thus, rules-based standards generally require more costly and stricter compliance. When principles-only standards are used, they provide much less structure and encourage easy compliance or can be more readily adapted to very different lines of business and business models. Finally, when principles-based standards are required, there is a stronger focus on the exercise of professional judgment, thus suggesting stronger regulation of such professionals. These broad classifications are adaptable in many other fields, such as information security and cloud computing services.

A second characteristic for standards is how they are distinguished by the thing or object of standardization. There will likely arise security standards that focus on various objects of standardization. Behavioral, managerial process and professional standards address human activity directly. Security professionalism and security audits are likely to focus on these matters.

By contrast, technical and interoperability standards focus on nonhuman, nonbehavioral characteristics. Again, other security standards likely focus on technical matters, particularly where software and hardware are unforgiving to particular electrical characteristics, electronic schematics or the numerical values in sensor readings. Technical standards are common in the natural sciences and engineering, so most environmental emissions standards, metrics of measurement, or electrical properties, are technical because they prescribe designs or clearly quantifiable performance measurable by physical, scientific methods. The narrowest approach to technical standards requires a focus solely on the physical properties of tangible objects. However, modern technical standards generally require repeated use of rules, conditions, guidelines, or characteristics for products as well as their related management processes, production methods and conformity assessment. Thus, technical standards increasingly include various supporting related management system practices because technical standards increasingly define terms, they classify components, they describe procedures, they specify dimensions, materials, performance, designs, or operations, they measure quality and quantity of materials, processes, products, systems, services, or practices, they require particular test methods or sampling procedures, and they describe the fit and measurements of materials size, resilience or strength.

Technical security design and operations standards are only part of security duties. Security management standards are needed to guide security personnel to
maintain achievement of those technical specifications. These latter are more managerial in character. Thus, distinguishing between behavioral/managerial/professional and technical standards provides key insight into the range of contemporary standards.\textsuperscript{101}

In the future, it will become increasingly difficult to distinguish adequately between purely technical standards and purely behavioral/managerial/professional standards. U.S. Office of Management and Budget (OMB) defines technical standards to include “ancillary human and management processes.” However, this was OMB’s attempt to exclude professional codes of conduct; in hindsight it simply confuses any clear standardization taxonomy. Consider how educational standards for admission, performance evaluation, graduation, and certification are frequently described as technical standards even though they are clearly behavioral, managerial and professionally related. Similar difficulties exist for cybersecurity standards because they merge both IT technical standards with behavioral, management, and professional standards of cybersecurity professionals who operate computer networks.\textsuperscript{62} Furthermore, conformity assessment combines technical standards with the behavioral and professional standards needed to practice technical standards and the metrology needed to determine conformity. For example, cybersecurity standards specify that IT staffs must meet educational achievement, pass professional examinations, and meet other personnel certification requirements.

Another common characteristic of standards is the focus on intended user groups and on the purpose of the standard. U.S.’s NIST seeks to classify standards by intended user group and the standard’s purpose. Intended user groups are likely narrow groups who must directly modify their behavior to comply with the standard or who are most directly impacted by the standard. These parties have the strongest incentive to understand the technical aspects of a standard because they must fully comply in order to supply quality products and services into those markets. These most intimate


Revision history of OMB Circular No. A-119 is typical to most documents attributable to prior presidential administrations. However, sometimes archival records are purged by later administrations, arguably to start with a clean slate. Nevertheless, certain government documents are essentially non-purgable residing in collections protected by archiving requirements such as the Federal Register and in privately accessible former administration collections such as archives of former White House records and in presidential libraries https://obamawhitehouse.archives.gov/omb/circulars_a119_a119fr

intended users generally exert some control over how the activity standardized produces side effects that will impact outsiders, both positive and negative externalities. User groups of security standards include auditors, IT professionals shareholders and bondholders, management, and subject individuals of the data secured by cloud computing systems (e.g., customers, suppliers, employees, targets of advertisements).

This NIST taxonomy of intended user groups includes only those most directly impacted by standards: firms, industries, nations, provincial/local governments, and international organizations that develop and implement the standard. The narrowness of this conception of user groups contrasts significantly with the affected parties given status to participate in standards rulemaking under U.S. regulatory process. Other affected parties impacted by de jure standards may participate more fully than they would in SDA undertaken in consortia or VCS bodies. Consider some common forms of standards classified by intended user group: company (in-house) standards, developed internally by a single industrial firm and meant for internal and affiliate uses; harmonized standards - either an attempt by a nation to become compatible with international or regional standards, or under bi-lateral international agreement; and industry standards developed by an industry for materials and products related to that industry. Standards informally developed or which guide the professional activities of security personnel may constitute de facto, security standards.

As to intended purposes, the NIST classification scheme is also initially instructive. A basic standard has broad-ranging effects in a particular field, such as a standard for security that many follow in securing telecommunications, cloud computing or the computer systems upon which cloud services are reliant. Standardized nomenclature or terminology standards enable commerce by providing clear contract language. Test and measurement standards define conformity assessment methods that evaluate performance or characteristics of products or processes. Product standards specify qualities or requirements to assure they serve their intended purposes. Process standards specify method steps like a production line’s functions or operations. Service standards address maintenance or repair. Interface standards define connections (e.g., telephone, computer network, wireless) and focus largely on accurate compatibility. Data standards include characteristics for which values or other forthcoming data will specify a product, process, or service such that their order and arrangement will not be misunderstood.

Another standards classification approach focuses on the object standardized and relates the standard to the object’s phase in the object’s own product life cycle. This may be described as the design or performance standards dichotomy. NIST describes this as “the manner in which [standards] specify requirements,” the classic ends vs. means approach. Design standards prescribe characteristics of the product’s components, construction or manufacture. For example, software that encrypts data by default follows an encryption design standard. By contrast, performance standards
describe a product’s function irrespective of the particular design used. Firewalls that limit intrusions that are evident from system logs or other journal entries can be evaluated using performance standards. Design standards presume a well-defined overall design provides adequate performance when using well-understood arrangements of familiar processes, personnel and components (means). Contrast this with performance standards because they are more flexible, permitting various designs so long as they achieve acceptable results (ends). So even if alternative or novel designs are deployed, compliance with a performance standard may be established. Thus, a design, means-based standard presumes adequacy of particular specified designs. By contrast, an ends-based standard sets performance adequacy and determines compliance later, during conformity assessment. Security standards implement both these approaches. System designs with proven characteristics are audited for conformity assessment while incident logs are inputs to assess performance of security systems through conformity assessment. Performance standards are results-oriented but may not achieve network effects where these are possible through specified designs. Design standards enshrine particular designs by raising switching costs and make alternative innovations more difficult to pursue.

Internal Control: the Essential Component to Information Security

Pressures for internal control emanate from myriad sources: some are market based, some are fiduciary based and some are sourced from various constituents but focused largely through public policy implementation, particularly de jure standards. While the first two drivers are critically important, they are discussed here largely as they relate to the third driver of public policy. The primary focus here is on how public policy drivers are executed, the strength of their influence and the likely responses in implementation of the controls required. There is an increasing recognition of pervasive vulnerability in tangible and intangible assets. This vulnerability is often focused through IT as a means of processing transactions, maintaining records, exercising financial stewardship and otherwise generally safeguarding the security of these assets and the PII of subject individuals, whether or not the latter are end-users.

Internal control systems are the key security methods for tangible and information assets. Controls assist to optimize decision-making and process effectiveness because they improve the accuracy and reliability of information. Controls also have other objectives external to the entities deploying them. This analysis recognizes the potential for some confusion in the various public policy regimes of control design, implementation, maintenance and evaluation.

The public policy imperatives for internal control have varying objectives as well as varying origins from a wide range of policy makers. First, professional standards are generally established by non-governmental organizations (NGO), self-regulatory organizations (SRO) and other professional societies, many of which remain not-for-profit. These benefit society generally or the professions more specifically as they improve the quality of professional services. Second, financial reporting and corporate
governance standards are required by statute and regulation and these are often based on professional standards and practice. These benefit society by improving the integrity of the capital markets and expand the economy as the financing of business and government becomes reliably available. Third, privacy laws and policies require security, information assurance and the component internal control environments. These internal controls are therefore required by contracts and statutes, although they are often implemented by agency regulations. They benefit subject individuals. Fourth, trade secrecy is developed through practice and the controls required to assure secrecy are evaluated largely through contract and case law. Trade secrecy controls benefit their owners and this provides innovation incentives considered essential to societal progress while also encouraging commercial ethics that benefit society. Finally, national security pressures largely originate from statutes and national defense agencies typically under coordination of the executive branch. Society benefits from internal control that protects national security.

Clearly, the drivers for internal control are pressures focused from various public policy sources. These constitute a confluence of legal, regulatory and other public policy forces that combine to influence the development, implementation, testing, revision and evolution of internal control. The confluence of these factors combine to focus pressure on the basic functions of business including finance, accounting, IT, eCommerce, transaction processing as these traditional functions are implemented through the economy’s operators of critical infrastructure. The confluence hypotheses recognize that government, professional and market pressures for internal control are generally consistent and reinforcing. When conflicts are identified, policies generally encourage refinements that eliminate the conflicts and make compliance manageable.

This confluence is not widely understood except among the professions and service providers responsible for their installation, testing and assessment. This considerable unawareness contributes to resistance to both investment that improves the control regime and resistance to acceptance of responsibility for control effectiveness. The result of this misunderstanding and these resistances is that there may be sub-optimal investment in internal control, wasteful duplications, unfortunate opportunity costs and public policy advocacy detrimental to sound public policy. Finally, recognition and acceptance of the synergies inherent in this confluence should improve internal control with direct, causal security benefits for all the intended beneficiaries: professionalism, subject individuals, financial market integrity, asset owners and managers and society.

---

Outsourcing Standards

The complexity of modern relationships requires exhaustive and complete mapping of supplier-customer relations than was necessary traditionally. Modern supply chains are multi-layered with parties located all over the world. Each relationship complicates design and audit tasks that inevitably require additional verification expense. Competitive pressures can translate into shortcuts in design, management and audit that increase risks. Both internal users and investors depending on the robustness of these relationships are increasingly vulnerable to default risk. It becomes difficult to engage in business, government or non-governmental organizational activity without at least some reliance on outsourcing to provide communications, software, computing resources, data storage, financial services, payment processing, consulting services and the like. This is a far cry from simple traditional manufacturing supply chain relations with a few upstream component parts suppliers and downstream distribution outlets.

Provisionally, *outsourcing* is the sub-contracting by organizations to external component suppliers or intermediate customers for product supply or to service organizations for expertise or work that is either unavailable internally or where internal capacity is limited or planned for elimination. *Offshoring* is the outsourcing of various services, including IT, to nations outside the organization’s host country.\(^{64}\) Key to the audit role in security compliance is the identification and valuation of transactions cost risks attendant to domestic and offshore outsourcing agreements. Risks include due diligence failures, service level performance metrics, dispute resolution risks, ownership and control of data or intellectual property as well as risks in maintenance of confidentiality and the protection of privacy. Offshore outsourcing increases these risks because there are inevitable difficulties triggered by widespread ignorance of key cultural and infrastructure differences in the host and outsourcing nations.

Outsourcing is integral to modern industrial organization (I/O) analysis of the network structure in industrial data supply chains.\(^{105}\) Considerable confusion and emotive reaction surrounds outsourcing because “offshoring” jobs to lower wage nations is a recurring and potent political issue.\(^{65}\) However, outsourcing is a durable and persistent I/O issue, particularly since the dawn of the industrial revolution because vertical integration was among the earliest organization forms stimulating the antitrust backlash of the gilded era. Adam Smith’s “division of labour” underpins specialization,

---

\(^{64}\) See generally, Bagby, John W., *Using an Industrial Organization (I/O) Lens to Enhance Predictive Analytics: Disentangling Emerging Relationships in the Electronic Surveillance Supply Chain*, LEGAL AND ETHICAL ISSUES IN PREDICTIVE DATA ANALYTICS, Virginia Tech University, June 20, 2014.

Cloud Competition & Security

particularly problematic in imperfect markets. Law and economics guru Ronald Coase developed an important line in the Theory of the Firm explaining firms as simply bundles of contracts. This sets the stage for understanding integration through internal expansion with employees when transactions costs of external contracting, or outsourcing, become inefficiently high.

Agency costs are one major problem that limit the attraction of outsourcing when the incentives of the agent, to which duties are outsourced, diverge too far from the incentives of the principal. As the Nobel laureate Oliver Williamson theorized, these problems are not limited to supply chain relations only in the private sector, but must be understood when government outsources to private sector suppliers, consultants and service providers. Agency cost analysis requires exploration of the moral hazard that generally results in the need for higher monitoring activity and their associated monitoring costs. Second, conflicts of interest underlie some moral hazards. Third, the alignment of incentives between principal and agent requires clever design of compensation metrics often embodied in service level commitments (SLC). Of course, these potential agency costs signal the need for periodic audit.

---


67 Financial economists generally use the term agency costs while economists tend to prefer the term principal-agent problem.

Labor economics has long examined the \textit{runaway shop} problem resulting when previously internal activities are outsourced to independent entities.\footnote{See generally, Local 57, International Ladies' Garment Workers v. NLRB, 374 F.2d 295 (D.C. Cir. 1967) \url{https://law.justia.com/cases/federal/appellate-courts/F2/374/295/458403/} (noting NLRB charge three types of unfair labor practices (ULP) in plant relocations: 1\textsuperscript{st} interference with organization, 2\textsuperscript{nd} discrimination/retaliation for union affiliation or activities, and 3\textsuperscript{rd} refusal to bargain with old union).} Transportation and communication efficiencies diminish the need for “co-location” of component part suppliers and independent service organizations. Edge cloud computing services likely resembles such nearby co-location strategies. Off-shoring outsourced activities may become rational when delivery timing is made sufficiently just-in-time (JIT) and suffers minimal transportation hazards. Electronic communication of data, usually the primary subject of the outsourcing, is a key reason outsourcing generally and offshoring specifically are becoming more attractive. Co-location of independent entities is seldom necessary, particularly at the hopeful design stage, for information supply chains. Of course, audit needs intensify as suppliers become increasingly remote or cannot be subjected to local legal process or remedies. All these complexities create challenges in designing or auditing supply chain relationships.

The purported rationale for modern outsourcing is typically based on two justifications: scale economies and core competence. The first rationale is frequently

\begin{itemize}
  \url{http://unige.ch/sciences/societe/socio/files/1114/0533/6204/Williamson_1981.pdf} Williamson is also known for theorizing about the incentives for preferring recurring supplier-customer relations over ad hoc relationships and for \textit{information impactedness} where information costs remain elusive.\footnote{In 2011 the NLRB attempted to revive the runaway shop doctrine against Boeing, In re Boeing Co. NLRB 19-CA-32431 Complaint (April 2011) \url{http://www.belaborthepoint.com/wpcontent/uploads/2011/09/NLRB-v-Boeing-Complaint.pdf} (discussing Dreamliner assembly allegedly moved from Washington to South Carolina for runaway plant purpose).} Under service level management (SLM) the monitoring and verification of agent activities has given rise to extensive attest activities of internal and external auditors as well as significant consulting activities directed to confirm the process efficacy of service organizations.
  \item The audit of Service Level Agreements (SLA) is governed by Generally Accepted Auditing Standards (GAAS), formerly well-known as the SAS-70 regime, replaced in 2010 by Statement on Standards for Attestation Engagements No. 16, Reporting on Controls at a Service Organization (SSAE16), now SSAE 18, discussed next, see e.g., Knolmayer, Gerhard F. & Petra Asprion, \textit{Assuring Compliance in IT Subcontracting and Cloud Computing}, \textit{NEW STUDIES IN GLOBAL IT AND BUSINESS SERVICE OUTSOURCING} (2011, Springer - Berlin & Heidelberg) at 21-45.
\end{itemize}
Cloud Competition & Security

Therefore, cloud hosting using IaaS and PaaS models are usually the only practical alternative(s). Furthermore, as search, association, network and other analytics become proprietary, then data customers have little choice but to use third party, outsourced cloud configurations given the concentration of intellectual property in both the data and the algorithms underlying the big data analysis.

The second, core competence argument is related to the first, but is linked through IP. That is, technology and knowledge are unique, scarce and expensive. For example, many smaller firms and most government agencies cannot produce the algorithms needed for adequate analysis or manipulation of big data. Therefore, outsourcing permits access to the best proprietary technologies. The labor economics argument is similar, only there the outsourcer cannot afford nor attract competent employees with competitive skill sets to operate the function in-house or to replicate the coveted algorithms de novo, so the function must be outsourced to gain access to scarce expertise.

Thus, the application of the core competence argument to information supply chains is straightforward. The outsourcer cannot afford to staff, purchase or license the technologies so their data must be licensed or otherwise they only gain access when provided by external service providers. A dramatic example - it is speculated that the large U.S. TelCos must outsource their data harvesting deliveries when requested by the intelligence community I/C.

Outsourcing Standards: Service Organizations

There was some stability in the service organization focus for audit for over 18 years before a more turbulent era ensued in 2010. Between 1992 and 2011, the audit of service organizations, entities independent of an audit client, was driven by the fairly well-known audit standard, entitled Service Organizations, Statement on Auditing

72 See e.g., Bamford, James, THE SHADOW FACTORY: THE ULTRA-SECRET NSA FROM 9/11 TO THE EAVESDROPPING ON AMERICA (Doubleday, New York 2008). For example, U.S. TelCo giants AT&T and Verizon allegedly outsource their NSA compliant Mass Associational Tracking electronic surveillance to third party service providers, the Sunnyvale CA-based Boeing subsidiary Narus and NASDAQ-listed Verint of Melville NY.
Standards No. 70 (SAS 70). These standards and their progeny dictate the conduct, by a service auditor, of audits covering the control environments of service suppliers, such as cloud computing services. Whenever an entity provides services to a user organization that are part of the user organization’s information system, SAS 70 was implicated. Auditors who report on a service organization’s internal control environment that impacts financial statements were governed by SAS 70.

In 2011, SAS 70 was replaced by SSAE 16, Reporting on Controls at a Service Organization, Statement on Standards for Attestation Engagements No. 16. The American Institute of Certified Public Accountants (AICPA) further refined the SAS 70/SSAE 16 regime with guidance to accountants encouraging the conduct of various services, collectively the System and Organization Controls (SOC), titled and trademarked as a suite of service offerings. Since 2017, SOC are governed by SSAE No.18 that replaced SSAE 16.

A complex interplay exists between these evolving private-sector created audit standards and federal law. The Sarbanes-Oxley Act (SOX), created in the wake of the Enron financial crisis, created the Public Company Accounting and Oversight Board (PCAOB) and SOX §404 separately requires publicly-traded companies to establish financial reporting internal controls that are documented, tested and maintained to assure effectiveness.

Sectoral laws impact security generally and cyber-infrastructure in particular. These constrain activities in particular industries ranging from several bellwether sectors like the federal regulation of healthcare, finance, intellectual property, federal

117 SAS 70 is widely recognized as the audit regime despite renumbering, first as SSAE 16, now SSAE 18, and the encouragement of various types of audit engagement under the SOC “Suite of Services” regime, see generally, Attestation Standards: Clarification and Recodification, Statement


Cloud Competition & Security

on Standards for Attestation Engagements No. 18, American Institute Certified Public Accountants, (April 2016)
https://us.aicpa.org/content/dam/aicpa/research/standards/auditattest/downloadabledocuments/ssae-no-18.pdf

administrative law, education, veterans’ affairs, deceptive trade practices,\textsuperscript{75} and children’s’ protection. The states are also active, primarily in cyber-infrastructure protection of identity theft with security breach notification (disclosure) requirements, spyware and data disposal provisions.

\textbf{Outsource Competence Assurance}

Scrutiny over outsourcing to independent service organizations is increasing as outsourcing risks become better understood. Since the 1990s, academics have explored many of the research questions raised by domestic outsourcing. Such questions are only complicated by offshore outsourcing. Outsourcing orthodoxy now regularly focuses on the identification and valuation of transactions cost risks attendant to outsourcing agreement negotiations. There are issues of due diligence failures, service level performance (SLP) metrics, dispute resolution risks, ownership and control of data and intellectual property as well as risks in maintenance of security, confidentiality and the protection of privacy. In practice, offshoring adds jurisdictional problems to the usual array of international agreements including the inevitable difficulties triggered by widespread ignorance of key cultural and infrastructure differences that increase the risk of offshore transactions.\textsuperscript{76} As with the challenges for law that jurisdiction imposes on litigation involving foreign nations, audit of offshored outsourcing is costly, potentially incomplete and conducted under varying cultural conditions that dictate unfamiliar business practices.\textsuperscript{77} Many such contracts involve data storage in the cloud.

For almost twenty years, SAS 70 was the primary standard for judging the reliability of IT outsourcing to service organizations. Under Statement on Auditing Standard No. 70 “Service Organizations,” the Auditing Standards Board of the American Institute of Certified Public Accountants created a standards-driven regime used to review the competence and reliability of outsourcing. Audits for IT controls exerted over outsourced services become part of the reliability judgment about the financial statements of a publicly-traded company. The review of financial statements of closely-

held, non-public companies are sometimes bound by audit standards (e.g., lender or regulator requirement), not-for-profits are frequently audited by accounting firms trained in SAS 70 techniques, and it is predictable that government entities will eventually conform to SAS 70 regimen, particularly among agencies that access the capital markets.

In June 2011, additional migration for the purpose of international harmonization was noted from U.S.-based generally accepted auditing standards (GAAS) and generally accepted accounting principles (GAAP) to International Financial Reporting Standards (IFRS). To facilitate this switch in the U.S., SAS 70 was replaced with Statements on Standards for Attestation Engagements No. 16. SAS 70 had provided two thresholds for auditing their control effectiveness. Type I engagement produces a Type I report, a description of their control environment and its suitability. The Type II engagement, produces a report on required tests of the control environment’s effectiveness. SSAE 16 now adds a third layer that covers a whole accounting period (typically fiscal year). This would likely reveal proprietary and confidential operations so Type III reports may limit the report’s use to specified audiences. Cloud services are frequently identified as within SAS 70 and are now also covered by SSAE 16, treated as hosted data centers and ASP providing cloud services such as SaaS.

Another method to improve the reliability, security and quality of service for cloud services is to impose a duty to expose them to audit in the service provider’s engagement contract. Service level commitments are frequently included as duties and metrics of performance in service level agreements (SLA), this comprises service level management (SLM). While SLC vary greatly by the type of service involved, it is foreseeable that a cloud SLC would likely envision service metrics (e.g., mips, gigs, allowable downtime, network monitoring, speed to reply, security breaches, backup protocols, recovery from downtime). Many are expressed as mean times. Compensation can be keyed to SLC metrics. Ownership of data and other intellectual property, data escrow and other backup mechanisms to safeguard against fundamental breach of the SLC should be part of any negotiations for outsourcing to cloud services.