INFORMATION LAW JOURNAL

A Publication of the Information Security and EDDE Committees
ABA Section of Science & Technology Law

WINTER 2017 VOLUME 8 ISSUE 1 EDITOR/FOUNDER: THOMAS J. SHAW, ESQ.

New Books on Emerging Technologies Law and Information and Internet Law

By Thomas J. Shaw

Two new legal technology books were published this month, comprehensively addressing the areas of global emerging technologies law and information and Internet law. These books analyze the legal implications of more than 30 emerging technologies, the processing of information, and the use of the Internet, *Read more*

Conflicting Document Production Laws May Result in International Discovery Restrictions

By Courtney Lotfi

Irrespective of the nature of the dispute or the forum in which it is pending, it is a fundamental principle that the party with the burden of proof must carry it in order to succeed. As a general rule, the claimant (plaintiff) carries the burden of proof and the respondent (defendant) will be absolved if the claimant cannot meet *Read more*

The Independent Chief Data Officer: A Weapon in the Arsenal of Information Security

By Michael Aisenberg

Some might question why or how the U.S. Intelligence Community (IC) can be offered as a model, or at least case study in cyber security and associated issues of organizational policy. But recent developments within the IC in the area of Infonomics and data management and security offer some important anecdotal *Read more*

Considerations Governing the Lifting of a Litigation Hold in Civil and Criminal e-Discovery

By Alec Webley, Alexander Hastings, and Edward Rippey

Well known is the rule that, once litigation is anticipated, all relevant documents typically must be retained. This is done primarily by means of the "litigation hold," a notice suspending an organization's usual document deletion policies and instructing employees to retain any documents relevant to the lawsuit. But, *Read more*

Executive Order 12333, the President-Elect, and the NSA

By April Doss

It's no secret that the national security community has been uneasy with candidate Trump, with many of its most esteemed leaders forming vocal, passionate parts of the #NeverTrump movement. In fact, in Aug. 2016, a group of prominent national security experts – all of whom had served as Republican political *Read more*

Blockchain Risk Factors in Securities Offerings and Filings

By Bo Harvey and John Servidio

The hype around bitcoin and similar digital currencies appears to be making way for similar enthusiasm over the underlying distributed ledger technology, or blockchain, that facilitates delivery and payment of digital currency transactions. Banks, financial intermediaries, financial technology startups and regulators are *Read more*

New Books on Emerging Technologies Law and Information and Internet Law

By Thomas J. Shaw

Two new legal technology books were published this month, comprehensively addressing the areas of global emerging technologies law and information and Internet law. These books analyze the legal implications of more than 30 emerging technologies, the processing of information, and the use of the Internet, presenting statutes, standards, guidance, cases, and legal ethics opinions from the U.S. and EU comparatively, along with Asia-Pacific and the Americas ex-U.S. Completely current up to the dates of publication, the books work together as a companion set.

The books' intended audience are lawyers new to emerging technologies, information, or Internet law including graduate and undergraduate law students, lawyers wanting to understand the latest developments in emerging technologies, information, and Internet law, lawyers who would like a single source describing and analyzing emerging technologies, information, and Internet law, and lawyers needing a global comparative approach to emerging technologies, information, and Internet law.

Emerging Technologies Law – Global Practice analyzes the U.S. and EU guidance, statutes, standards, cases, and ethics opinions for more than 30 emerging technologies, explaining the law that currently exists while also noting unsettled issues for future resolution. It starts by presenting a brief history of how technology and the law have interacted through the last few centuries and a framework for understanding the legal impacts of any emerging technology. The next six chapters discuss the following emerging technologies: social media, mobile computing, BYOD, cloud computing, digital identity, digital authentication, biometrics, critical infrastructure, smart grids, smart meters, the Internet of Things (including smart homes, smart cities, industrial Internet, connected cars, driverless cars, smart appliances and televisions), Big Data, virtual currencies, distributed ledgers, electronic health records, telemedicine, robots, artificial intelligence, virtual reality, 3D printing, wearables, mobile health devices, drones, augmented reality, and mobile payments.

Information and Internet Law – Global Practice provides insight by looking at the current statutes, regulations, and directives in the United States and Europe, supplemented by statutes in Asia and the Americas ex-U.S. It discusses and identifies issues raised by the latest U.S. and EU cases on protection of information and use of the Internet. It starts with an explanation of risk for lawyers and a risk-based, lifecycle approach to information and Internet law. The areas of information law addressed are privacy, information security, and data protection law across the world, unlawful data disclosures through cybercrime and data breach, and lawful data disclosures related to messaging and surveillance activities. The areas of Internet law analyzed are access including equal access, jurisdiction, speech, intermediary liability, intellectual property on the Internet, e-commerce, and website agreements.

Thomas J. Shaw, Esq. *is a globally-based attorney at law, CPA, CIPP/Europe, CIPP/US, CRISC, ECM[M], CISM, ERM[P], CISA, CGEIT and CCSK, asst. professor of emerging technologies, information, and Internet law at leading universities, and author of the books* Emerging Technologies Law – Global Practice (2016), Information and Internet Law – Global Practice (2016), World War I Law and Lawyers – Issues, Cases, and Characters (2014), Cloud Computing for Lawyers and Executives - A Global Approach, Second edition (2013), World War II Law and Lawyers – Issues, Cases, and Characters (2013), Children and the Internet – A Global Guide for Lawyers and Parents (2012), Cloud Computing for Lawyers and Executives – A Global Approach (2011), *lead author/editor of* Information Security and Privacy – A Practical Guide for Global Executives, Lawyers and Technologists (2011), *and editor/founder of this publication and its antecedents. He runs DPO Services, providing Data Protection Officer functions for U.S. and foreign firms required to comply with the EU's new General Data Protection Regulation and can be reached at thomas@tshawlaw.com.*

Conflicting Document Production Laws May Result in International Discovery Restrictions

By Courtney Lotfi

Irrespective of the nature of the dispute or the forum in which it is pending, it is a fundamental principle that the party with the burden of proof must carry it in order to succeed. As a general rule, the claimant (plaintiff) carries the burden of proof and the respondent (defendant) will be absolved if the claimant cannot meet that burden. By raising an objection or pleading a defense, the respondent becomes the claimant and must, in turn, carry its burden. Thus, claimants must prove their claims and defendants must prove their defenses, counterclaims, or set-off rights.[1]

The role of documentary evidence is paramount in most proceedings. Documents, contemporaneous or otherwise, assist the parties in determining, developing, and testing the nature of their claims and defenses, they can influence and shape procedural considerations from the outset and, when submitted as evidence, they can aid in substantiation.

In an increasingly global and multinational world documents that may be relied upon during proceedings, regardless of whether they are produced as evidence, may contain an international component. For example, they may be in the possession of a foreign party or may have originated abroad. The note that follows addresses the potential conflicting national laws that may apply in litigation and international arbitration with respect to discovery (often termed "disclosure" abroad) and how these conflicts may limit or curtail the broad approach to discovery employed in the United States.

Common and Civil Law Jurisdictions Employ Vastly Different Approaches to Discovery

The United States ("US") is a common law jurisdiction with broad rules for lawyer-driven pretrial discovery of information. Documents and things in the possession of the opponent are traditionally obtained through requests for production, a pre-trial discovery tool which enables parties to a dispute to seek discovery of non-privileged matters relevant to a party's claim or defense.

Until the 2015 amendment, the Federal Rules of Civil Procedure ("FRCP") permitted discovery of information relevant to claims or defenses or, upon a showing of good cause, to the broader "subject

[1] *See, e.g.,* JEFFREY WAINCYMER, PROCEDURE AND EVIDENCE IN INTERNATIONAL ARBITRATION 763 (2012); Courtney Lotfi, *Documentary Evidence and Document Production in International Arbitration*, in YEARBOOK ON INTERNATIONAL ARBITRATION, Vol. IV 100 (Marianne Roth & Michael Geistlinger eds., 2015).

matter" of the litigation. In addition, many courts and practitioners understood that information was discoverable if it appeared "reasonably calculated to lead to the discovery of evidence."[2]

The scope of discovery was somewhat curtailed in 2015 when FRCP Rule 26 was amended to eliminate discovery of the "subject matter," remove the "reasonably calculated" language, and place a heightened emphasis on proportionality. Currently, parties to federal court litigation in the United States may "obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense and proportional to the needs of the case."[3] Despite these curtailments, several courts have continued to rely on outdated formulations,[4] and the revised Rule continues to permit discovery of information even if it is not admissible.[5]

Requests for production in US federal court litigation need not be specific and need only describe with reasonable particularity each item or category of item sought.[6] While it has been common to request "any and all documents related to…," several commentators (including some judges) have suggested that this will no longer be tolerated as it is inconsistent with the important notion that discovery must be proportional to the needs of the case.

Given the broad discovery available in US federal court litigation, parties to a pending or threatened action often must preserve, collect, process, and prepare to produce all relevant information in their possession or control that is responsive to requests. This obligation applies to foreign parties subject to US jurisdiction, and can extend to foreign subsidiaries or affiliates of parties in US litigation. Under the FRCP, federal courts can order the production of documents from abroad.[7]

This party driven approach to discovery is unique in its liberal approach and, until recently, somewhat limited judicial oversight, particularly when compared to civil law jurisdictions.[8] Most civil law jurisdictions in contrast do not permit party-initiated or other forms of discovery.[9] Evidence taking in inquisitorial systems is subject to strict judicial oversight,[10] with parties having little to virtually no right to demand relevant materials from the opponent.[11] The taking of evidence is generally considered the

---

[2] Fed. R. Civ. P. 26(b)(1).
[3] Fed. R. Civ. P. 26(b)(1); Chief Justice John G. Roberts, Jr. 2015 Year-End Report on the Federal Judiciary, *available at https://www.supremecourt.gov/publicinfo/year-end/2015year-endreport.pdf.*
[4] *See In re Bard IVC Filters Prods. Liab. Litig.*, 2016 WL 4943393 (D. Ariz. Sept. 16, 2016).
[5] Fed. R. Civ. P. 26(b)(1)("Information within this scope of discovery need not be admissible in evidence to be discoverable.").
[6] Fed. R. Civ. P. 34(b)(1)(A).
[7] *See* Lawrence W. Newman & David Zaslowsky, *The Conflict in Production of Documents from Abroad*, 244/15 N.Y.L.J. 1 (Jul. 22, 2010); *see also Societe Nationale Industrielle Aerospatiale v. U.S. Dist. Ct. S.D. Iowa*, 482 U.S. 522 (1987); *Int'l Soc'y for Krishna Consciousness, Inc. v. Lee*, 105 F.R.D. 435 (S.D.N.Y. 1984).
[8] *See, e.g.*, Timothy P. Harkness et al, *Discovery in International Civil Litigation: A Guide for Judges* 1 (2015), *available at* http://www.fjc.gov/public/pdf.nsf/lookup/Discovery-in-International-Civil-Litigation.pdf/$file/Discovery-in-International-Civil-Litigation.pdf; GARY B. BORN, INTERNATIONAL COMMERCIAL ARBITRATION 1894 (2009).
[9] Born, *supra* note 9 at 1893.
[10] *See, e.g.*, Harkness, *supra* note 9 at 1.
[11] Born, *supra* note 9 at 1893.

sole prerogative of the state in connection with trials (or investigations), and pre-trial discovery is largely precluded.[12] In those limited circumstances where obtaining documents from a counterparty is permitted in civil law jurisdictions, a court order is usually required and will only be granted if the sought-after document can be named, its contents described in sufficient detail, possession by the other party is established, and legal grounds for production are present.[13]

These distinctions in the domestic approaches to document production must be borne in mind in instances where data and information could be sought from a foreign jurisdiction, as must the distinction between the classification of the burden of proof, which invariably influences approaches to discovery and production.[14]

Data Protection Laws and Blocking Statues in the European Union Restrict the Transfer of Personal Information for the Purposes of US Litigation

The European Union ("EU") considers the protection of personal data a fundamental human right and has enacted privacy laws aimed at restricting cross-border processing and transfer of data or information for use in foreign jurisdictions.[15] This has been accomplished through the use of (i) data protection laws, which prohibit transmission of data capable of identifying a person (such as name, address or identification number) to non-participating jurisdictions, and/or (ii) blocking statutes, which restrict the transfer of information and documents for use in foreign proceedings.[16]

The EU Data Privacy Directive 95/46 has provided the framework for the implementation of data protection laws by member states.[17] It defines personal data as "any information relating to an identified or identifiable natural person."[18] This broad definition includes "all communications containing a name, address, identification number, or other identifying information such as information within a To/From/CC field of an e-mail or memos."[19] Production of sensitive personal data – information on racial or ethnic origin, political opinion, religious and philosophical beliefs, trade-union membership, and data concerning health and sex life – is prohibited.[20]

---

[12] *See* Kurt Heller & Thomas Kustor, *Constitutional Law, The Judicial System and Administration*, in AUSTRIAN BUSINESS LAW: LEGAL, ACCOUNTING AND TAX ASPECTS OF BUSINESS IN AUSTRIA (Kurt Heller et al. eds., 2008, 19th Suppl.).

[13] *See* German Code of Civil Procedure (*Zivilprozessordnung*), Section 142; French Code of Civil Procedure (*Code de procedure civile*), Articles 11, 145; Italian Code of Civil Procedure (*Codice di procedura civile*), Article 210.

[14] Waincymer, *supra* note 2 at 765 (citing MATTI KURKELA & HANNES SNELLMANN, DUE PROCESS IN INTERNATIONAL COMMERCIAL ARBITRATION 41 (2005)(Civil law legal systems tend to consider the burden of proof substantive while common legal systems consider it procedural.)).

[15] *See* Lawrence W. Newman & David Zaslowsky, *The Conflict in Production of Documents from Abroad*, 244/15 N.Y.L.J. 1 (Jul. 22, 2010).

[16] *See* Harkness *supra* note 9 at 24-25.

[17] *Id.* at 25.

[18] *Id.* (quoting Council Directive 95/46, art. 2(a), 2005 O.J. (L 281) (EC), available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML).

[19] *Id.*

[20] *Id.*, *see also* Council Directive 95/46, art. 8, 2005 O.J. (L 281) (EC).

Implementation of data protection among member states has taken several forms. In Germany, for example, the Federal Data Protection Act (*Bundesdatenschutzgesetz,* "BDSG") governs personal data privacy protection. It prohibits the transmission of personal data if the person concerned has a legitimate interest in withholding the personal data.[21] A legitimate interest exists when the level of data protection in the foreign jurisdiction is not equivalent to the level of protection provided in Germany.[22] The US has traditionally been designated as a country which provides an inadequate level of data protection by the European Commission in respect to Directive 95/46.[23] Thus, any transfer of personal data without consent of the individual or works council is a violation of the BDSG in the case of Germany, and could result in fines payable to the offended person – i.e., the individual whose data was "impermissibly retained, disclosed, or transferred,"[24] or up to a year in jail.[25]

A similar approach has been adopted in France, which also applies stringent data protection laws and blocking statutes. There, "no person shall comply with requests from U.S. courts based on or resulting directly or indirectly from a list of foreign laws purported to have extraterritorial application."[26]

A new framework was adopted by EU Commission on 12 July 2016 to provide clarity for businesses relying on transatlantic data transfers and to protect the fundamental rights of anyone in the EU whose personal data is transferred to the US.[27] Data can be transferred across the Atlantic under the new Privacy Shield; however, stringent data protection rules continue to apply.

US companies in receipt of personal data from the EU must process the information according to strong data protection rules and safeguards.[28] They must have a privacy policy in line with European Privacy Principles and must renew "membership" to the Privacy Shield on an annual basis.[29] Those in the EU have the right to, *inter alia*, be informed on the type of personal data possessed, the reason why, the company's intent to transfer the data.

---

[21] Harkness *supra* note 9 at 69-70; *see also* The Sedona Conference, *Germany, in* International Overview of Discovery, Data Privacy & Disclosure Requirements 100 (Axel Speis et al eds. Sept. 2009).
[22] Harkness *supra* note 9 at 70; BDSG, Section 4b, para 2(2).
[23] Harkness *supra* note 9 at 70.
[24] *Id.* at 25.
[25] Section 43 of the BDSG provides: "Anyone who, without authorization… stores, modifies or communicates… any personal data protected by this Act which are not common knowledge shall be punished by imprisonment for up to one year or by a fine."
[26] Harkness *supra* note 9 at 67.
[27] *See The EU-U.S. Privacy Shield*, available at http://ec.europa.eu/justice/data-protection/internaitonal-transfers/eu-us-privacy-shield/index_en.htm. The new framework replaces the previously existing Safe Harbor agreement which authorized data transfers between the EU and US for more than a decade. The Safe Harbor agreement was invalidated by the European Court of Justice's decision in *Schrems v. Data Protection Commissioner* on October 6, 2015. *See Schrems v. Data Protection Commissioner,* ECJ Case No.l C-362/14, available at http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30d55dcd21cf05ea40af8af0dac3be832508.e34KaxiLc3qMb40Rch0SaxyKaNz0?text=&docid=172254&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=674772; *see also* ECJ Press Release No. 117/15, *The Court of Justice declares that the Commission's US Safe Harbour Decision is invalid*, available at http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf.
[28] *See The European Commission, Guide to the EU-U.S. Privacy Shield* 7 (2016).
[29] *Id.* at 8.

Critically, the Privacy Shield companies may only use personal data for the purposes for which it was collected or subsequently authorized.[30] "Using… [personal] data for a purpose that is incompatible with the original purpose is never allowed."[31] If the new purpose is "materially different" from the original purpose, the Privacy Shield company may only use the personal data if the person does not object or, in the case of sensitive data, if consent is obtained.[32] Companies must ensure personal data is "kept in a safe environment and secured against loss, misuse, unauthorized access, disclosure, alteration or destruction."[33] As evident from the restrictions placed on data transfers, these recent developments may have a significant effect on US litigation, particularly with respect to discovery.[34]

Treatment of European Data Protection Laws and Blocking Statues by U.S. Courts

In addition to evoking limitations on discovery recognized by the FRCP,[35] parties have sought to rely on stringent data protection laws as a basis for limiting discovery and access to documents in domestic litigation. US courts have typically relied on the Supreme Court case *Societe Nationale Industrielle Aerospatiale v. U.S. Dist. Ct. S.D. Iowa* and on the multifactor test set forth in the Restatement (Third) of Foreign Relations Law Section 44(1)(c) in determining whether to excuse parties from complying with discovery requests on the basis of foreign prohibitions (e.g. the disclosure of otherwise protected personal data).[36] This section advises

> a court or agency in the United States should take into account the importance to the investigation or litigation of the documents or other information requested; the degree of specificity of the request; whether the information originated in the United States; the availability of alternative means of securing the information; and the extent to which noncompliance with the request would undermine important interests of the United States, or compliance with the request would undermine important interests of the state where the information is located.[37]

---

[30] *Id.* at 10.
[31] *Id.*
[32] *Id.*
[33] *Id.* at 11.
[34] The Privacy Shield is not without its critics and has been challenged. *See, e.g.,* Reuters, *French Privacy Groups Challenge the EU's Personal Data Pact with U.S.*, FORTUNE (Nov. 2, 2016), available at http://fortune.com/2016/11/02/privacy-shield-pact-challenge/(reporting that French and Irish groups have challenged the adoption of the Privacy Shield by the European Commission).
[35] *See, e.g.,* FRCP Rule 26(b).
[36] Harkness *supra* note 9 at 28. The American Bar Association has also urged, where possible, that US courts "consider and respect, as appropriate, the data protection and privacy laws of any applicable foreign sovereign, and the interests of any person who is subject to or benefits from such laws, with regard to data sought in discovery in civil litigation." *See Urges State and Local Bars to Respect Foreign Laws on Data Protection and Privacy*, ABA House of Delegates, Midyear Meeting 2012 (Jan. 12, 2012), available at http://www.americanbar.org/news/abanews/aba-news-archives/2013/08/urges_state_and_loca.html.
[37] Restatement (Third) of Foreign Relations Law of the United States §442(1)(c)(1987).

Other factors which have been considered by some US courts include the severity of possible sanctions for disclosure, whether the foreign law prohibiting disclosure appears likely to be enforced against the party, and the motives of the blocking statute.[38]

US federal district courts have recognized foreign limitations on data transfers in applying the above.[39] For example, a motion to compel the production of documents in Europe was denied on the basis of EU Directive and German data protection law in *Salerno v. Lecia, Inc.*[40] Likewise, a preliminary injunction against enforcement of state statute which could infringe constitutional grant of federal authority over foreign affairs was granted in *Gerling Global Reinsurance Corp. of Am. v. Quackenbush* as a result of, *inter alia*, conflicting with European data protection laws.[41]

In contrast, other US federal district courts have declined to limit discovery on the basis of foreign data protection laws and blocking statutes even if requiring production would result in a violation of foreign law.[42] For example, the Southern District of New York required production of documents from abroad when it found that there was "no substantial reason to depart from the procedures set forth in the Federal Rules of Civil Procedure" in *In re Vivendi Universal, S.A. Securities Litigation*.[43] In *Vivendi* the court found that the United States had an "obvious" interest in the application of its procedural discovery rules when the action was pending in the United States, the plaintiffs' alleged violation of US law, and when the third party witness upon which the subpoena was issued was served in the United States. In contrast, and based on the evidence presented to the *Vivendi* Court, France was found to have "little interest in the enforcement of its Blocking statute" when the legislative history of the statute indicated that the statute was not "intended to be enforced against French subjects but was intended rather to provide them with tactical weapons and bargaining chips in foreign courts."[44] Other courts have found the same on substantially similar grounds in the past.[45]

Recent case law, however, reconfirms the reliance on *Societe Nationale* and the Restatement (Third) of Foreign Relations Law Section. Thus, when the United States District Court for the Eastern District of Louisiana was unable to conduct a full analysis of whether document production should be limited on the basis of foreign law after its review of the briefing, and the record and statements made by counsel, it ordered the production of a privacy log to help ascertain the type of information contained in the

---

[38] Harkness *supra* note 9 at 28-29.
[39] *Id.* at 26.
[40] *Salerno v. Lecia, Inc.*, 1999 WL 299306 (W.D.N.Y. Mar. 23, 1999).
[41] *Gerling Global Reinsurance Corp. of Am. v. Quackenbush*, 2000 WL 777978, at *9–10 (E.D. Cal. June 9, 2000)
[42] *See* Harkness *supra* note 9 at 25 (citing *Columbia Pictures Indus. v. Bunnell*, 2007 WL 2080419, at *12 (C.D. Cal. May 29, 2007)).
[43] *In re Vivendi Universal, S.A. Sec. Litig.*, 2006 WL 3378115, at *3 (S.D.N.Y. Nov. 16, 2006).
[44] *Id.*
[45] *Id.* (citing *Société Nationale Industrielle Aérospatiale v. United States District Court for the Southern District of Iowa, supra,* 482 U.S. at 544 n. 29; *Bodner v. Banque Paribas, supra,* 202 F.R.D. at 375;*Valois of America v. Risdon Corp., supra,* 183 F.R.D. at 348-49; *Rich v. KIS California, Inc.,* 121 F.R.D. 254, 258 (M.D.N.C.1988); *Adidas (Canada) Ltd. v. SS Seatrain Bennington,* 80 Civ.1911(PNL), 82 Civ. 0375(PNL), 1984 WL 423 at *3 (S.D.N.Y. May 30, 1984)).

requested personnel files. The court in *In re Xarelto (Rivaroxaban) Products Liability Litigation* premised its holding on the basis that "[a]n American court should employ all of the tools at its disposal before treading on the laws and policies of foreign nations. A privacy log is one such tool."[46]

Failure by a party to US litigation to disclose relevant information may result in sanctions such as contempt, dismissal or default, or may result in a finding of fact adverse to the non-disclosing / non-complying party.[47] Before doing so, however, "courts will typically consider the conflicted party's good faith effort to comply with the discovery requested (including requesting permission from local authorities to produce the evidence)."[48]

Conversely, compliance with the US discovery requests has resulted in attorney sanctions in Europe.[49]

Treatment of Data Protection Laws and Blocking Statues by International Arbitral Tribunals

Some have suggested that discovery and other evidence-taking powers of international tribunals should be limited to the powers available in local courts at the *situs* of arbitration.[50] Under this approach, broad requests for production could be made and granted if a liberal jurisdiction such as New York were the seat of arbitration given the approach applied to litigation in that jurisdiction. In instances where the seat of arbitration were in a jurisdiction which adopts a more restrictive approach to discovery, broad requests for production would be impermissible.[51]

The majority approach, however, rejects this suggestion and instead holds that international arbitration is not limited to national court legislation.[52] Instead, the procedural law of the arbitration, which is established by the arbitration legislation at the seat of arbitration, ordinarily gives effect to the parties' procedural autonomy and grants broad procedural discretion to the tribunal.[53] Thus, neither the substantive nor procedural laws of the seat of arbitration govern procedural aspects of the arbitration unless the parties agree.[54]

Document production in international arbitration has become more common even though the presumption is that parties will establish their case based largely on the documents within their possession.[55] In 2012 Queen Mary University study on international arbitration, 62% of respondents reported that more than half of their cases involved requests for document production. Seventy-four

---

[46] *In re Xarelto (Rivaroxaban) Products Liability Litigation,* 2016 WL 2855221 at *5 (E.D. La. May 16, 2016).
[47] Harkness *supra* note 9 at 29.
[48] *Id.*
[49] Newman & Zaslowsky *supra* note 16 at 2.
[50] *See* NIGEL BLACKABY, CONSTANTINE PARTASIDES ET AL, REDFERN AND HUNTER ON INTERNATIONAL ARBITRATION 181-82 (5th ed., 2009); Born *supra* note 9 at 1887.
[51] Lotfi *supra* note 2 at 104.
[52] Born *supra* note 9 at 1887.
[53] *Id.*
[54] Blackaby & Partrasides *supra* note 46 at 392.
[55] *See, e.g.,* NATHAN D. O'MALLEY, RULES OF EVIDENCE IN INTERNATIONAL ARBITRATION: AN ANNOTATED GUIDE 36, 38 (2012).

percent of common law lawyers and 21% of civil law lawyers reported that more than 75% of their cases involved requests for production.[56]

When requests for production are made in international arbitration, a middle ground between the broad common law and restrictive civil law standards is often adopted. The International Bar Association's Rules on the Taking of Evidence in International Arbitration ("IBA Rules"), adopted in 1999 and revised in 2010, have gained widespread acceptance within the community and are often applied in international arbitration either by explicit reference in procedural rules or *de facto* through practice.[57]

Under these rules, requests for production must be made with specificity and seek documents which are "relevant to the case and material to its outcome."[58] They cannot be in the possession, custody or control of the requesting party and must be assumed in the possession of the requested party.[59] To maintain a request for production under Article 3(3) of the IBA Rules, the request must contain:

> (a) (i) a description of each requested Document sufficient to identify it, or (ii) a description in sufficient detail (including subject matter) of a narrow and specific requested category of Documents that are reasonably believed to exist; in the case of Documents maintained in electronic form, the requesting Party may, or the Arbitral Tribunal may order that it shall be required to, identify specific files, search terms, individuals or other means of searching for such Documents in an efficient and economical manner;
>
> (b) a statement as to how the Documents requested are relevant to the case and material to its outcome; and
>
> (c) (i) a statement that the Documents requested are not in the possession, custody or control of the requesting Party or a statement of the reasons why it would be unreasonably burdensome for the requesting Party to produce such Documents, and (ii) a statement of the reasons why the requesting Party assumes the Documents requested are in the possession, custody or control of another Party.[60]

This approach is patently more restrictive than the broad discovery available under the FRCP in domestic US litigation. The distinction between Anglo-American practice and discovery in international arbitration is aptly described in the English case of *BNP Paribas v. Deloitte Touche LLP*, where differences between discovery and disclosure in relation to a London Court of International Arbitration ("LCIA") arbitration were discussed: "There is an important distinction between requiring documents

---

[56] *See* 2012 International Arbitration Survey: Current and Preferred Practices in the Arbitral Process at 20.
[57] *See* Lotfi *supra* note 2 at 105.
[58] IBA Rules on the Taking of Evidence in International Arbitration, Art. 3(3)(2010); *see also* ICC Publication 843 -Techniques for Controlling Time and Costs in Arbitration.
[59] *See* IBA Rules on the Taking of Evidence in International Arbitration, Art. 3(3)(2010).
[60] *Id.*

to be produced as evidence of some fact… and asking for disclosure to trawl through documents to see if they support the applicant's case."[61] International arbitration adopts the former and not the latter.[62]

Parties to international arbitration may seek to resist the production of documents on several grounds including attorney-client privilege, non-compliance with the requirements of the IBA Rules (if they are adopted), and privacy laws.

As is the case with litigation, the EU's stringent data protection laws may apply in international arbitration. Although Article 26(1)(d) of the EU's 1995 Directive permits the transfer of personal data if necessary or legally required to establish a claim or defense, such "legal claims" are subject to "strict interpretation" and may only be applied in "civil proceedings" if personal data has been requested pursuant to the Hague Convention.[63]

Experienced international arbitral tribunals often limit discovery. As a result, there is a minimal risk that a party's production of documents in international arbitration would violate data protection laws.[64] As a practical point, and to further minimize the risk, tribunals may issue confidentiality orders at the beginning of proceedings or permit redaction of potentially protected information.[65]

Courtney Lotfi *is counsel at Redgrave LLP where she provides advice and counsel to foreign clients on procedural and evidentiary issues in complex multinational litigations. Before joining Redgrave LLP she was a principal associate at Freshfields Bruckhaus Deringer LLP and focused her practice on international arbitration.*

[61] O'Malley *supra* note 51 at 38 (quoting *BNP Paribas v. Deloitte & Touche* [2003] EWHC 2874 (comm), para. 6, Court of Appeal Commercial Court, Case No. 2003/946).
[62] *Id.* at 38.
[63] *See* R. Doak Bishop & Thomas Childs, The Requirement of Fair and Equal Treatment with Respect to Document Production in International Arbitration 7-8, *available at http://www.kslaw.com/imageserver/KSPublic/library/publication/9-10IBAChilds.pdf.*
[64] *Id.* at 8.
[65] *Id.*

The Independent Chief Data Officer: A Weapon in the Arsenal of Information Security

By Michael Aisenberg

Some might question why or how the U.S. Intelligence Community (IC) can be offered as a model, or at least case study in cyber security and associated issues of organizational policy. But recent developments within the IC in the area of Infonomics and data management and security offer some important anecdotal points, if not lessons learned, for organizations managing data, and the legal and policy professionals who support them.

On November 21, 2016, Steven Prossser assumed the role as the second appointed Chief Data Officer (IC CDO) of the U.S. Intelligence Community (IC). Mr. Prosser reports to the Chief Information Officer of the U.S. IC (IC CIO), as did his predecessor, a widely respected, now retired data professional.

This appointment in a largely techno-bureaucratic role should normally be unremarkable, both as a matter of U.S Government operational practice and as a maturity indicator in the cyber security ecosystem, were it not for several collateral facts which do make it at least notable.

First, Mr. Prosser is the second IC CDO appointed in 2016; his predecessor as IC CDO served only a few months in his role before retiring at the end of a highly lauded career. Second, for now, at least, Mr. Prosser will, like his predecessor, report not to the Director of National Intelligence (DNI) but to one of the DNI's deputies, the IC Chief Information Officer. And third, the other 16 components of the U.S. intelligence community all have individuals serving in various capacities of "chief data officer" or similar roles, and convening together in a new, only recently chartered "IC Chief Data Officer Forum." Some of these individuals, like Mr. Prosser, report to their component agency CIO; others report directly to the agency head, or to other leadership roles. And fourth, there is presently no IC Directive, IC standard or other authoritative guidance that defines the roles and responsibilities or even reporting structure for the IC CDO

A key point for the casual observer is, therefore, that within the U.S. intelligence community, where arguably, data is THE most critical asset of the entity, and, like other agencies of government and in the data-dependent commercial community broadly, the role of data, the special nature of Big Data, and how to manage it across its entire life cycle, and the specific nature of the function to be responsible for addressing these questions is very much a work in progress.

Perhaps spurred in part by the IC's excruciating self-examination of data stewardship practices precipitated by the Snowden "revelations", but most certainly in part pre-dating that episode and reflecting the explosion in data in every data-engaged institution, including the IC, the practical implications for management of issues such as "what IS our data?", "what does it mean to us and our

mission an entity?", and "how should data be managed to optimize its asset value, support its utility and minimize its risks?" all have converged in a perfect storm of institutional complexity. These issues now vex any entity using and attempting to manage data—big or small, and have created an appetite for, indeed a necessity for the establishment of managers dedicated to the care and feeding of the organization's data-the CDO.

For the law, and especially for attorneys engaged in practices at the nexus of technology and law, these issues and their management pose a special challenge. Foremost among them are the bureaucratic decisions of architecture: where should the CDO reside institutionally?, to whom should it report?, and what is the scope of its roles and responsibilities?. There has evolved in the past decade since the first discussions of the CDO role a legion of research studies supporting a variety of business models for the CDO. While there are arguments across the waterfront of structural options, one—the CDO as peer of the CIO and other C-suite support to the CIO—offers a variety of beneficial attributes that make it a rational choice.

The arguments have organization foundation on at least four fronts, including legal authorities both in government and in commercial practice.

The emergence of massive data sets as critical assets (Big Data) and the growing reliance on external service providers (Cloud) place a high premium on those aspects of data management and structure which contribute to stability and reliable continuity of organizational operations. This is true in the IC, and it is true in business and other data dependent organizations.

While the capacity of the CDO role to contribute to needed stability and operational continuity is perhaps best described as "unproven", and it is not uncommon for the CDO to reside in and operate in the Chief Information Officer organization, for many entities, including those in government and in the IC in particular, this reflects the still forming understanding across 17 often heterogeneous agencies of how to address the reality of "data as an asset."

Location of the CDO within the CIO organization offers the benefit of a usually well-established existing institutional bureaucracy; but that may be at high price in terms of efficacy and real impact on utilizing data as an organizational asset. This becomes readily apparent if one drills down on the specific data stewardship functions of a mature CDO role.

The emerging "science" of *Infonomics* as it has been dubbed by its proponents takes an orthogonal view of data and its hygiene-in relation to the networks and other hardware typically associated with "IT". In advocating for the role of CDOs, Infonomics adherents address data NOT from its posture as an artifact running on the CIO's network infrastructure, but rather *as the critical asset of data dependent organizations*—the currency in a Big Data economy.

In spite of the structural variants for the CDO locus, and the critiques and outright detractors of various structural approaches, the weight of informed opinion is that *a C-suite function dedicated to the growing business role of advocacy for practices supporting the mission-linked elements of data management* has had, and will have an invaluable impact on the successful achievement of institutional objectives in any data-dependent organization.

What specifically does such a senior CDO do? If the CIO runs the network and IT systems—the infrastructure over which data moves, and the business managers acquire or generate the data which is the asset moving on that infrastructure, what is left for the CDO ?

In fact, much; in today's data dependent environment, "someone" must own responsibility for

the entire data life cycle—milestones, critical practices and risks. The CDO is typically charged with responsibility for understanding data creation, acquisition, ingestion, conditioning for discovery, registration in repositories, venues of use and analysis, tagging, dissemination/sharing, retirement and destruction, familiarity with the eclectic issues of Personally Identifiable Information and related privacy considerations, and issues stemming from Cloud use.

In government, especially national security-sensitive and IC agencies, add concerns with classification, foreign users of classified or sensitive data, consequences for non-US person data, FOIA, sharing of sensitive unclassified data with the private sector ("CUI"), the aggregation and compilation of data sets, and unique government limits on cloud practices.

In or out of government, the CDO must also be conversant with technical aspects of data architecture, often sharing responsibility for information assurance, data architecture or other functions often delegated to a Data Architects or Data Scientist.

These roles all combine into a knowledge base closely related to BUT unmistakably distinct from the responsibilities of the CIO.

For most organizations, that means that a CDO must be capable of advising and redirecting mission conduct regarding data stewardship, across data's entire life cycle—both as mentor and advisor to business generators and users of data, and as manager and master where necessary to assure proper conduct. The CDO must be capable of advocacy for the mission-rooted functions and value of data, perhaps in conflict with orthodoxies of network architecture or even security advanced by traditional CIOs. This advocacy for "the mission" might include the relationship to the data's existence as THE artifact moving on the electronic network managed by the CIO, and thus, the very rationale and *raison d'etre* that the network, and the CIO even exist.

Accepting that to accomplish these roles and functions, the CDO should be an independent "C-suite" officer at a peer level to the CIO and other core "headquarters" support functions, brings us to the

question of what mechanisms can organizations and counsel use to create the proper structure and achieve a place there for an effective CDO as data steward.

If the scope of activities and likely statement of roles and responsibilities of a CDO makes its operational independence desirable and functionally practical, the rationale and means for this independent placement is rooted in at least four considerations: (1) legal authority, (2) structural necessity (3) functional opportunity and (4) management precedent.

Legal Authority: CDOs must have their function spelled out in corporate or NGO chartering instruments—corporate charter, by-laws, operating procedures, partnership agreement—whatever the applicable governance instrument is—at a level of detail equivalent to the CFO, GC, and CIO. When newly created, the imprimatur of Board approval should be unambiguous.

In government agencies generally, while there is no present specific authority for a "CDO" role, the USG-wide implementation of information architecture and security related to it has been the product of several widely understood statutes and government wide policy statements dating to the 1990s. General IT acquisition practice has been rooted in the Competition in Contracting provisions of the 1996 Clinger-Cohen Act, revised in 2014 under FITARA, while CIO IT security and its management responsibilities have their roots in the 2002 Federal Information Systems Management Act (FISMA) and its 2014 overhaul, FISMA II. These statutes, and implementing guidance such as OMB Circular A-130, revised in 2016, dictate the role of Federal agency Chief Information Officers and its responsibilities—they are unfortunately, uniformly silent on the role of a "chief data officer".

For IC agencies, authorities are rooted in The National Security Act of 1947, as amended, and particularly the 2004 Intelligence Reform and Terrorism Protection Act (IRTPA), which creates the DNI, the ODNI and its functional organs, including establishment of an Assistant DNI for Information, the IC CIO. The CIO role is given specific detail by Intelligence Community Directive 500,(ICD 500) which spells out the duties, roles and responsibilities of the IC CIO, supported by ICD 501 on Data Sharing, and ICD 703 on Classified Information.

Functional opportunity: For most entities, the "kitchen sink" nature of the CIO function makes it a natural home for the CDO role. This is not by design, but by default. The evolution of CIOs, and more recently, security-focused "Chief Information Security Officers" (CISO) has occurred typically within a single monolithic organization within entity management. In some entities, aspects of CISO responsibility lie with the risk officer, CFO or even GC. Attenuation of reporting away from dedicated IT management such as the CIO can have equally severe consequences as "captive" data responsibility embedded entirely within the CIO organization.

Structural necessity: The unique data stewardship functions that should be the primary responsibility of the CDO not only make it prudent that the CDO be independent of both their client business organizations AND any extant CIO organization, they make it NECESSARY, for two principal reasons.

First, as already alluded to, the primary responsibility of the CDO must be to support the role of data as an entity asset. While hosting a CDO function within a CIO organization is not a travesty or otherwise in-appropriate, it is unquestionably "sub optimal" from the perspective of maintaining an independent view of *data architecture* a*nd security*, properly the responsibility shared with the CIO as responsible manager of *IT infrastructure architecture and security*.

Second, a similar set of considerations of independent view apply to the CDO's relationship with "client" business organizations. It is on their behalf who the CDO must be capable of both advising and supporting on mission rooted data stewardship practices, and acting to remediate them where the business operating group may not be properly maintaining their own data stewardship responsibilities.

Management Precedent

In most organizations, in the absence of any other suitable existing Community-wide operational bureaucracy, the CIO is a logical place to house the CDO. Furthermore, in view of several aspects of historical CDO scope—including technical data architecture activities and other "data science" functions, many CDO offices are structured to encompass these functions, creating a bridge between business management aspects of CDO functions and more technical CIO roles. But in practice, the visionary role of CDO as an independent voice for data life cycle practices not only requires the capacity to have an independent view on these issues, but to forcefully advocate for practices which may from time to time be antagonistic to CIO practices or interests.

As noted, none of the US government general legal authority instruments mentions a "Chief Data Officer", as that term had begun to be used in industry. But by 2014, a movement towards incorporating elements of data security, data architecture, data conditioning and other elements of the emerging "Big Data" life cycle created an appetite for a role within IC components, and in 2015, the CIO appointed an IC Chief Data Officer, under a memo signed by the IC CIO. (E/S 2016-00152, 31 March 2016). It is noteworthy that within the IC in many of the IC component agencies like DIA, NSA and FBI which have established CDO roles, they are independent of the agency CIO.

Conclusion

The IC provides an anecdotal example of the challenges in establishing a role for an entity-wide steward for the data and its existence as a critical asset of an entity. While many options for both structure and operation exist, achievement of a range of critical data custody objectives is enabled by the creation of a Chief Data Officer function independent both of the business missions it must support and assist, and the CIO-infrastructure role with which it must partner, but often, must also maintain a leveraged posture to enable advocacy on behalf of the data.

As these options are considered, counsel must be clear on available options, and provide instruments that establish roles in unambiguous but appropriately flexible manner within the framework provided by existing legal authority and governance/chartering instruments.

Michael Aisenberg *is Chair, ABA Information Security Committee; Senior Fellow, George Washington University Center for Cyber & Homeland Security; Principal Cyber Policy Counsel, The MITRE Corporation.*

Considerations Governing the Lifting of a Litigation Hold in Civil and Criminal e-Discovery

By Alec Webley, Alexander Hastings, and Edward Rippey

Well known is the rule that, once litigation is anticipated, all relevant documents typically must be retained.[1] *This is done primarily by means of the "litigation hold," a notice suspending an organization's usual document deletion policies and instructing employees to retain any documents relevant to the lawsuit*.[2] *But,* much less attention is paid to the final step: determining when a litigation hold may be released. Yet this step can be fraught with difficulties: remove the hold too soon and risk harsh penalties;[3] remove it too late and documents will begin to accumulate — and your legal risks, not to mention storage costs, along with them.[4]

While the timing of when a legal hold begins has attracted considerable discussion from courts,[5] commentators,[6] and even the civil rules Advisory Committee,[7] much less attention has been paid to when such a hold must be lifted. This article aims to address this gap by examining some of the common litigation hold release scenarios and making observations about the rulings of courts and others in this area, along with a few common-sense recommendations.

Before considering these legal questions, we wish to stress a prosaic point: organizations with document retention systems should ensure those systems can readily remove a litigation hold; in particular, removal of a litigation hold should be properly communicated from the legal department to the right people inside the organization.[8] In certain cases, an organization's failure to expressly remove

---

[1] *See* Zubulake v. UBS Warburg LLC, 220 F.R.D. 212, 217 (S.D.N.Y. 2003) ("The duty to preserve attache[s] at the time that litigation was reasonably anticipated.")

[2] *See generally* The Sedona Conference® Working Group on Electronic Document & Retention & Production (WG1), *The Sedona Conference® Commentary on Legal Holds: The Trigger & the Process*, 11 Sedona Conf. J. 265 (2010).

[3] *See* Fed. R. Civ. Pro. 37(e) (2015) (sanctions for the deliberate destruction of electronically stored information, including, if done with intent to deprive another party of information in the litigation, entry of default judgment).

[4] *See, e.g.*, Matthew Scott, *New rules for data retention*, Corporate Secretary (Sept. 27, 2012), https://www.corporatesecretary.com/articles/ediscovery-and-records-management/12336/new-rules-data-retention/ (estimating between $2 and $20 to store each gigabyte of data).

[5] *See, e.g.*, Zubulake, *supra* note 1; AJ Holdings Grp., LLC v. IP Holdings, LLC, No. 600530/2009, 2014 WL 4652899 (N.Y. Sup. Sept. 15, 2014).

[6] *See,* Paul W. Grimm et. al., *Proportionality in the Post-Hoc Analysis of Pre-Litigation Preservation Decisions*, 37 U. Balt. L. Rev. 381 (2008) (collecting commentary).

[7] Fed R. Civ. P 37(e) advisory committee's note to 2015 amendment; *see also* John G. Roberts, *Chief Justice's Year-End Report on the Federal Judiciary 2015* at 8 (Dec. 31, 2015), https://www.supremecourt.gov/publicinfo/year-end/2015year-endreport.pdf (discussing new e-discovery rules).

[8] *See* The Sedona Conference® Working Group on Electronic Document & Retention & Production (WG1), *The Sedona Conference® Commentary on Legal Holds: The Trigger & the Process*, 11 Sedona Conf. J. 265 (2010) (providing for a similar recommendation as its Guideline 11).

a litigation hold when they probably could have done so is *itself* sufficient to trigger a duty to preserve documents.[9] While, as we shall see, there are inevitably edge cases where it is unclear when a litigation hold may be released, there are bright-line cases too; organizations should ensure they can take advantage of those bright-line cases and ensure that releasing litigation holds is integrated into their document retention practices.

First-Party Civil Litigation

The most common cause for issuing a litigation hold is when an enterprise is about to engage in some form of litigation as a party. In the simplest litigation of the *A versus B* type, the obligation to keep a litigation hold in place with respect to a given lawsuit typically ends with respect to a given party when the lawsuit is fully resolved, with the final judgment entered and appeals exhausted. Of course, as is so often the case in civil litigation, ambiguity on this precise end-point can be readily dealt with by a stipulation between the parties; there is little to be lost and much to be gained by simply agreeing to a clear and indisputable date when a given party's document preservation obligations are over. The trouble tends to crop up in situations where a defendant faces future *potential* lawsuits that will draw on the same documents as a lawsuit that has fully concluded. In such cases, courts have occasionally held that the existence of the past lawsuit is sufficient to make the defendant "reasonably anticipate" that future lawsuits might be incoming.

The central question appears to be the relationship between past lawsuits and the present one. Thus, for example, if a defendant is being sued by one plaintiff for an alleged wrong that hurt other potential plaintiffs, courts have held that the duty to preserve documents starts with that first lawsuit.[10] Likewise, on occasion courts have found that knowledge of an industry-wide problem likely to be litigated is enough to require a litigation hold for potential future lawsuits, even if past litigation has already been resolved.[11]

By contrast, if a defendant is facing different *kinds* of lawsuits, whether by scale or subject matter, that happen to share documents with future lawsuits, it can be argued that the duty to preserve for one type does not "bleed over" from one set to another. Thus, for example, a past medical malpractice indemnification claim over an allegedly defective drug was held not to be enough to put a defendant "on notice" to preserve documents for private products liability lawsuits on that same drug.[12] Likewise, a court recently held that *individual* isolated products liability lawsuits did not reasonably lead to the

[9] In re Actos (Pioglitazone) Prod. Liab. Litig., No. 6:11-MD-2299, 2014 WL 2872299, at *22 (W.D. La. June 23, 2014).
[10] M & T Mortg. Corp. v. Miller, No. CV2002-5410(NG)(MDG), 2007 WL 2403565, at *6 (E.D.N.Y. Aug. 17, 2007) ("Even had the [first action] ended before commencement of [the current case], the . . . defendants should have reasonably anticipated that separate litigations could have been brought by individual purchasers, which has indeed occurred.")
[11] Livingston v. Isuzu Motors, Ltd., 910 F. Supp. 1473, 1494 (D. Mont. 1995); *see also* In re Napster, Inc. Copyright Litig., 462 F. Supp. 2d 1060, 1070 (N.D. Cal. 2006) (dismissal of prior lawsuit did not allow defendant to lift a litigation hold, since it had reason to know further lawsuits were inevitable).
[12] In re Pradaxa (Dabigatran Etexilate) Prod. Liab. Litig., No. 312MD02385DRHSCW, 2013 WL 5377164, at *13 (S.D. Ill. Sept. 25, 2013).

belief that a *nationwide* products liability action was "down the road."[13] A concluded criminal or regulatory investigation has also been held to be sufficiently different in kind as to not give a "reasonable anticipation" of future civil litigation.[14]

The central lesson here for organizations is to exercise due caution at the end of a lawsuit; it may well be worth taking a moment to think about whether new lawsuits, of the kind just resolved, might be lurking on the horizon. If so, both case law and cost-saving considerations point in the direction of retaining the hold, even if no lawsuits seem to be immediately threatening. If not, however, the organization may be well advised to remove the litigation hold and bring its regular document retention policies back into action, provided of course there are no other reasons to anticipate future litigation.

Third-Party Litigation

Litigation holds are not always created in response to a lawsuit: they can also come about when an organization is required to produce documents in response to a "third party subpoena," a demand to produce documents in a lawsuit in which the organization is unlikely to be impleaded as a full-fledged party.[15] The obligation to preserve relevant documents attaches when a subpoena is served, simply by virtue of the need of the third party to comply with the subpoena.[16] But once a subpoena has been substantially complied with and the case has concluded, we could find no case that has sanctioned an organization for lifting a litigation hold and thereby destroying documents relevant to other litigations in which the destroying organization was also a third party.[17] Indeed, there is some authority for the proposition that there is *no duty at all* for a third party to preserve evidence in a lawsuit in which it is not likely to be a party.[18]

---

[13] In re Ethicon, Inc. Pelvic Repair Sys. Prod. Liab. Litig., 299 F.R.D. 502, 516 (S.D.W. Va. 2014).

[14] *See, e.g.*, In re Delta/AirTran Baggage Fee Antitrust Litig., 770 F. Supp. 2d 1299, 1308 (N.D. Ga. 2011) (a civil investigative demand issued by the Department of Justice does not give rise to the reasonable expectation of litigation, since such demands often do not lead to actual prosecution); Brigham Young Univ. v. Pfizer, Inc., 282 F.R.D. 566, 572 (D. Utah 2012) (same); Point Blank Sols., Inc. v. Toyobo Am., Inc., No. 09-61166-CIV, 2011 WL 1456029, at *24 (S.D. Fla. Apr. 5, 2011) (same).

[15] *See* Fed. R. Civ. Pro. 45 (2015).

[16] *See, e.g.*, In re Napster, Inc. Copyright Litig., 2006 WL 3050864, at *6 (N.D. Cal. Oct. 25, 2006) (duty to preserve documents attached once organization received a third party subpoena).

[17] *See, e.g.*, United States v. Amerigroup Illinois, Inc., No. 02 C 6074, 2005 WL 3111972, at *2 (N.D. Ill. Oct. 21, 2005) (quashing a subpoena seeking the restoration of deleted emails from backup tapes as unduly burdensome).

[18] *See, e.g.,* In re Ex Parte Glob. Energy Horizons Corp., 647 F. App'x 83, 87 (3d Cir. 2016) (third parties have no duties to preserve documents prior to receiving a subpoena); Andra Grp., LP v. JDA Software Grp., Inc., No. 3:15-MC-11-K-BN, 2015 WL 12731762, at *16 (N.D. Tex. Dec. 9, 2015) (finding no duty for a third party to preserve evidence, even under the new Federal Rules of Civil Procedure; explaining that even if the third party "had a duty to preserve evidence, Rule 37(e) would not apply because [the third party] is not a party."); Holmes v. Amerex Rent-A-Car, 710 A.2d 846, 849 (D.C. 1998) ("Absent some special relationship or duty rising by reason of an agreement, contract, statute, or other special circumstance, the general rule is that there is no duty to preserve possible evidence for another party to aid that other party in some future legal action against a third party.").

Of course, a subpoena might be sufficient to alert an organization that it is likely to be a party to litigation, triggering a broader obligation to preserve documents and preventing the organization from lifting the litigation hold first implemented for a third-party subpoena.[19] And some states recognize a tort of spoliation that can serve as another source of liability for third parties found to have destroyed relevant evidence.[20]

Given the relatively unsettled state of the field, organizations should consider common-sense litigation hold lift practices for third-party subpoenas. In particular, just as with civil litigation, it may be advisable to take a moment and consider, once a subpoena has been substantially complied with, whether litigation might now be "reasonably foreseeable." If it is clear that no litigation is on the horizon, or even over the horizon, the litigation hold could potentially be lifted.

On a more pragmatic note, however, it may be advisable to hold on to subpoenaed documents until the conclusion of the case for which they were requested. If the inherent risk that the subpoenaed documents will lead to litigation is low, and the chances that the documents will be relevant to the case again (perhaps because it will be remanded, or discovery will be lengthy or involve more parties) is high, it may well be more cost-effective to keep the production around rather than file for motions to quash.

Criminal and Regulatory Investigations

In a conventional criminal judicial proceeding, the rules on releasing litigation holds for a defendant track those of civil suits: once final judgment has been entered and direct appeals exhausted, a private party generally no longer has an obligation to preserve documents.[21] In reality, of course, an organization will likely either be a third party to a criminal case (in which case the same third-party rules discussed above likely apply) or will expend the vast majority of its e-discovery resources in negotiations with prosecutors, usually federal prosecutors, sometimes before charges are filed.[22]

Discovery in prosecutorial negotiations may focus on the fullest, fastest, and frankest production of documents to prosecutors so as to help persuade the Government that, at a minimum, the defendant is fully cooperating with its investigation, and that its investigation is truly getting to the bottom of the

[19] *See, e.g.*, PBell Inc. v. GE Lighting, LLC, No. 6:14-CV-00012, 2014 WL 1630754, at *15 (W.D. Va. Apr. 23, 2014) (third party to lawsuit on notice that it could become impleaded when it first received requests for documents); Peskoff v. Faber, 244 F.R.D. 54, 64 (D.D.C. 2007) (same).

[20] Benson v. Penske Truck Leasing Corp., No. 03-2088 MA/V, 2006 WL 840419, at *3 (W.D. Tenn. Mar. 30, 2006) ("third-party spoliation occurs when a third party destroys evidence that could have been used by a plaintiff against a different defendant in a separate suit."); *but see* Temple Cmty. Hosp. v. Superior Court, 20 Cal. 4th 464, 976 P.2d 223 (1999) (declining to recognize the tort of third-party spoliation in California, and collecting cases).

[21] Fed. R. Crim. P. 16(c) (2013) (duty for continuing disclosure ends at the conclusion of trial).

[22] *See generally* Daniel Fetterman & Mark Goodman, Defending Corp. & Indiv. in Gov. Invest. § 6:15 (2015) (general overview of white collar investigations).

alleged wrongdoing.[23] The chief difficulty in the lifting of litigation holds in this "negotiation" phase arises when an organization *thinks* it has completed a criminal or civil inquiry before the government only to learn that the investigation has restarted, or is still ongoing.

This sort of thing happens more often than one might think. In some cases, for example, a corporation might secure a deferred prosecution agreement or non-prosecution agreement that is silent as to the preservation of critical documents. More prosaically, a corporation may participate in an investigation before a regulator or prosecutors for a time and then receive a communication from the regulator that it has no interest in taking action against that corporation—or perhaps simply doesn't hear back from the government at all. In all of these cases, it is possible for the government to resume the investigation and, indeed, file charges. But this leaves an organization in a difficult position, not knowing when it is "safe" to resume the "regular order" of its document retention policy.

In some cases, this difficult position can be avoided by stipulating in the consent order, non-prosecution agreement, or plea bargain with the regulatory agency or prosecutors what, if any, obligations for document preservation the organization must assume. In other cases, especially if an organization is neither facing charges nor negotiating in earnest for an agreement of some sort (such as when an organization is simply in receipt of a governmental request for documents as part of a larger investigation), this option is not available.

Under these circumstances, an organization ought to carefully consider whether, and under what circumstances, the costs of maintaining a litigation hold exceed the costs of a possibly premature revocation of the hold. This is a prudential and factually-intensive inquiry: an investigation in which an organization is clearly only a peripheral participant may present a far different risk profile to one in which the organization is the center of attention. What matters is that the question of lifting a hold is considered as an integral part of the conversation around document preservation.

Conclusion

Just as the rules surrounding the creation of litigation holds continue to grow in difficulty and complexity, so too do the considerations governing when a litigation hold ends. Further, a document retention policy is of little use if huge swaths of documents are placed beyond its ambit for all time. That said, the decision to release a legal hold is an extremely fact-intensive decision that varies based on a party's circumstances and requires close consultation with counsel.

[23] *See* United States Attorney's Manual § 9-28.700, 9-28.800, and 9-28.900. *See also* SEC Enforcement Manual § 6.1.2 (Mar. 9, 2012) (the provision of all information relevant to the underlying violations is a factor in the Commission's determination as to whether an investigated company will be granted leniency)

Alec Webley *is a litigation associate at Covington & Burling LLP (awebley@cov.com).* ***Alexander Hastings*** *(ahastings@cov.com) is a government contracts and litigation associate and a member of the firm's E-Discovery Practice Group.* ***Edward Rippey*** *(erippey@cov.com) is a partner at the firm, handles complex commercial litigation, and is Chair of the E-Discovery Practice Group.*

Executive Order 12333, the President-Elect, and the NSA

By April Doss

It's no secret that the national security community has been uneasy with candidate Trump, with many of its most esteemed leaders forming vocal, passionate parts of the #NeverTrump movement. In fact, in Aug. 2016, a group of prominent national security experts – all of whom had served as Republican political appointees over several administrations – signed a letter denouncing Trump. Their criticism could not have been more clear: "From a foreign policy perspective, Donald Trump is not qualified to be President and Commander-in-Chief. Indeed, we are convinced he would be a dangerous President and would put at risk our country's national security and well-being." [1]

In the days since the election, those concerns have persisted, with Ben Wittes of the Brookings Institution and Lawfare blog writing that, he will be analyzing the next President's foreign policy decisions "with the working assumption that our nation must be protected both by and from the president."[2] And those comments are just the ones from conservative think tanks and from within the President-elect's own party. Equally concerned voices have been arising from the left, from groups like the American Civil Liberties Union.[3]

So what does this have to do with Executive Order 12333 and the NSA?

Let me start with a conversation I had a few weeks ago, when I was contacted by a reporter who wanted to know, "If Trump were elected President, could he misuse the NSA?"

The reason the reporter contacted me is because of my past: although I'm currently in private practice, advising clients on cybersecurity and privacy law, I spent over a decade at the NSA. I managed counterterrorism programs, led the creation of NSA's vetting process for cloud analytics, served as a foreign liaison officer, and – in my last post before resigning from NSA – served as the Associate General Counsel for Intelligence Law, where I led the group of several dozen attorneys who were responsible for providing legal advice on NSA's worldwide intelligence operations including its oversight and compliance programs, privacy and civil liberties, and operational dimensions of its new technology development. It was a rewarding, humbling, and fascinating career. I was, and remain, proud to have worked at an Agency filled with so many people – many of them brilliant linguists, analysts, mathematicians, and technologists – who are deeply committed to the rule of law and the defense of our nation.

---

[1] http://www.nytimes.com/interactive/2016/08/08/us/politics/national-security-letter-trump.html
[2] https://www.lawfareblog.com/burden-donald-trump
[3] https://www.aclu.org/blog/speak-freely/if-donald-trump-implements-his-proposed-policies-well-see-him-court

Let me pause for the asterisk here, because I can feel it coming: Some of you who are reading this are already objecting in outrage, "Rule of law?!? Are you kidding? After the things that NSA has done?"

So, I'll repeat it: yes, the rule of law. How do I know? I was one of the people who gave the annually-required briefings on the sometimes-arcane details of technical compliance with the regulations and policies governing NSA's intelligence activities. I was one of the people who worked full-time answering questions every day – questions about compliance with the complex set of regulatory and policy constraints, of statutes, court-ordered procedures, procedures imposed by the Attorney General, rules defined by the Department of Justice, policy requirements of the Office of Director of National Intelligence (ODNI) and the Department of Defense (DoD), policy constraints set internally by NSA, policy limits defined by agreements with partners, and yes, the limits of the Constitution.

NSA has hundreds of people[4] working day and night in roles similar to the one that I used to fill: an entire workforce of lawyers, compliance officers, and a civil liberties and privacy office,[5] all of whom are dedicated to ensuring the rule of law, compliance with policy, and protection of privacy and civil liberties. And those are just some of the tangible internal safeguards, the resources available to the NSA workforce to address questions about how to ensure that NSA's operations are being carried out in lawful and appropriate ways. Equally important are the structural safeguards like the NSA's Office of the Inspector General (OIG), and the many external oversight bodies which have been described in detail elsewhere.[6]

All of these structural safeguards, internal and external, are critically important. And yet – in government just like in the private sector – some of the most significant protections are the intangible safeguards that go hand-in-hand with having a culture of compliance. So what exactly does a "culture of compliance" mean? Former NSA Deputy Director John C. "Chris" Inglis might have said it best when he was asked for his reaction to Oliver Stone's fictionalization of Edward Snowden's leaks. In an interview, Inglis explained that, "The film was grossly incorrect technically, but that was not the most egregious thing about the movie. It's that it was spiritually incorrect. It was well wide of conveying a true sense of how the NSA purports itself."[7]

Here's my experience of the reality of how NSA comports itself: rigorous self-reporting of errors, scrupulous attention to detail, and continuous internal debate not only about what *can* be done from a technical perspective, but what *may* be done from a legal perspective, and what *should* be done from a policy perspective.

---

[4] http://blogs.wsj.com/riskandcompliance/2014/01/23/compliance-in-government-qa-with-john-delong-of-the-nsa/
[5] https://www.nsa.gov/about/civil-liberties/
[6] http://m.nsa.gov/about/faqs/oversight-faqs.shtml
[7] http://www.nextgov.com/technology-news/tech-insider/2016/09/former-nsa-deputy-director-calls-out-snowden-movie-grossly-inaccurate/131911/

Which brings me to the current questions about what to expect under the future administration of President-Elect Trump.

Could the future president amend EO 12333, the foundational executive order that underpins many of the activities of the intelligence community? Absolutely. But the last time EO 12333 was under major review, the amendments took years of interagency discussion and review before changes were signed in 2008.[8] Could the future president direct his Secretary of Defense and Director of National Intelligence to change important policies that govern intelligence activities by DoD and ODNI components like the NSA? Of course. But recent efforts to change the critically important DoD procedures for handling U.S. person information, DoD 5240.1-R, took years to complete. (Depending on how one counts the starts and re-starts for this effort, the attempts to revise this 1982 policy were going on for nearly a decade before a new policy manual was finally issued in August of this year).[9]

So, as other commentators have pointed out,[10] the bureaucracy can be a protection in itself against presidential overreach or against the destabilizing effects that could result if policy reversals take place too quickly, a kind of policy whiplash.

So I offer here a few thoughts worth remembering, noting that for those who fear that surveillance may be ratcheted up to unacceptable levels under President Trump, these thoughts might prove comforting. First, the NSA sits far outside the Washington beltway. Although it's only a few dozen miles, the cultural distance between DC and Ft. Meade is vast. NSA personnel, like everyone in the intelligence community, are bound not only by the Hatch Act which prohibits most forms of partisan political expression that ordinary citizens take for granted; NSA personnel are further constrained by an enhanced set of Hatch Act rules that apply to intelligence professionals.[11] The rules makes sense: the last thing a free and democratic country needs is to have an intelligence community that is politicized, that sways according to partisan winds. Perhaps it was because people recognized the importance of that truth, I don't recall hearing anyone at NSA complain about the restrictions on what would otherwise be their First Amendment rights to engage in political expression. On a personal level, among colleagues I came to know well, it became possible over time to gauge what people's political leanings might be; but this was only in informal conversation among close friends, far outside the workplace and in non-work-related contexts.

Second, NSA has no political appointees, except for its director, an active-duty military officer who is nominated by the Secretary of Defense after concurrence from the DNI. Under existing DoD policy (and in keeping with the longstanding policy requirements that have been in place for decades), the Director of NSA, who also serves as Chief of the Central Security Service, must be an active duty

[8] https://it.ojp.gov/PrivacyLiberty/authorities/executive-orders
[9] http://dodsioo.defense.gov/
[10] http://www.nytimes.com/2016/11/10/opinion/are-there-limits-to-trumps-power.html?_r=0
[11] https://osc.gov/Pages/HatchAct-AdditionalResouces.aspx

general officer in the military, and must be of no less than three-star rank.[12] An active-duty military general or admiral is a very different kind of political appointment than the "politicals" that we so often think about who are appointed through the Presidential Personnel Office process to high-ranking posts around DC. To be clear, those civilian political appointees can often bring deep expertise and important perspective to the posts they hold. However, they typically are also affiliated with a specific political party in ways that are wholly different from the non-partisan obligations of serving military officers.[13]

And third, NSA is a sticky place – it's the kind of place where people come to serve and end up remaining for decades. So the civilian workforce – from general schedule regular employees through the senior executive service – is filled with people who have worked for decades at the NSA, carrying out mathematics research, language translation, signals collection, computer security, intelligence analysis, and a multitude of other functions (from human resources to logistics to budget and finance work and more) through multiple administrations of presidents from both parties, through multiple Secretaries of Defense and heads of the intelligence community (both the DNI and the former Directors of Central Intelligence). Throughout those changes, the people who work and serve at the NSA have been reminded regularly of the importance of their own oaths to the Constitution, through annual training, day-to-day oversight activities, and the like. Most importantly, they work immersed in that culture of compliance that I believe Chris Inglis was referring to when he talked about the spirit or essence of NSA. As a result, the NSA personnel who work in its intelligence mission have remained focused on a core set of principles: that the NSA stands at the shores of the nation and looks out, monitoring threats from foreign adversaries; obtaining foreign intelligence information that the President and his advisors can use to inform national policy making; and gathering the tactical intelligence that allows US military commanders around the world to protect their troops and our allies.

Even before Trump's election, some commentators were raising concerns that if he were elected President, he might direct NSA to undertake surveillance of Americans in ways that would be unlawful, even unconstitutional. I don't think we know yet whether he – or any other president – might direct such actions, but I fully expect that there would be a robust set of checks and balances to stand in his way. And based on my experience working there – through both Republican and Democrat administrations – I expect that one of the greatest, non-structural defenses against any President who tried to misuse the agency would be the people who work at the NSA.

Much of the reporting about NSA since 2013 has done a disservice to the dedicated women and men who work there, who carry out the work honorably and diligently and compliance with the law. After all, the biggest debates public debates were not about law, but about policy: should the government use Section 702 of the FISA Amendments Act, should the government collect metadata in bulk if that collection was also used in narrowly constrained ways and subject to painstaking oversight? It would

[12] http://www.dtic.mil/whs/directives/corres/pdf/510020p.pdf
[13] http://www.dod.mil/dodgc/defense_ethics/ethics_regulation/1344-10.html

be hard to fault the people at NSA if they found it demoralizing to be viewed as public enemy number one, to be viewed as reckless and rogue, when they undertook their daily work with close attention to detail, with self-reporting, within complicated and important constraints. Now, in the face of a new set of policy questions, those very same people are the ones who I believe are most likely to stand up in the face of any attempts by this or other presidents at unlawful or unconstitutional overreach.

If this election cycle has taught us anything, it's that making predictions from traditional assumptions is a fool's errand when it comes to this extraordinary election cycle, this non-traditional President-elect, and his principal advisors. I don't believe we know yet what direction President Trump's national security focus will take, or what his policies will be. But I have the benefit of having had many years of an inside look at NSA. Based on that, I have high confidence that the men and women at NSA – from the workforce through the senior leaders – will be among the first to speak up if the new administration should direct them to take actions that run contrary to the principles of civil liberties and privacy that they deeply – spiritually – hold dear.

April Doss *chairs the Cybersecurity and Privacy practice at Saul Ewing, and is the former Associate General Counsel for Intelligence Law at NSA. The views and opinions expressed here are the author's and do not reflect those of NSA/CSS.*

Blockchain Risk Factors in Securities Offerings and Filings

By Bo Harvey and John Servidio

The hype around bitcoin and similar digital currencies appears to be making way for similar enthusiasm over the underlying distributed ledger technology, or blockchain, that facilitates delivery and payment of digital currency transactions. Banks, financial intermediaries, financial technology startups and regulators are actively exploring how distributed ledger technology can improve similar functions in financial markets for other "digital" assets, including securities.

As one of many examples, in May 2016, the governor of Delaware announced a "Delaware Blockchain Initiative." One aspect of the governor's initiative is to determine if Delaware should changes to its corporate law in order to facilitate Delaware companies' use of distributed ledger technology to issue securities. To be sure, certain changes to existing statutes may be necessary to allow the use of distributed ledgers in corporate governance, contractual or capital markets contexts. The issue for regulators, issuers and investors to consider is how distributed ledger technology is currently regulated, or should be regulated. The answer will depend on how the technology is used and in what context. The simple choice of market participants to use distributed ledgers in certain contexts does not by itself remove such use from the ambit of current regulatory regimes.

In the capital markets space, issuers and other market participants are actively exploring distributed ledgers to facilitate the issuance, clearing, settlement and trading of securities. In that regard, existing securities laws and regulations will continue apply. We examine what risks issuers and their counsel may consider in preparing appropriate risk factors concerning distributed ledger technology in offering documents or filings the Securities and Exchange Commission (SEC). Risk factors play an important part in registration statements, annual 10-K filings (and 10-Q filings in some cases) as well as prospectuses and other disclosure documents. Effective risk factors meaningfully and concisely describe, in plain English, risks specific to a company, its industry or its securities.

Issuers and their counsel should consider disclosing material risks when using distributed ledger technology in business operations or in issuing "digital securities." (Like digital currencies such as bitcoin, digital securities are held on a distributed ledger, with certain necessary differences to accommodate the specific nature of securities clearing, settlement and trading.) As with disclosure generally, crafting effective risk factors depends on the facts that surround each issuer's business and securities. Therefore, issuers and their counsel should conduct further fact-specific analysis of a company's business, operations, financial position, future financial performance and securities in order to determine whether any of these risks apply, and how to draft an appropriate disclosure

related to any such risk. Risk factors should also be periodically re-evaluated. Such re-evaluation is especially appropriate in light of the quickly changing technological and regulatory landscape surrounding blockchain.

Companies with businesses or operations involved with distributed ledger technology, or that are considering using the technology to issue "digital securities" or other assets, may want to consider the following as they draft risk factors:

- *The technology is new and many of its uses may be untested*. This is perhaps obvious. While bitcoin and digital currencies have more established payment mechanics, the payment mechanics when using distributed ledger technology to transact in other types of assets, such as securities or derivatives, is less clear.

- *Lack of regulation.* Digital currencies such as bitcoin are largely unregulated, and the regulatory environment is rapidly evolving. As a result platforms on which they trade may be exposed to adverse regulatory action, fraudulent activity or even failure. For instance, in 2014 Mt. Gox, which was at the time the world's largest bitcoin exchange, filed for bankruptcy when it was reported that $450 million worth of the platform's bitcoins had disappeared or been stolen by hackers.

- *Theft, loss or destruction*. Transacting on a distributed ledger depends in part specifically on the use of cryptographic keys that are required to access a user's account (or "wallet"). The theft, loss or destruction of these keys impairs the value of ownership claims users have over the relevant assets being represented by the ledger (whether "smart contracts," securities, currency or other digital assets). The theft, loss or destruction of private or public keys needed to transact on a distributed ledger could also adversely affect a company's business or operations if it were dependent on the ledger.

- *Competing platforms and technologies*. The development and acceptance of competing platforms or technologies may cause consumers or investors to use an alternative to distributed ledgers.

- *Cybersecurity incidents*. Cybersecurity incidents, such as the Mt. Gox hack, may compromise an issuer, its operations or its business. Cybersecurity incidents may also specifically target user's transaction history, digital assets, or identity, thereby leading to privacy concerns.

- *Intellectual property claims*. A proliferation of recent startups attempting to apply distributed ledger technology in different contexts means the possibility of conflicting intellectual property claims could be a risk to an issuer, its operations or its business. This could also pose a risk to distributed ledger platforms that permit transactions in digital securities.

- *Lack of liquid markets, and possible manipulation of blockchain-based assets*. Digital assets that are represented and trade on a ledger-based platform may not necessarily benefit from viable trading markets. Stock exchanges have listing requirements and vet issuers, and perhaps users. These conditions may not necessarily be replicated on a distributed ledger platform, depending on the platform's controls and other policies. The more lax a distributed ledger platform is about vetting issuers of digital assets or users that transact on the platform, the higher the potential risk for fraud or the manipulation of digital assets. These factors may decrease liquidity or volume, or increase volatility of digital securities or other assets trading on a ledger-based system.

- *Third party product defects or vulnerabilities*. Where distributed ledger systems are built using third party products, those products may contain technical defects or vulnerabilities beyond a company's control. Open-source technologies that are used to build a distributed ledger application, such as Ethereum, may also introduce defects and vulnerabilities.

In drafting appropriate risk factors involving blockchain, practitioners should also keep in mind the SEC's cybersecurity disclosure guidance from October 13, 2011 (available here) which advises issuers to review, on an ongoing basis, the adequacy of their disclosure relating to cybersecurity risks and incidents. While this guidance relates specifically to cybersecurity, the principles and recommendations laid out by the SEC may also apply, to an extent, to distributed ledger technology, with appropriate modifications to account for context.

Distributed ledger technology has the potential to disrupt and improve several functions within the financial industry, including issuance, clearing, settlement, and trading of securities. As banks and financial technology companies seek to take advantage of its benefits and overcome its challenges, capital markets practitioners need to bear in mind that existing securities laws and regulations continue to apply, including providing meaningful and effective disclosure of risks related to the technology in any securities offerings and filings.

Bo Harvey *is an associate with McGuireWoods LLP in the capital markets group and data privacy and security team, and concentrates his practice in the areas of asset management, derivatives, financial regulation, cybersecurity and emerging financial technology. He represents banks, investment managers, insurance companies and other financial institutions, as well as energy companies and corporate entities in connection with a variety of transactions and in providing related regulatory advice. He received his J.D. and M.B.A. from Duke University, and is admitted to practice in New York and California. His profile can be viewed here and his blog can be viewed here.*

John Servidio *is a Partner with McGuireWoods LLP. John's practice focuses on capital markets, with an emphasis on derivatives and structured products. He advises on structuring equity financial products and other capital markets transactions. He works with banks, asset managers, financial intermediaries and corporate entities to execute capital markets transactions. In addition to providing transactional advice, John serves as counsel to banks and other financial institutions on CFTC, SEC and cybersecurity regulatory matters. He received his J.D. and M.B.A. from Pepperdine University, and is admitted to practice in New York and Illinois. His profile can be viewed here and his blog can be viewed here.*

Editor's Message

With this issue, we are starting the eighth full year of publishing the *Information Law Journal* each quarter and are continuing to welcome authors and readers from similarly-focused committees across the ABA. This issue again presents articles from lawyers and technologists focusing on various aspects of leading-edge domestic and international practice in information, Internet, and emerging technologies law. From the startup of the *Information Law Journal* and its antecedents, nearly 200 different authors have found their voices and expressed their views writing in these pages.

The first article describes two new companion books comprehensively analyzing the areas of emerging technologies law and information and Internet law from a global comparative basis, primarily using the laws and cases of the U.S. and EU. The second article is from Courtney Lotfi of Redgraves LLP, addressing the issues with international dispute resolution and the production of documents restricted by differing legal regimes. The third article by committee co-chair Michael Aisenberg describes the role of the chief data officer in the U.S. intelligence community. The fourth article is written by the team at Covington & Burling LLP led by partner Edward Rippey on the lifting of legal holds in criminal and civil matters. The fifth article, by partner April Doss of Saul Ewing LLP, analyzes the recent election and the impact on the National Security Agency. The sixth article, from McGuireWoods LLP associate Bo Harvey and partner John Servidio, covers the risk factors involving the blockchain in the area of securities filings. Thank you to all of the authors.

Our next issue (Spring 2017) is scheduled to be published by early March 2017. I ask all readers of the *Information Law Journal* to share their experiences and knowledge with their fellow professionals by writing an article for this periodical. Every qualified submission within the scope of the periodical and meeting the requirements explained in the **Author Guidelines** will be published, so please feel free to submit your articles or ideas, even if you are not quite ready for final publication. The issue following the Spring issue (Summer 2017) will be published in June 2017. Until then ...