ARTICLE:

INTERNATIONAL ASPECTS OF MIGRATING DIGITAL FORENSICS IN THE CLOUD

By **John W. Bagby and Joseph J. Schwerha**

The cloud's unstable design has had a significant effect on digital forensics. Promised efficiencies of the cloud map fairly well into the digital forensic regime, particularly for investigations where all people with relevant information are independently doing their own searching. However, as more data migrates to the cloud there are burdens on privacy, security and the development of forensic quality evidence: particularly off-shored data, persistent file rotation and frequent modification of metadata. This article explores these difficulties in light of existing and proposed standards. The re-interpretation of procedural and evidence law may be needed to reduce the risk of injustice as cloud architectures evolve.

Introduction

The 'cloud'[1] is a vague and broad term for a set of on-line services, e.g., SaaS, IaaS, PaaS offering IT savings and new functionality.[2] Early cloud experiences indicated problems between the advantages offered by cloud services and traditional forensic practices. This article explores the public policy forces that may shape the future of cloud forensics. Cloud advocates claim transformative benefits: economies of scale, reliability, the ability to increase resources when necessary, ubiquitous accessibility, and enabling collaboration.[3] However, cynics of cloud computing argue that cloud services are unreliable for the inexperienced.[4] Despite the need for caution, wholesale migration to data hosting by cloud service providers (CSP) seems inevitable, and cloud forensics remains an unexplored territory for security and forensic professionals.[5]

Cyberforensic needs in the cloud are important to law enforcement, regulators, litigators, investigators, and the intelligence communities, together with the providers

1 *See generally Stephen Mason and Esther George, 'Digital evidence and "cloud" computing', 27 Computer L. and Security Rev. 524-528 (September 2011).*

2 *David Mitchell Smith, 'Hype Cycle for Cloud Computing', Gartner RAS Core Research Note No. (1 August 2012) ('While clearly maturing and beyond the Peak of Inflated Expectations, cloud computing continues to be one of the most hyped subjects in IT. We look at the different aspects of the topic and where the technologies are on Gartner's Hype Cycle for Cloud Computing, 2012.').*

3 *See generally Peter Mell and Timothy Grance, The NIST Definition of Cloud Computing, NIST, Spec. Pub. No. 800-145 at 6 (September 2011) available at http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf (sets standard cloud definitions including 'Essential [cloud] Characteristics'):*
NIST defines Essential [cloud] Characteristics to include (paraphrased here):
(i) On-demand self-service (unilaterally, without CSP human interaction),
(ii) Broad network access (varying consumer platforms obtaining access to data and processing capacity through networks),
(iii) Resource pooling (multi-tenant model of physical computing resources (storage, processing, memory, and network bandwidth) with 'location independence' such that consumers have no control or knowledge over the resources' exact location),
(iv) rapid elasticity (seemingly unlimited and the ability to increase resources when necessary), and
(v) metered service (usage directly dictates variable pricing).
Hereinafter to avoid confusion, the term 'client' is given only the computer services definition: user workstation and associated software. 'Client' is not used in the sense of consumer purchasing services from an independent service organization (ISO). Consistent with this convention, the term 'consumer' is used to identify the buyer of services from an ISO.

4 *For instance, see Michael Daconta, 'REALITY CHECK-Commentary: Why cloud computing is still a red herring', GNC (11 September 2009) available at http://gcn.com/articles/2009/09/14/reality-check-cloud-computing-as-red-herring.aspx (arguing cloud successes are largely proprietary clouds and prudence demands that government should set cloud standards before plunging into significant cloud deployments) citing Art Whittmann, 'Practical Analysis: Are We Sure this Isn't Clouded Judgment? INFO WEEK 11 April 2009) available at http://www.informationweek.co.uk/cloud-computing/software/practical-analysis-are-we-sure-this-isnt/216500080.*

5 *Keyun Ruan, Joe Carthy, Tahar Kechadi and Mark Crosbie, 'Cloud Forensics' Chapter 2 in Gilbert Peterson and Sujeet Shenoi (eds), 7th IFIP ADVANCES IN DIGITAL FORENSICS VII, vol. 361, (2011 Springer: Berlin and Heidelberg):*
'Cloud forensics is a cross discipline of cloud computing and digital forensics. ... Digital forensics is the application of computer science principles to recover electronic evidence for presentation in a court of law. Cloud forensics is a subset of network forensics. Network forensics deals with forensic investigations of networks. Cloud computing is based on broad network access. Therefore, cloud forensics follows the main phases of network forensics with techniques tailored to cloud computing environments.'

of relevant consultancy services. Increasingly access is needed to content, metadata, log records and document attachments located in the cloud. Cloud security and cloud forensics share the same characteristics of information assurance: economics, data integrity, accessibility, public policy constraints and the enabling technologies;[6] all are predictable problems deduced from the economics of security.[7]

While the evaluation of cloud economics remains in its infancy,[8] cloud efficiencies may be overstated. This problem is exacerbated because CSPs target unsophisticated consumers, habitually exaggerate cloud benefits, and cloud consumers too frequently fail in their own due diligence despite the well-known, traditional contracting risks for unsophisticated consumers.[9] This article assumes the reader is familiar with cloud architecture and functionality. However, a provisional cloud definition can provoke discussion and analysis, even as cloud architectures and services evolve.

A definition from the National Institute for Standards and Technology (NIST) provides a useful starting point.[10] Cloud Service Models include Software as a Service (SaaS) in which the cloud consumer uses the CSP's application (programs) running on a cloud (hardware) infrastructure, making these accessible from various customer devices, such as using a web browser for e-mail for instance. The customer does not manage or control the infrastructure, network, servers, operating systems, storage or application capabilities, other than the possible exception to a limited extend to re-configure the settings. Platform as a Service (PaaS) permits customers to create or acquire application programs and arrange these to the CSP's cloud-based infrastructure. The CSP then manages or controls the underlying cloud infrastructure (e.g., network, servers, operating systems, storage). Infrastructure as a Service (IaaS) enables the CSP to provide processing, storage, networks, and other fundamental computing resources that permits the customer to install and run arbitrary software (e.g., operating systems, applications). In IaaS, the customer has control over operating systems, storage, and the applications, but not over the underlying cloud infrastructure.[11]

Argument: the cloud benefits digital forensics

The promises of efficiency made by proponents of cloud technology translate well into the digital forensics domain. The cloud might enable lower costs and enhanced effectiveness in marshalling and collecting electronically stored information (ESI) for review, analysis and use as 'forensic quality evidence.' Could the cloud enable 'crowd sourcing' of investigatory data?[12] If so this arguably might lower dispute resolution costs by making pre-trial discovery documents in civil litigation accessible to the public.[13] Document availability in various 'cloud-like' environments illustrates that cloud-based discovery

6 *A complete treatment of cloud insecurity is beyond the scope of this article, but such matters intimately affect cloud forensics. See generally, B. R. Kandukuri, V. R. Paturi and A. Rakshit, 'Cloud Security Issues', 2009 SERVICES COMPUTING (IEEE) 517 (September 2009); Tim Mather, Subra Kumaraswamy and Shahed Latif, CLOUD SECURITY AND PRIVACY: AN ENTERPRISE PERSPECTIVE ON RISKS AND COMPLIANCE, (O' Reilly Media 2009); L. M. Kaufman, 'Can Public-Cloud Security Meet Its Unique Challenges?' 8 IEEE Sec.and Priv. 55 (July-Aug. 2010); Ronald L. Krutz and Russell Dean Vines, CLOUD SECURITY: A COMPREHENSIVE GUIDE TO SECURE CLOUD COMPUTING (Wiley 2010); Vic (J.R.) Winkler, SECURING THE CLOUD: CLOUD COMPUTER SECURITY TECHNIQUES AND TACTICS (Syngress 2011).*

7 *For instance, see John W. Bagby, 'Assessing Critical Infrastructure Risk After a Decade of Fragmented Regulation of Security Protections', No. ALSB2011_0110; Academy of Legal Studies in Business, New Orleans LA 8.4.11 available at http://faculty.ist.psu.edu/bagby/Pubs/ALSB2011_0110_paper.pdf (arguing market failure in achieving incentives sufficient to optimize investment in cyber-infrastructure security due to: (i) a complex, layered supply chain, (ii) situations where different people have vastly different amounts of information, (iii) externalities, (iv) people who take advantage without paying for the cost of the benefit, (v) direct costs and uncertain benefits, and (vi) hacker incentives).*

8 *See generally Asoke K. Talukder, Lawrence Zimmerman and H.A N. Prahalad, 'Cloud Economics: Principles, Costs, and Benefits', Chapter 20 in N. Antonopoulos and L. Gillam (eds.) Cloud Computing: Principles, Systems and Applications, (2010 Springer-Verlag London Ltd.), (in which they develop a conceptual model: the 'Cloud Computing Reference Model').*

9 *For instance, see Stuart D. Levi and Kelly C. Riedel, 'Cloud Computing: Understanding the Business and Legal Issues', Practicallaw.com (2010) available at http://us.practicallaw.com/8-501-5479.*

10 *Peter Mell and Timothy Grance, 'The NIST Definition of Cloud Computing', NIST, Spec. Pub. No. 800-145 at 6 (Sep.2011) available at http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.*

11 *Peter Mell and Timothy Grance, 'The NIST Definition of Cloud Computing'.*

12 *It is interesting to think that the move to the cloud, combined with predictive coding techniques could create world that is significantly simpler; but, it is as of yet uncertain as to whether such techniques would satisfy existing legal requirements.*

13 *For instance, see Master Settlement Agreement (web site), Office of Attorney General, State of California Department of Justice, available at http://oag.ca.gov/tobacco/msa. The National Association of States' Attorneys General (NAAG) also provides access to litigation repositories of tobacco litigation documents, available at http://www.naag.org/backpages/naag/tobacco/msa/msa-pdf/MSA% 20with% 20Sig% 20Pages% 20and% 20Exhibits.pdf.*

repositories enhance research and public policy.[14]

A 'Litigation Online Document Collection' resides in the cloud

Electronic discovery costs could be reduced with ubiquitously accessible, litigation-readiness rooms located in the cloud. As multiple litigants contribute and are authorized to obtain access to these repositories, this design could replace physical storage media. Such a litigation-readiness room could be either proprietary and confidential or open source for public accessibility. The analogy is to a war room, which is a central physical repository of relevant information to enable coordinated expertise in sense-making.[15] The resulting concentration facilitates the formulation of findings, strategic planning and expert analysis for decision-making. A famous war room was used by Winston Churchill in WWII; Churchill declared shortly after becoming Prime Minister, 'This is the room from which I will direct the war.'[16] In physical war rooms the participants project images, hang maps, and display potentially relevant data to assist in analysis and planning activities for various missions. Such investment in war room facilities, training and readiness are most justified in high stakes situations. War rooms concentrate information, the development of hypotheses, the testing of assertions, the stimulation of debate and ultimate decision-making where transaction and communication costs are reduced, delays minimized and relevant considerations are conveniently juxtaposed.

In adapting such traditional war room designs to litigation, pre-trial discovery, political campaigns and crisis management, the modern embodiment is particularly useful during crises where urgency demands swift, thorough and expert response. An electronic litigation-readiness room, possibly located in the cloud, constitutes a repository of documents, data and other information. Thus, users have easy access to a robust literature collection of primary and secondary litigation documents, often made selectively available to defined groups but also potentially publicly – a form of 'open source' forensics.

Electronic evidence repositories could encourage settlements on litigation claims theretofore considered infeasible. Public cloud repositories of electronic discovery or disclosure and other cyber-forensic data arguably enhances the collaborative advantages[17] of free collaborative efforts for open source intelligence investigations.[18]

Of course, there are legal risks in going beyond true open sources, such as in using clandestine investigatory methods. There are regulatory, civil, and criminal liabilities for wire tapping,[19] burglary,[20] treason or espionage,[21] assault,[22] bribery,[23] economic espionage or trade secret theft,[24] among others. Defensive hacking and some cyber forensics methods considered acceptable for national intelligence purposes, such as evidence collected in disrespect of the search and seizure protections of the Fourth Amendment of the U.S. Constitution, will not be acceptable. Moreover, indiscriminate on-line forensics, particularly involving intelligence activities crossing national borders, risks international retaliation, trade sanctions and wholesale trade bans.[25]

Counter argument: the cloud impedes digital forensics

Many cloud-based services expose digital forensics to new forms of failure. Some cloud services undermine fair and due process. Most centrally, cloud data is generally

14 *As a result of considerable tobacco litigation, including complaints filed by 46 state attorneys general in the U.S. and the Food and Drug Administration (FDA), several tobacco document databases are currently supported by stable, non-cloud data providers. Presumably, some of the tobacco documents are cloud-based. For example, the University of California-San Francisco (UCSF) Library and Center for Knowledge Management hosts the Legacy Tobacco Documents Library (LTDL) under funds provided by the American Legacy Foundation. The UCSF Tobacco Documents Bibliography permits search of published research into various effects of tobacco and the tobacco industry using key word and Boolean search techniques as well as traditional bibliographic archival indexing. The LTDL is available at http://www.library.ucsf.edu/tobacco/docsbiblio.*

15 *Simon Attfield and Ann Blandford, 'E-disclosure viewed as 'sensemaking' with computers: The challenge of "frames"' 5 Digital Evidence and Electronic Signature Law Review (2008) 62 – 67.*

16 *http://www.iwm.org.uk/visits/churchill-war-rooms.*

17 *Don Tapscott and Anthony D. Williams, WIKINOMICS: HOW MASS COLLABORATION CHANGES EVERYTHING (2006) New York: B and T.*

18 *On the value of citizen investigative journalism as applied to the crowd-sourcing of investigations, see Paul Bradshaw and Andy Brightwell, 'Crowdsourcing Investigative Journalism: Help me Investigate – A Case Study' in Eugenia Siapera and Andreas Veglis, eds, The Handbook of Global Online Journalism (Wiley-Blackwell, Oxford, 2012).*

19 *18 U.S.C §§2510-22 (2006).*

20 *MODEL PENAL CODE §221.1.*

21 *18 U.S.C §§793-98 (2006).*

22 *MODEL PENAL CODE §211.1.*

23 *18 U.S.C §§201-27 (2006).*

24 *18 U.S.C §§1831-1839 (2006).*

25 *For instance, see Joris Van Hoboken, Axel Arnbak and Nico Van Eijk,' Obscured by Clouds or How to Address Governmental Access to Cloud Data from Abroad', (9 June 2013), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2276103.*

opaque and this complicates forensics. Cloud file and directory structures are unstable and in constant flux. The off-shoring of data and general cloud practices cause persistently rotating file locations that tag with frequent metadata modifications in activity logs and file access. Many nations outside of the United States and Europe are typical hosts for cloud services. Most have generally less-well developed laws regulating privacy and security or that create litigation process rights. The prevailing cloud practices erect barriers of cost, reliability, and access (lack of reciprocity) to conduct accurate forensics due to the international location of cloud repositories. Nearly all these conditions are inconsistent, not only with U.S.-style litigation expectations, but of most jurisdictions across the world.

Challenges of digital forensics in the cloud

In the U.S., it is uncertain whether the current rules of evidence and trial procedure are adequately adapted to the cloud. The cloud, by its nature, is unstable and instability is generally inconsistent with traditional evidentiary safeguards. Consider that any snapshot of a cloud system's data is not likely to reflect the original data exactly; records of all data changes may not be preserved adequately; money-saving cloud arrangements probably mean that back-up of data is not frequent; storage location stability and accuracy of data are compromised. Cloud transaction records may fail to accurately identify the timing and source of file changes. There are two major factors in this cloud unreliability in evidentiary preservation: system states are unstable and cloud system architectures are not stable.

Cloud system states are unstable

The cloud is widely promoted as offering an advantage: cloud system states are unstable. Files are constantly updated, moved to back-up locations, and repeatedly imaged, often at alternate locations – a back-up security advantage. While this results in a proliferation of duplicate data that enables forensic analysis of file evolution (development of a manuscript) it also results in multiple redundant copies. Duplicates may exist for only short, transitory times. Cloud-based files, logs and metadata change frequently. These system states may sometimes be predictable and well documented (logged), but would also be random, unpredictable and evanescent at other times. The credibility and forensic quality of evidence is undermined by the lack of stability. Furthermore, such deficiencies can cause evidence to be dismissed for a variety of reasons: authenticity, custodial integrity, best evidence, hearsay, exclusionary incompetence and relevance.

The most basic forensic challenge of cloud-based ESI may be best captured with this ironic query: 'What is that Cloud Server's Street Address Again?'[26] Subpoenas and other court process to produce ESI and civil litigation pre-trial discovery require accurate physical location data for targeted files, back-up data, responsible custodians (humans), and knowledgeable supervisors. Accurate and stable physical location data enables an understanding of a discovery target's system design and practices that informs all other discovery needs.[27] Pattern interrogatories frequently seek design, vendor and configuration data to enable later phases of discovery, including interrogatory questions seeking details about (i) network infrastructure, (ii) internet access and usage, (iii) computers and server hardware, (iv) software applications, (v) back-up systems and regimes, (vi) electronic communication systems and practices (e-mail, voice mail, IM, SMS, work-related social networking), (vii) traditional telephony, (viii) mobile (device) communications, and off-site work location systems and protocols. Similar considerations attend regulatory and criminal investigations.

The physical location of records has always been a challenge for judicial or regulatory authorities as they extend their reach to the physical location of information storage. While off-shoring and cloud systems use diminishes costs for the cloud consumer, these practices actually raise costs for litigation opponents, ESI requestors and law enforcement when information is stored outside the jurisdiction. Concerns arise when cloud repositories are physically located off-shore. Many foreign nations fail to fully embrace the full-facts provision duties of many nations' civil litigation and regulatory enforcement. This risks inefficient access to relevant ESI when it resides off-shore. Furthermore, CSPs probably move data frequently to take advantage of cost savings, to

26 For instance, see, Karyn Benson, Rafael Dowsley and Hovav Shacham, ' Do You Know Where Your Cloud Files Are?' ACM Cloud Computing Security Workshop CCSW' 11, (21 October 2011) and Brandon Butler, ' Do you know where your cloud data is? When data goes into the cloud, customers may want to know exactly where that is, but providers don' t always say' , Network World, 25 April 2012.

27 FED.R.CIV.P. 33. Interrogatories frequently seek brand, model, design, location and custodian information about computer and information processing systems to aid requesting parties in civil discovery in refining their identification of deposition targets and drafting deposition examination questions, as well as the refinement of production of (ESI) documents requests, see generally, Sharon D. Nelson, Bruce A. Olson and John W. Simek, THE ELECTRONIC EVIDENCE AND DISCOVERY HANDBOOK: FORMS, CHECKLISTS AND GUIDELINES (American Bar Association, 2006).

permit the rapid movement of resources when necessary, and to locate data in jurisdictions with lower regulatory burdens (e.g., privacy, security, record retention, disclosure duties) – a classic 'race to the bottom.' Cloud proliferation raises opacity and imposes information accessibility challenges that may undercut 'traditional notions of fair play and substantial justice.'[28]

Cloud architecture is an unstable bundle of contracts

The cloud is actually a collection of numerous services and service models susceptible to various architectures. Indeed, cloud service providers tout their innovation, much of which represents new configurations, controlling software, hardware and its physical location, functionality and security. The cloud can be expected to evolve with changing architecture despite attempts by NIST to define stable states. Indeed, the cloud is a technical embodiment of Berle and Means 'Bundle of Contracts' in which many suppliers to the CSP are unaffiliated except through outsource sub-contracts.[29] Furthermore, it should be expected that many contracts in that bundle are not long-term contracts as were popular in the twentieth century as stable sources of supply or long-term loyal customers. At-will outsourcing creates an unstable web of contracts between client and CSP when the latter outsources or off-shores cloud services to CSP sub-contractors in real time and for various services (e.g., server capacity, increasing or decreasing operations, security, connectivity, legal services, billing services).

Cloud vendors and consulting services that promote migration to the cloud argue that this 'virtualization' of the cloud, including its inherent instability, is a virtue because it is flexible. The cloud is actually defined by its legal contracts and not primarily by some technical system map or schematic specification. Indeed, technical system visualizations seldom adequately detail any nuanced terms or conditions of cloud end-user license agreements, service level commitments (SLC) or the complex outsource service agreements or service-level metrics (also known as 'measurements') (SLM) that define adequate performance, material breach of contract and activate contractual obligations (e.g., payments based on metered performance, penalties, termination, audit, data ownership or other intellectual property rights).

Therefore, the instability of cloud system states and architecture, when combined with unpredictable physical locations for ESI storage, pose great problems for privacy rights or for obtaining access to information in litigation. That is, the discovery or investigation target has the right to resist 'fishing expeditions' and demand a limited scope for the investigation or discovery request.

Particularity, minimization and scope

Under the Fourth Amendment of the U.S. Constitution,[30] and many other nations' legal process requirements, there is a requirement for 'particularization' for search warrants and subpoenas.[31] Interpretive case law has required 'minimization'[32] to avoid 'fishing expeditions'[33] or breaching various privileges,[34] and discovery rules require the scope of all discovery devices be limited by relevance to issues expected at trial.[35] One benefit claimed by cloud providers is 'co-tenancy', which particularity acts to exacerbate minimization and scope requirements. Physically neighbouring virtual drive space, files, and sectors are commingled among various individual and independent cloud consumers. The data of unaffiliated parties is spread throughout the server farm(s) used by the CSP for uncertain groupings of clients. This haphazard but 'efficient' cloud design could be done differently, such as in the case of private clouds that have few co-tenants or allocate identifiable sectors or servers to particular consumers. The particularity requirement is an even more challenging problem in discovery of trade secret documents[36] and possibly for expression protected under the First Amendment to the U.S. Constitution to avoid allegations of the chilling effect of prior restraint.[37]

28 *International Shoe Co. v. Washington, 326 U.S. 310 (1945).*

29 *Adolf A. Berle, and Gardiner C. Means, THE MODERN CORPORATION AND PRIVATE PROPERTY, 2nd edn (Harcourt, Brace and World, New York 1967).*

30 *U.S. CONSTITUTION, AMENDMENT IV: ' The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized,' (emphasis added).*

31 *For instance, see Berger v. New York, 388 U.S. 41 (1967) (citing Etnick v. Carrington, 19 How.St.Tr. 1029 to condemn ' general warrants' because they lack particularity); United States v. Scarfo, 180 F.Supp.2d 572 (D.J.J.2001) (' certain modicum of particularity').*

32 *For instance, see Clifford S. Fishman, ' The ' Minimization' Requirement in Electronic Surveillance: Title III, the Fourth Amendment and the Dread Scott Decision' , 28 AM.UNIV.L.REV. 315 (1979).*

33 *For instance, see Hickman v. Taylor, 329 U.S. 495, 507 (1947); Stephen Smith, 39 B.C.L.REV. 691 (1998); Richard L. Marcus, ' Discovery containment dedux' , 9 B.C. L.REV. 747 (1998).*

34 *For instance, see FED.R.EVID. 502 (preserving privilege in various situations, e.g., inadvertent waiver); FED.R.CIV.P. 26(b)(1) (discovery limited to nonprivileged matters); FED.R.CIV.P. 26(b)(5)(b) (mandating pre-trial conference address privilege issues in documents produced).*

35 *FED.R.CIV.P. 26(b)(1) (duty to disclose limited by relevance to claims or defenses, trial judge may expand relevance to include any matter involving the subject matter in the litigation).*

36 *Warden v. Hayden, 387 U.S. 294, 302-03 (1967).*

37 *For instance, see Marcus v. Search Warrant, 367 U.S. 717, 730-31 (1961); Stanford v. Texas, 379 U.S. 476, 485 (1965); A Quantity of Books v. Kansas, 378 U.S. 205, 210 (1964); Heller v. New York, 413 U.S. 483 (1973).*

Multi-jurisdictional transaction costs

The providers of cloud services claim that a significant advantage is the movement across national borders in order to find the lowest costs. The costs of transactions are reduced in migrating data over borders at will given the high speed and high quality bandwidth increasingly available. Cloud services will continue to be complex services, created by an intricate web of outsourcing contracts. As with all international commerce, the enforceability of contracts becomes less certain and thereby imposes an increased risk that your side could default. It should be expected that cloud services will mimic other international commercial practices by focusing on international enforcement agreements, comity and negotiated choice of law or forum to identify and inform business risk analysis.

Data havens cause failure of reciprocity

Reciprocity between state or provincial governments and between nations characterize the development of international law. Such challenges are overcome despite the natural incentives of nations to avoid burden on their own citizens, domestic business organizations or government entities. Indeed, litigation by foreign nationals or governments risk embarrassment, international incident and pecuniary liability. Sovereign immunity protects government entities from litigation or prosecution initiated in or by someone in a foreign nation. But this traditional international law concept does not, generally, apply to private citizens or business organizations and commercial enterprises.[38] Indeed, confidentiality and privacy exemptions are deeply rooted in cultural autonomy. Some nations have had a long history in thwarting litigation initiated by foreign nationals. Current strong data protection laws are further evidence of this self-interested protectionism.[39] Switzerland would appear to have a national business model devoted to bank secrecy, making it the quintessential banking haven including data transfer restrictions that have chronically plagued off-shore efforts at justice.[40] Bank secrecy has apparently played at least some role in preserving Swiss neutrality. However, from the perspective of the U.S., European aversion to foreign law enforcement and litigation extends beyond bank secrecy.

Blocking laws are another exemplar. Consider that civil discovery is generally inconsistent with primary trust in the inquisitorial powers of trial judges in civil law nations.[41] Indeed,

> [n]o aspect of the extension of the American legal system beyond the territorial frontier of the United States has given rise to so much friction as the request for documents in investigation and litigation in the United States.[42]

Blocking laws were originally enacted to prevent foreign private plaintiffs and regulators from obtaining document production largely to prove antitrust and securities claims. Blocking laws are national laws that erect barriers to discovery during litigation initiated off-shore. Blocking laws take several forms, some broadly protect a specified industry from litigation by foreign nationals, while other forms of blocking endows regulators with some discretion to permit the fulfillment of discovery requests. When most narrowly drawn, blocking laws prohibit compliance unless that nation's own procedural requirements are fulfilled.[43]

Difficulties from blocking laws eventually prompted negotiations in The Hague Conference on Private International Law. Some success was achieved in the early 1970s when the Hague Conference enacted the *Convention of 18 March 1970 on the Taking of Evidence Abroad in Civil or Commercial Matters* (Hague Evidence Convention) authorizing 'letters rogatory' among signatory states without the much more uncertain and

38 See generally, John W. Bagby, and Gary L. Gittings, 'The Elusive Discretionary Function Exception From Government Tort Liability: The Narrowing Scope of Federal Liability', 30 AM.BUS.L.J. 223-269 (September 1992) (analytic framework for governmental immunity under discretionary function exception).

39 Suffice to say that there is a significant bibliography relating to the controversy over blocking laws.

40 As of this writing, pressures from U.S. tax regulators for changes in European banking secrecy have resulted in promises by Austria and Luxembourg to share bank account data, putting further pressure on the Swiss to change bank secrecy. Some limited Swiss actions to relax bank secrecy is underway, but there remains strong opposition making wholesale repeal unlikely – Raphael Minder, 'Pressure Mounts on Vaunted Secrecy of Switzerland's Banks', New York Times (23 May 2013).

41 Although the position is more nuanced, for which see the individual chapters in Stephen Mason, ed, International Electronic Evidence (British Institute of International and Comparative Law, 2008), the main thrust of the point remains.

42 For instance, see RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 442, Reporters' Note 1 (1987).

43 David W. Ogden and Sarah G. Rapawy, 'Discovery in Transnational Litigation: Procedures and Procedural Issues' (16 March 2007) ABA Business Law Section Spring Meeting – WilmerHale, available at http://apps.americanbar.org/buslaw/newsletter/0058/materials/pp1.pdf. See also Yvonne G. Grassie, 'Foreign Bank Secrecy and Disclosure Blocking Laws As a Barrier to SEC Policing of Transnational Securities Fraud', 65 WASH.U.L.Q. 259 (1987); Stephen Mason, 'Some international developments in electronic evidence', Computer and Telecommunications Law Review, 2012, Volume 18, Issue 1, 23 – 32.

costly process of pursuing evidence through diplomatic channels.[44] However, it is yet to be seen whether such methods will work in a business environment where so much intelligence is based in the cloud.

Addressing cloud forensic risks

Existing laws and various national and international standards already address risks to security and justice. The most compelling approach to address these risks is to simply adapt these existing authoritative constraints to the cloud environment. Some aspects require little adaptation and remain consistent with strict constructionism[45] while others may require an evolutionary approach.[46]

Role of outsourcing standards

The use of the cloud to facilitate pre-trial discovery is a significant method to easily and efficiently exchange documents, make these documents available for examination to geographically dispersed authorized users, and to assure uniformity (i.e., version control). Pre-trial discovery, always a costly process, imposes burdens for document retention, document search and relevance retrieval, document review for privilege exclusion, copying and distribution. This burden induces settlement incentives. Although the power of networked computer systems should have reduced discovery costs, instead, the efficiency gains of electronic manipulation were overwhelmed by the costs of an increased volume of information, addressing problems with duplicate copies and preliminary drafts, and using innovative analytical techniques.[47] Pressures to contain the costs of electronic discovery have led to reinforcing the traditional initial cost of assignment,[48] cost shifting,[49] balancing factors,[50] and sampling techniques. Outsourcing data to the cloud promises data processing savings but it may place some information beyond legal reach in some cases, so overall cost reduction is speculative at best given the likelihood of unexpected side effects.

CSP are actually *independent service organizations* to whom outsourcing is contracted, and this implies outsourcing risks. Academics often use an analogy to industrial organizations derived from theories of law and economics, as well as from business strategy, because these provide useful conceptual frameworks. Provisionally, outsourcing is the sub-contracting by any type of organization to an external supplier. These contracts may source tangible goods from a custom product supplier or source services from a *service organization*. Outsourcing IT work is a well-recognized subset of the service outsourcing in which expertise or work is sought that is either unavailable internally or is needed where internal capacity is insufficient, too expensive or its elimination is planned. Off-shore outsourcing delegates services to service providers located in nations outside the organization's host country.

Since the 1990s, academics have explored many of the research questions raised by domestic outsourcing; these questions are only complicated by off-shore outsourcing. Outsourcing orthodoxy now regularly focuses on the identification and valuation of transaction cost risks attendant to outsource agreement negotiations. There are issues of due diligence failures, service level performance (SLP) measurements, dispute resolution risks, ownership and control of data and intellectual property as well as risks in the maintenance of security, confidentiality and the protection of privacy. In practice, off-shoring adds jurisdictional uncertainties to the usual array of international agreements, including the inevitable difficulties caused by widespread ignorance of important cultural and infrastructure differences that increase the risk of off-shore transactions.

For almost twenty years in the U.S., 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 used a standards-driven regime used to review the competence and reliability of outsourcing. Audits for IT controls exerted over outsourced services are a part of the judgment about the reliability of financial statements of publicly-traded companies. The review of financial statements of closely-held, non-public companies are sometimes bound by

44 *Societe Nationale Industrielle Aerospatiale v. U.S. District Court, 482 U.S. 522, 541 (1987) (Federal Rules of Civil Procedure valid authority to collect evidence from foreign parties for U.S. lawsuits).*

45 *For instance, see Livingston Hall, 'Strict or Liberal Construction of Penal Statutes', 48 HARV.L.REV. 748-774 (March 1935) and Thomas Y. Davies, 'The Supreme Court Giveth and the Supreme Court Taketh Away: The Century of Fourth Amendment Search and Seizure Doctrine', 100 J. CRIM. L. AND CRIMINOLOGY 933 (2010).*

46 *Pamela Samuelson, 'Five Challenges for Regulating the Global Information Society, Regulating the Global Information Society', in Christopher T. Marsden ed., Regulating the Global Information Society, (Routledge, 2000).*

47 *Oppenheimer Fund, Inc. v. Sanders, 437 U.S. 340, 358 (1978).*

48 *Oppenheimer Fund, Inc. v. Sanders, 437 U.S. 340, 358 (1978).*

49 *Zubulake v. UBS Warburg, 217 F.R.D. 309 (S.D.N.Y. 2003).*

50 *GUIDELINES FOR STATE TRIAL COURTS REGARDING DISCOVERY OF ELECTRONICALLY-STORED INFORMATION, Conference of Chief Justices (August 2006) available at http://ncsc.contentdm.oclc.org/cdm/ref/collection/civil/id/56.*

audit standards, such as when imposed by a lender or regulator requirement. Not-for-profit organizations 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 obtain access to the capital markets.

To satisfy the aim of international harmonization, in June 2011, additional migration was noted from U.S.-based generally accepted auditing standards (GAAS) and generally accepted accounting principles (GAAP) to International Financial Reporting Standards (IFRS). SAS 70 was replaced with Statements on Standards for Attestation Engagements No. 16 (SSAE 16). SAS 70's two thresholds for auditing their control effectiveness are retained and enhanced by SSAE 16. Type I engagement produces a Type I report, a description of the control environment and its suitability. The Type II engagement produces a report on required tests of the effectiveness of the control environment. SSAE 16 now includes a third layer that covers a whole accounting period (typically fiscal year) and may limit the report's use to specified audiences. Cloud services were frequently identified as within SAS 70, but are now covered by SSAE 16 as hosted data centers and application service providers (ASP) provide cloud services such as SaaS. SAS 70 and SSAE 16 provide one source of partial relief for cloud service customers if the cloud service vendor has negligently outsourced component services. Thus, in the cloud outsourcing environment, the SAS 70 reports verify that the outsource service provider operates faithfully and that the outsource customer, often the cloud service provider, has controls in place and these controls are working to assess default risk.

Role of strong contracts

Cloud reliability, security and quality can be defined in the service provider's engagement contract. Service level commitments (SLC) frequently specify duties and performance measurements in service level agreements (SLA), overseen by service level management (SLM). SLC vary greatly by the type of service involved. A cloud SLC is likely to state service measurements (e.g., mips, gigs, allowable downtime, network monitoring, speed to reply, security breaches, recovery from downtime) expressed as mean up or down times. SLC often cover availability of data, speed of processing, security arrangements, and permit further outsourcing. The pricing relating to the ability to adapt to increasing or decreasing demands is of particular concern. Compensation levels per unit of measured performance (storage units (gigs), transaction queries, guaranteed uptime) typically run higher at higher levels of service. Prices often rise at the consumer's increased levels of needs. For example, 'basic' cloud services, initially available at low prices, rise at higher levels, a form of 'bait and switch'. Terms of service may also include provisions declaring the consumer's data or other intellectual property are owned by the CSP. Provisions may be negotiated about data escrow and back-up practices to safeguard against a fundamental breach of the SLC.

Cloud services contracts resemble adaptations of license and service provider agreements but may also function like leases.[51] CSPs may become concerned that a few jurisdictions will decide that cloud services combine tangible goods as products (software) along with services (storage).[52] Many CSPs outsource component services to outsource suppliers, the latter may be domiciled in yet other jurisdictions. The enforceability of these outsource relations by the consumer of the CSP is doubtful. Accountability for full performance of these component, outsourced services may not be available to customers even under a third party beneficiary theory, making litigation against the sub-contractors impractical under any circumstances traditionally addressed by third party practices (e.g., interpleader, impleading).

Cloud services include typical licensing provisions adapted to the cloud service: (1) a grant clause describing the services or software or both services and software, (2) a co-tenancy clause permitting non-exclusive 'occupation' of adjoining server capacity, (3) exclusivity requiring the cloud consumer to do all its cloud business with that SCP, (4) sublicensing provisions permitting the CSP a veto over the consumer's assignment to a successor business (e.g., subletting by tenant requiring landlord permission), (5) duration and termination provisions, (6) warranties, (7) indemnification provisions, (8) definitions of terms, (9) disclaimers, (10) choice of law provisions, (11) choice of forum clauses, and (12) arbitration requirements given the likelihood that data will probably move across international borders.

51 *John K. Halvey and Barbara Murphy Melby, INFORMATION TECHNOLOGY OUTSOURCING TRANSACTIONS: PROCESS, STRATEGIES, AND CONTRACTS, 2nd edn (2005, John Wiley NY).*

52 *Gross v. Symantec Corp., No. C 12-00154 CRB (N.D. Cal. July 31, 2012) (holding software license constitutes sale of goods governed by Uniform Commercial Code (UCC)).*

Control and ownership of the consumer's data is a common problem in cloud contracts that can negatively affect forensics. The CSP might own the consumer's data, impairing forensics, imposing lock-in pressure on the cloud consumer to retain the CSP and enabling high-priced charges for increasing demands.[53] Furthermore, the CSPs custody or further outsourcing of the consumer's data to independent server farms in another nation adds further complication and enhances lock-in.[54] When cloud consumers regularly back-up their data, it is likely that the promised cost savings do not occur. Frustrating forensics, the CSP may not be obligated to search for and produce particular data (e-mails, files, metadata) without a clear SLC term or optional service level at additional cost.

Cloud forensics cause legal conundrums

One model of cloud forensics involves the initial acquisition of ESI from a standalone computer, analyzing logs and internet artifacts of cloud transactions that could be retained, e.g., Dropbox or Sugar Sync uploads. However, the second method occurs when the customer obtains remote access to data from a remote system. In such a case, an automatic connection and request is made to the remote cloud repository for the image, file, e-mail and associated metadata. The legal justifications for obtaining access to such evidence differs, depending upon whether the context is criminal action, regulatory investigation or civil litigation.

Assuming the evidence sought is not located within the jurisdiction where the court is located, some form of remote forensics might be used. This involves the acquisition of evidence from a computer over which there is control, but which is geographically distant. Travel to collect this evidence raises cost issues. While such cost savings can be substantial domestically, they generally rise much higher internationally. In the U.S. it is expensive to image a single computer hundreds of miles away, but international travel is typically even more expensive. In a civil case, the remote acquisition of evidence from a CSP presumes the party is a consumer under a court's jurisdiction and that consumer has contractual rights to the data sought.[55]

In civil cases, ESI may be acquired remotely under some legal authorization, but the ESI must be not privileged. The discovery of social media is an increasing source of cloud forensic evidence, and no social networking privilege appears to exist.[56] Traditional civil discovery presumes the forum court has jurisdiction over the parties and the parties control their respective data. This simply enables courts to order discovery of ESI held in the cloud.

Privacy laws may also apply. Under the U.S. federal statute, the Electronic Communications Privacy Act (ECPA), parties may not be able to force third parties (e.g., CSP) to produce their client's ESI, if covered by the Stored Communications Act (SCA), a component of ECPA. The SCA restricts those entities that fall under the definition of an 'Electronic Communications Service' (ECS) or a 'Remote Computing Service' (RCS) from voluntarily supplying covered communications to an outsider. No SCA exception exists for civil litigants to directly request records pertaining to opposing parties.[57]

A possible resolution is to permit the judge to order the party with 'disposition or control' over the data (i.e. the defendant) to provide the ESI. No litigant with a FaceBook account could validly rely on the SCA to refuse to comply because they are neither an ECS or RCS under the SCA. When the data repository is not a party to the litigation, the opposing party would file a motion to compel enabling the court to order revelation of that ESI. ESI located outside the U.S. or its territories is resolved on a case-by-case basis, but would probably require an examination of the national laws in the country where the data is located.

Criminal procedure issues in cloud forensics

At the U.S. federal level, authority to issue warrants is based upon geographic boundaries. Jurisdiction to issue search warrants is governed by the Federal Rules of Criminal Procedure. A federal magistrate judge may issue a warrant under Fed. R. Crim. P. 41(b):

> (b) Authority to Issue a Warrant. At the request of a federal law enforcement officer or an attorney for the government:

53 *'Lock in' describes customer dependency on a particular vendor when changing contracts to another vendor would impose high switching costs: John W. Bagby, Sandeep Purao and Prasenjit Mitra, 'Standards Development, Disruptive Innovation and the Nature of Participation: Lock-In, Lock-Out, Holdup', 34TH RESEARCH CONFERENCE ON COMMUNICATION, INFORMATION AND INTERNET POLICY, Telecommunications Policy Research Conference (TPRC) 30 September 2006, Arlington VA available at http://faculty.ist.psu.edu/bagby/Pubs/BagbyPuraoMitraStdsLockHold2.pdf.*

54 *Witt Ulrich, '"Lock-in" vs. "critical masses" — Industrial change under network externalities', 15 International Journal of Industrial Organization 753 (October 1997) available at http://www.econ.mpg.de/files/2004/staff/witt_LockInVSCriticalMasses.pdf.*

55 *Litigation is also presumed here, but consider that in an internal investigation (employee browsing adult pornography at work) while not a crime, might violate work rules and constitute a breach of employment contract and thereby cause for termination of employment but not immediate litigation.*

56 *Largent and Largent v. Reed, et al., Court of Common Pleas of Franklin County at 9 (November 7, 2011).*

57 *Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965 (C.D. Cal. 2010) (holding that Facebook was both an ECS and an RCS, depending upon the function of the site at that particular time).*

(1) a magistrate judge with authority in the district – or if none is reasonably available, a judge of a state court of record in the district – has authority to issue a warrant to search for and seize a person or property located within the district;

(2) a magistrate judge with authority in the district has authority to issue a warrant for a person or property outside the district if the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed;

(3) a magistrate judge – in an investigation of domestic terrorism or international terrorism – with authority in any district in which activities related to the terrorism may have occurred has authority to issue a warrant for a person or property within or outside that district;

(4) a magistrate judge with authority in the district has authority to issue a warrant to install within the district a tracking device; the warrant may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both; and

(5) a magistrate judge having authority in any district where activities related to the crime may have occurred, or in the District of Columbia, may issue a warrant for property that is located outside the jurisdiction of any state or district, but within any of the following:

(A) a United States territory, possession, or commonwealth;

(B) the premises – no matter who owns them – of a United States diplomatic or consular mission in a foreign state, including any appurtenant building, part of a building, or land used for the mission's purposes; or

(C) a residence and any appurtenant land owned or leased by the United States and used by United States personnel assigned to a United States diplomatic or consular mission in a foreign state.

Some scholars argue that search warrants should change in the modern era by revising requirements for search and seizure via a warrant that should evolve to reflect the realities of search practices, arguing:

> '... that the warrant process must be reformed in light of the new dynamics of computer searches and seizures. In the last two decades, the widespread use of computers has lead to a new kind of evidence in criminal cases: digital evidence, consisting of zeros and ones of electricity.'[58]

For example, Professor Kerr argues the distinction between searching and seizing evidence dictates change.[59] For example, a warrant might be better designed if it simply describes the computer to be searched rather than its physical location:

> '[I]magine an FBI field office has a computer in its possession and needs a search warrant to search the machine. The 'place to be searched' could be a particular description of the computer itself, held in the custody of the FBI field office. That is, the warrant would name the specific movable property to be searched, rather that the physical place where that moveable property happens to be stored.'[60]

Of course, moving away from geographic based search descriptions will undoubtedly raise other problems.

Vagaries of delivering Notice to the cloud

There are notification difficulties in enforcing search warrants for cloud-based searches, mostly due to the fact that the search is conducted remotely. Some scholars suggest digital searches may currently provide inadequate oversight and record-keeping requirements. Brenner and Frederiksen argue that better detail is needed for inventories accompanying a warrant:

> 'These inventories should be supplied in addition to the back-up copies of any seized data. The inventories are not substitutes for back up copies ... For computer media or seized files the inventory should describe the type of media, capacity (if known), number seized, and a listing of the files contained on the media.'[61]

However, if the only access to the hard disk drive to be

58 *Orin S. Kerr, ' Search Warrants in an Era of Digital Evidence', 75 MISS. L. J. 85 (2005) (arguing search and seizure via warrant must evolve given modern search practices).*

59 *Orin S. Kerr, ' Search Warrants in an Era of Digital Evidence', at 133.*

60 *Orin S. Kerr, ' Search Warrants in an Era of Digital Evidence', at 134.*

61 *Susan W. Brenner and Barbara A. Frederiksen, ' Computer Searches and Seizures: Some Unresolved Issues', 8 MICH. TELECOMM. TECH. L. REV. 39, 98 (2002) available at http://www.mttlr.org/voleight/Brenner.pdf.*

searched is through a network connection, it is hard to provide some of this other information. Thus, in order to search for ESI in criminal matters, or to acquire evidence in civil or regulatory cases, when based upon a description of the device itself, it may be impossible to comply with the legal requirements of inventory, return and receipt. Similar difficulties exist for the custodial care responsibilities. The officer would have trouble providing the required receipt or for the return[62] of the property seized where the place searched is a computer at an unknown location.[63]

A recent U.S. federal case in Texas confirms this difficulty. *In re Warrant to Search a Target Computer at Premises Unknown* illustrates why the search warrant application 'specifying' a computer at an unknown location was denied:

> 'In early 2013, unidentified persons gained unauthorized access to the personal email account of John Doe, an individual residing within the Southern District of Texas, and used that email address to access his local bank account. The Internet Protocol (IP) address of the computer accessing Doe's account resolves to a foreign country. After Doe discovered the breach and took steps to secure his email account, another email account nearly identical to Doe's – the address differed by a single letter – was used to attempt a sizeable wire transfer from Doe's local bank to a foreign bank account. ... [T]he location of the suspects and their computer [was] unknown.'[64]

This warrant was not typical, the government sought to secretly install data extraction software on the suspect's computer. Once remotely activated, the government would have the 'capacity to search the computer's hard drive, random access memory, and other storage media; to activate the computer's built-in camera; to generate latitude and longitude coordinates for the computer's location; and to transmit the extracted data to FBI agents within this district.' The Government sought records of the IP addresses used; records of internet activity, including firewall logs, caches, browser history and cookies, 'bookmarked' or 'favorite' web pages, search terms that the user entered into any internet search engine, and records of user-typed web addresses; records evidencing the use of the IP addresses to communicate with the [victim's bank's] e-mail servers; evidence of who used, owned, or controlled the TARGET COMPUTER at the time things described in this warrant were created, edited, or deleted, such as logs registry entries, configuration file, saved user names and passwords, documents, browsing history, user profiles, e-mail contents, e-mail contacts, 'chat,' messaging logs, photographs, and correspondence; evidence of software that allow others to control the TARGET COMPUTER was used; and records of applications run.

Three significant questions were raised: (1) exceeding territorial limits of a Rule 41 search warrant, (2) failure to comply with the Fourth Amendment's particularity requirements and (3) compliance with Fourth Amendment video surveillance using the computer's attached camera.[65] Exceeding a warrant's territorial scope was crucial to the judge's rejection of the government's argument that territorial limits would be satisfied so long as the property (ESI) would 'be examined in this judicial district.'[66] The judge re-cast this justification as follows:

> '... because its agents need not leave the district to obtain and view the information gathered from the Target Computer, the information effectively becomes "property located within the district"... [thus rejecting it because]... a Rule 41 warrant would permit FBI agents to roam the world in search of a container of contraband, so long as the container is not opened until the agents haul it off to the issuing district.'[67]

The legality of using such 'Trojan Horse' warrants to conduct remote searches is suspect. However, Professor Brenner argues that Trojan Horse programs to remotely search U.S. citizens' computers does not violate the search and seizure protections if the search warrant authorizes a remote investigation or a valid exception to the warrant requirement exists (e.g., exigency).[68] This line of reasoning would enable remote and surreptitious examination of citizens' computers. The fruits of such investigations would therefore constitute admissible evidence in criminal prosecutions. Such a situation differs 'wildly from the searches with which the drafters of the Fourth Amendment were concerned.'[69]

62 *Fed. R. Crim. P. 41(C) and (D).*
63 *In re Warrant to Search a Target Computer at Premises Unknown, No. H-13-234M, United States District Court, S.D. Tx (April 22, 2013) (denying application for warrant in part because the location of the targeted computer was unknown).*
64 *In re Warrant to Search a Target Computer at Premises Unknown, at 1.*
65 *In re Warrant to Search a Target Computer at Premises Unknown, at 2.*
66 *In re Warrant to Search a Target Computer at Premises Unknown, at 2.*
67 *In re Warrant to Search a Target Computer at Premises Unknown, at 2.*
68 *Susan W. Brenner, ' Remote Computer Searches and the Use of Virtual Force' , 81 MISS. L.J. 1229 (2012).*
69 *Susan W. Brenner, ' Remote Computer Searches and the Use of Virtual Force' , at 6 (citations omitted). The author she describes is herself.*

The international dimensions of such Trojan Horse tactics are also significant.[70] 'Dissonance' between states and nation-states with differing search and seizure standards seems likely.[71] The most severe case is arguably where the search authorizing state or nation permits Trojan Horse intrusions but the target jurisdiction, where the data is located, does not. The authorizing jurisdiction might argue the search occurs within its boundaries while the target jurisdiction would have a strong argument that the seizure occurred in the target's territory, but might expand that to include the actual search also occurred within the target's boundaries.

A taxonomy developed by Professor Brenner suggests the following uncertainties about an Idaho warrant to search an Ohio computer:

> 'Did the search therefore occur (i) 'in' Ohio because that is where the target of the search was located, (ii) 'in' Idaho because that is where the searchers were located or (iii) in both? This issue does not arise with traditional, non-remote searches because the searchers and the target(s) of the search are necessarily physically proximate while the search takes place. With cyberspace, the search dynamic can be altered, so physical proximity is no longer inevitable.'[72]

If trans-border wiretapping of telephony is the governing analogy, taken from the U.S. federal standard, then 'the communication is "intercepted" where the tapped phone is located *and* where the "listening post" is located.'[73] It seems likely that the party seeking to suppress the introduction of ESI acquired in such a Trojan Horse search would have a strong argument if the state or nation where the process originates prohibits searches outside its borders.

Modifying ECPA to enable location-based search authority

ECPA and its SCA component[74] permits access to certain types of communications when stored with certain public providers. These provisions are a complex legal morass.

If ESI is not covered under ECPA, then traditional Fourth Amendment principles apply to search and seizure of that ESI. ECPA jurisprudence has expanded search and seizure capability for the U.S. states by empowering state courts to require law enforcement to acquire certain ESI outside that state's boundaries. Indeed, it is generally acknowledged that U.S. state courts cannot order that state's law enforcement to acquire from repositories physically located in other states.[75] ECPA expands the traditional state boundary limits under revisions enacted following 9.11 in the USA Patriot Act.[76] The USA Patriot Act expands extra-territorial search powers to state and local prosecutors by adding them to the term 'court of competent jurisdiction.'[77] As the American Prosecutors Research Council eloquently explains:

> 'The Patriot Act specifically amended Section 2703(d) of the ECPA to authorize state courts of "competent jurisdiction" to issue legal process under various sections of the ECPA unless "prohibited by the law of such State." §2711(3) defines a "court of competent jurisdiction" to issue legal process to include a court as defined by 18 U.S.C. §3127. Section 3127(2)(B) states "a court of general criminal jurisdiction of State authorized by the law of that State to enter orders authorizing the use a pen register or a trap and trace device." Thus, state and local prosecutors can use the ECPA to obtain, from their own state courts, legal process for collection of e-mail information and e-mail.'[78]

Under this ECPA interpretation, a state court uses the power from the Federal statute to compel production of certain ESI from sources outside their respective state lines. There are other federal statute expansions of state powers.[79]

Cloud computing raises particular problems in ESI acquisition under ECPA. Arguably, this requires a major revision of the statute. Georgetown Adjunct Professor Marc J. Zwillinger set forth five reasons why cloud computing calls for a revision to the ECPA:[80]

70 *Susan W. Brenner, 'Law, Dissonance and Remote Computer Searches', 14 UNIV. N. CAR. J.O.L.T. (2012).*
71 *Susan W. Brenner, 'Law, Dissonance and Remote Computer Searches'.*
72 *Susan W. Brenner, 'Law, Dissonance and Remote Computer Searches' at fn. 104.*
73 *Susan W. Brenner, 'Law, Dissonance and Remote Computer Searches', citing United States v. Denman, 100 F.3d 399, 403-04 (5th Cir. 1996).*
74 *18 U.S.C. Sect. 2701, and following.*
75 *For example, see Pa. R. Crim. P. §200, which states: 'A search warrant may be issued by any issuing authority within the judicial district wherein is located either the person or place to be searched.'*
76 *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, Pub. L. No. 107-56, 114 Stat. 272 (26 October 2001).*
77 *'The ECPA, ISPs and Obtaining E-mail: A Primer for Local Prosecutors', American Prosecutors Research Institute, Bureau of Justice Assistance (July, 2005), 3.*
78 *'The ECPA, ISPs and Obtaining E-mail: A Primer for Local Prosecutors', at 7.*
79 *18 U.S.C. §2703(e). Another argument might combine the U.S. Constitution's Commerce and Supremacy Clauses to expand state court jurisdiction.*
80 *'Electronic Communications Privacy Act and the Revolution in Cloud Computing: Hearing Before the Subcommittee on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary', 111th Cong., September 23, 2010 Serial Number 111-149 (Statement by Adjunct Professor Marc J. Zwillinger), 118-120, available at http://judiciary.house.gov/hearings/printers/111th/111-149_58409.PDF.*

1. For materials such as e-mails or private messages that are intended to be the most protected, the definition of 'Electronic Storage' is difficult to apply'.
2. The 180 day rule is arbitrary and based upon a false assumption.
3. Congress intended content to be more protected than transactional records in theory, but in practice content does not get enough protection.
4. The SCA is not technology neutral.
5. The complete silence on access by civil litigants, criminal defendants and estates of deceased users creates uncertainty and unnecessary litigation.[81]

The ECPA expands state seizure powers, but its labyrinth of exceptions and inane rules need revision. For example, the ECPA empowers the state to order disclosure of e-mails opened just a few days old via the ECPA provisions. However, that same state would be forced to apply for and obtain a search warrant in another state where those same e-mails were downloaded to a computer user's computer located there.

If consent is absent, a state court order compelling acquisition of remotely accessed ESI stretches the jurisdictional limits of current state law. Cloud forensics involves obtaining access to computer systems. At present, it is uncertain whether state courts may mandate search and seizure (remote search), when the ESI is located outside their jurisdiction using a computer located within their jurisdiction. While computer forensics has long utilized these technologies to remotely acquire evidence through a network, the authority of a court to order and compel law enforcement is analogous to ordering an officer to go out of state to seize evidence, a practice not generally allowed without the cooperation of local law enforcement. Similar territoriality problems are inherent in international cloud forensics. At both civil and criminal levels, crossing borders implicate the other sovereign state's laws.

Assume this scenario: a state court a issues search warrant to search a folder stored in the 'cloud' by a CSP. The folder contains both communications and documents. The folder is clearly accessible through the computer located in Pennsylvania, being mapped as a drive thereon. Would such a search be legal? An initial question is: who is the target? The U.S. Fourth Amendment does not apply to non-citizens if the search is conducted outside the U.S. At least one U.S. case exemplifies this position.[82]

In 1999, the U.S. Federal Bureau of Investigation (FBI) unsuccessfully sought assistance from Russian authorities to detain a suspected hacker, Alexey Ivanov who had allegedly intruded into 'the computer systems of businesses in the United States' to steal financial information and engage in extortion allegedly threatening public disclosure and embarrassing exposure. The FBI resorted to an undercover operation to lure Ivanov and his partner Vasiliy Gorshkov, to Seattle for a promised interview with a telephone company, Invita. The Russians demonstrated their hacking skills using Invita computers, not knowing the FBI had installed key loggers to record keystrokes. Their credentials (usernames and passwords) were used to obtain access to the Russian computers remotely from the U.S. and download 250 gigabytes of their data. The Russians were arrested and indicted. When the Russians attempted to suppress the ESI as evidence in their prosecution, the U.S. Supreme Court affirmed the District Court that the U.S. 'Fourth Amendment does not apply to searches. . . search[es] and seizures seizur[es] of a non-resident alien's property outside . . . the United States.' As non-resident aliens and the search made on a server on Russian soil, the search was entirely in Russia.

Thus, when the target is a foreign national, the remote search would not violate the Fourth Amendment because it does not apply to aliens and for searches conducted on foreign soil. However, this does not address the ESI of U.S. citizens located on foreign soil, a scenario that describes perhaps a majority of cloud ESI search and seizure potential in the modern environment.

There may be laws other than ECPA and SCA that would prohibit remote searches. In 'Law Enforcement Challenges in Transborder Acquisition of Electronic Evidence from "Cloud Computing Providers"',[83] Professor Schwerha outlined some of the legal difficulties posed by the Council of Europe's Convention on Cybercrime, which the United States has signed and ratified. While the convention does not function as a domestic U.S. law, it could act as an argument as to how to interpret U.S. law because when the U.S. ratified the same, it essentially verified that its laws were in harmony with the articles set forth in the Convention. That discussion paper primarily addresses the existing problems with acquiring ESI

81 *'Electronic Communications Privacy Act and the Revolution in Cloud Computing: Hearing Before the Subcommittee on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary', 118-120.*

82 *Susan W. Brenner, 'Law, Dissonance and Remote Computer Searches', 14 North Carolina Journal of Law & Technology 1 (2012), 43-92.*

83 *J. Schwerha, 'Law Enforcement Challenges in Transborder Acquisition of Electronic Evidence from 'Cloud Computing Providers",' Council of Europe, Project on Cybercrime (Strasbourg, 15 January 2010).*

internationally from SCPs. The primary section of the Convention on Cybercrime applicable to transborder searches is article 32, which states as follows:

> Article 32 – Trans-border access to stored computer data with consent or where publicly available a Party may, without the authorization of another Party:
>
> a. access publicly available (open source) stored computer data, regardless of where the data is located geographically; or
>
> b. access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.'

Articles 31, 33 and 34 also deal with transborder acquisition of evidence, though only with cooperation. Article 32 primarily covers remote searches. Cloud computing provides various challenges:

> 1. It is impossible to know where the sought after data resides;
>
> 2. If you do not know where the data resides, then you cannot determine what laws apply;
>
> 3. The idea that the investigating officer may have to get consent brings about numerous other difficulties;
>
> 4. If the investigative authority searches the computer possessed by a suspect that utilizes the services of a Cloud Computing Provider, then any data obtained there from might be meaningless; and
>
> 5. There could be significant difficulties in admitting the evidence obtained from a Cloud Computing Provider.

Thus, it is very hard to recognize a clear solution for making cloud forensics universally legal without staying within a single jurisdiction. Curiously, many people would practice due diligence before buying property or starting a business in an unfamiliar state or country with unfamiliar laws. But, increasing numbers of people show little self-restraint in storing their valuable data in whatever state, nation or jurisdiction chosen by their 'free' on-line storage provider.

Are there solutions?

The law traditionally adapts to new technologies somewhat more slowly than the technologies change. The car and telephone ushered in big changes, eventually resulting in the development of whole fields of new law. The most significant legal challenge posed by cloud forensics is that the internet fails to respect borders, at least most of the time. It may be 'cool' and exciting to have immediate, ubiquitous and authorized access to one or more computers from another country at any one time. However, inherent procedural difficulties are created by the physical, cultural and legal barriers to cloud forensics, in civil, regulatory and criminal procedural contexts, both domestically and internationally.

Solutions should move away from traditional geographic boundaries as the method of determining legality. Perhaps some sort of minimum contacts analysis under the watershed U.S. Supreme Court case *International Shoe* might guide how, whether and when remote acquisition is appropriate.[84] This might be affected as part of the initial scheduling conferences for trials, or like a temporary restraining order (TRO) hearing for evidence. A standard might require a showing that the party seeking remote access could prove there is a likelihood that the evidence sought is relevant, and that the least intrusive and successful method would be direct acquisition via a cloud forensic tool. Similar such hearings authorize evidence acquisition by the U.S. Marshal in Federal civil cases. Criminal courts also have a long history of considering the propriety of allowing compelled acquisition of evidence through applications for warrants and other procedural mechanisms.

Perhaps the data, not the repository's owner, sub-contractor or server, must have had some minimum contacts with the jurisdiction seeking its acquisition remotely. Therefore, if the data had been utilized in commerce previously within that court's jurisdiction, the test of within the boundaries would be met. For example, assume a plaintiff wants access to files the defendant has remotely stored in another nation. Perhaps, the defendant counters it is limited by CSP contract to read-only access by the defendant's wholly-owned subsidiary. Under this set of facts, a court could determine that once the data had been used in the forum court's jurisdiction, an inherent right exists to review that data as part of the

84 *International Shoe Co. v. Washington, 326 U.S. 310 (1945).*

pending proceedings.

However, it might require new laws to authorize law enforcement (criminal) or the courts (regulatory, civil) to make production, search and seizure mandatory because that data was stored on or was accessible through a computer system within the jurisdiction. Perhaps that translates to mandatory domestic back-ups for data stored remotely. Database registration, not unlike the requirement in the European Union that every organization processing personal data is required to notify the relevant authority, might also enable access rights under service of court process (i.e. subpoena, warrant). The concept of geographically-based jurisdiction must be reexamined at the domestic level. Defining search as the acquisition of evidence via a computer from within the jurisdiction of the court could then lead to the principle of remote acquisition of ESI from that computer being properly authorized.

Conclusion

Technological evolution continually challenges existing law. However, the evolution of the law typically lags behind technology development, relegating law to play a perpetual catch-up role. The development of the cloud as a ubiquitous storage repository and software ('app') service provider fundamentally changes the relationships between users and suppliers of software and hardware. The cloud reinforces the need for reliable connectivity and fundamentally changes the software business model from unlimited use under purchased license to 'pay per use' when software is provided as a service (SaaS). Of course, the risks of exploitation from this lock-in must be weighed against the enormous economic pressures to save capital expense by moving to the cloud and enable more work from mobile devices. Cloud and SaaS are actively marketed for immediate cost savings, promised benefits of productive work anywhere, and to attain the benefits of quick shifts in demand through the seemingly unlimited ability of the cloud to deal quickly with increasing demand.

Expanding functionality of computing equipment in general and mobile devices in particular is clearly evident. Law must be flexibly drafted to accommodate rights given such transformational technologies. No longer should statutes, regulations and case law assume existing technology will continue unchanged for any foreseeable future. Instead, law should be intentionally written to address both the contemporary problem at hand while retaining flexibility to adapt as technology evolves. Of course, this is challenging, particularly for the constitutionality of penal statutes that must be fairly precise. Nevertheless, the future of design, functionality, ownership and use should be considered in drafting opinions, regulations and statutory language. Legislative history has always been a useful source of such forward-looking adaptability. Similarly, general and enduring principles, sometimes composed as elements, enable stable precedents. Flexible law can adapt to changing technology more readily than overly detailed specifications that are technology-specific.

The case of mobile devices such as smart phones makes a compelling case for both flexibility and a functional rather than a design orientation in defining rights, duties, and prohibited behaviours. Miniaturization, a corollary to the increasing storage capacity represented in Moore's Law,[85] made mobile device computing power increases inevitable. The geolocation revolution spurred on by global positioning services (GPS) but now enhanced with other technologies (e.g., cell triangulation, RFID) may have been less foreseeable than miniaturization. Privacy law lags behind the use of location-based advertising architectures significantly, and so many users remain unaware of the privacy issues that the law may be unable to reclaim such privacy rights.[86]

Document retention policies are always challenging. Three major incentives coalesce to place pressure on the need for official policies, and these are too often not well followed in practice. First, there are increasing business reasons for data retention. The major function of information sciences, the management of information systems and the search disciplines are to expand the usefulness of data mining and analysis, a form of sense-making.[87] Second, various statutes require data retention of fairly specific types of documents for generally specific durations. Third, retained data may expose its owner, author and others implicated thereby to litigation risks when that data concerns wrongdoing. One argument is that these new and expansive repositories of data may increase data availability for useful and mandatory purposes but it also increases exposure to the risk of liability. Under this argument, transition to the cloud is unlikely to reduce exposure to risk derived from revelations that a party might be to blame.[88]

Of course, if CSPs expressly or impliedly promise

85 *See generally Sally Adee, ' the data: 37 Years of Moore' s Law' , 45 SPECTRUM 56, IEEE (May 2008).*

86 *See generally Andrew J. Blumberg, and Peter Eckersley, ' On Locational Privacy, and How to Avoid Losing it Forever' (August 2009) available at https://www.eff.org/wp/locational-privacy.*

87 *K. A. Taipale, ' Data Mining And Domestic Security: Connecting The Dots To Make Sense Of Data' , 5 Colum. Sci. & Tech. L. Rev. 2 (2003).*

88 *Scott Zimmerman and Dominick Glavach, Cyber Forensics in the Cloud, 14 IANEWSLETTER 4 (Winter 2011).*

document destruction when convenient to avoid embarrassment of liability, then the cloud itself may destroy some evidence. Cloud services are so frequently hosted in other jurisdictions or other nations, that discovery, investigations and forensics may actually be obstructed more effectively. Indeed, the international aspects of cloud computing are daunting. Without robust and enforceable memoranda of understanding (MOU) for law enforcement cooperation, it will become difficult to discover or forensically investigate any files stored outside the nation of litigation. Thus, an individual person's files as well as business records held in the cloud might regularly elude law enforcement, regulators and opposing civil litigants.

In sum, the increasing adoption of cloud services imposes vast new challenges to criminal law enforcement, regulatory enforcement and civil litigation. Cloud data may be impossible to delete, but forensic techniques and jurisdiction of most tribunals is not sufficiently well-defined yet to assure use of cloud data effectively in legal proceedings. But then hiding incriminating data on 'another planet' may actually be a smart strategy.

Professor John W. Bagby and **Associate Professor Joseph J. Schwerha** are members of the editorial board

