May
2011
Volume 59
Number 3

United States
Department of Justice
Executive Office for
United States Attorneys
Washington, DC
20530

H. Marshall Jarrett
Director

The United States Attorneys' Bulletin is published pursuant to 28 CFR § 0.22(b).

The United States Attorneys' Bulletin is published bimonthly by the Executive Office for United States Attorneys, Office of Legal Education, 1620 Pendleton Street, Columbia, South Carolina 29201.

Managing Editor
Jim Donovan

Law Clerk
Carmel Matin

Internet Address
www.usdoj.gov/usao/reading_room/foiamanuals.html

Send article submissions and address changes to Managing Editor,
United States Attorneys' Bulletin,
National Advocacy Center,
Office of Legal Education,
1620 Pendleton Street,
Columbia, SC 29201.

E-Discovery

In This Issue

What We See in the Clouds: A Practical Overview of Litigating Against and on Behalf of Organizations Using Cloud Computing

Allison C. Stanton
Director of E-Discovery
Civil Division
U.S. Department of Justice

Andrew J. Victor
Trial Attorney
Torts Branch, Civil Division
U.S. Department of Justice

I. Introduction

Where is the evidence? This question, while always a challenging one, elicited a simpler answer before the dawn of the twenty-first century. Today much of the complexity arises from the tremendous effort to locate, collect, and use electronically stored information in both civil and criminal cases. These processes have compelled companies, local governments, and federal agencies alike to embrace "cloud computing," the next step in the evolution of electronic data storage, and to outsource their data, services, and Information Technology (IT) infrastructure. As a result, litigators are challenged to adapt old strategies to new technology when litigating against or on behalf of organizations using cloud computing.

This article will provide a basic overview of cloud computing, explain the current movement of federal agencies and the private sector into the cloud, discuss the opportunities and challenges for litigators when confronted with this technology, and provide practical suggestions for litigators when seeking evidence in the cloud.

II. What is this "cloud" you speak of?

United States Chief Information Officer, Vivek Kundra, stated that "[j]ust as the Internet has led to the creation of new business models [that were] unfathomable 20 years ago, cloud computing will disrupt and reshape entire industries in unforeseen ways." VIVEK KUNDRA, FEDERAL CLOUD COMPUTING STRATEGY 33 (2011). Cloud computing appears in many forms but the common underlying feature is that a person accesses software programs or creates, saves, and retrieves data from a group of computers usually owned by a third-party, the cloud service provider. The user accesses the data via the Internet. Cloud computing extends to a wide range of services from payroll systems to research and development databases. One of its most common services, however, is Web email, where a user composes, receives, and saves email by logging into a Web site. Traditionally, email would be located on a computer owned and located in the organization. With cloud computing, the user can still access their account via a company or personal computer but the email messages are located on a server owned by a third-party.

The National Institute of Standards and Technology (NIST) defines cloud computing as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources . . . that can be rapidly provisioned and released with minimal management effort or service provider interaction." NIST Definition of Cloud Computing, version 15 (2009). Cloud computing has five basic characteristics: (1) shared resources, (2) scalability, (3) elasticity, (4) pay-as-you-go, and (5) self-provisioning of resources. TIM MATHER ET AL., CLOUD SECURITY AND PRIVACY: AN ENTERPRISE PERSPECTIVE ON RISKS AND COMPLIANCE (2009).

The shared resources characteristic involves multiple users employing the same resources, similar to multiple organizations using the same warehouse to store boxes of files. Scalability is the ability to scale up to massive numbers of systems, bandwidth, and storage space. Elasticity is how users can rapidly increase and decrease resources as needed, analogous to increasing the shelf space used in a warehouse and then decreasing it when the storage is no longer needed. Pay-as-you-go refers to paying only for resources used for the time needed, such as renting storage space only for as long as necessary. Self-provisioning of resources occurs when users decide what additional systems, software, and/or network resources are needed.

There are also different types of clouds. Each type of cloud is named after the type of groups who share the space in the cloud. A "private cloud," for example, is operated solely for an organization so that individuals outside of the organization are unable to access the cloud. A "public cloud" is made available to the general public or a large industry group and is owned by an organization selling cloud services. *See infra* Figure 1. A "community cloud" is shared by several organizations and supports a specific community that has shared concerns.

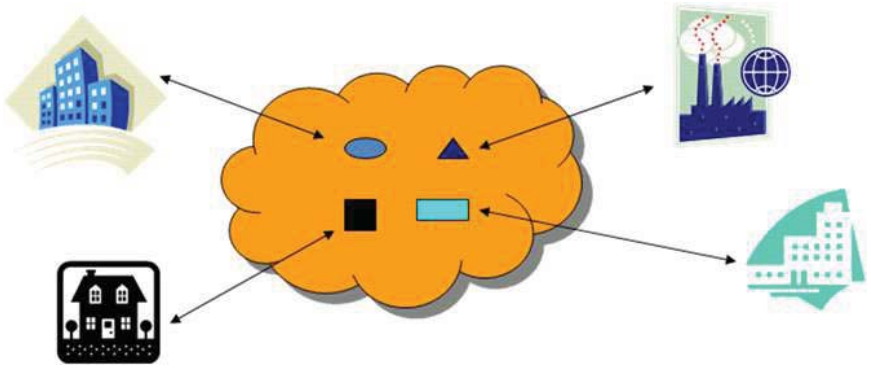

FIGURE 1: example of a public cloud.

Three common cloud computing services have been developed for each of these three types of clouds: (1) software-as-a-service (SaaS), (2) platform-as-a-service (PaaS), and (3) infrastructure-as-a-service (IaaS). As these names denote, cloud computing offers services to users, transforming the traditional computing operations into something closer to a common utility, such as electricity or water, a resource that can be used on demand. SaaS, for example, can be an email service or something more complex like payroll software used by an organization. Instead of accessing the software on its own computers, the organization accesses and runs an application hosted on a cloud provider's servers. TIM MATHER, ET AL., CLOUD SECURITY AND PRIVACY: AN ENTERPRISE PERSPECTIVE ON RISKS AND COMPLIANCE (2009).

Cloud computing also offers economic efficiencies and benefits for an organization. SaaS, IaaS, and PaaS allow an organization to reduce its reliance on internal IT infrastructure by requiring only a

connection to the Internet. An organization, for example, no longer has to buy expensive computer equipment or software licenses to run email systems in-house. A cloud provides one central location for data or applications, eliminating the need to establish multiple systems or IT centers that may spread across a large geographic space. An organization also does not have to worry about repairing or trouble-shooting the systems it uses because the cloud provider performs that responsibility. These cost savings benefits are some of the main characteristics that have attracted organizations, and now federal agencies, to this new technology.

III. Movement of federal agencies and the private sector to the cloud

The government's responsibility is "to achieve the significant cost, agility and innovation benefits of cloud computing as quickly as possible." VIVEK KUNDRA, FEDERAL CLOUD COMPUTING STRATEGY 33 (2011). On December 9, 2010 the White House announced that "[e]ach [federal] agency will identify three 'must move' [IT] services within three months, and move one of those services to the cloud within 12 month[s] and the remaining two within 18 months." VIVEK KUNDRA, 25 POINT IMPLEMENTATION PLAN TO REFORM FEDERAL IT (2010), *available at* http://cio.gov/documents/25-Point-Implementation-Plan-to-Reform-Federal%20IT.pdf.

Transforming the federal government's IT infrastructure at such an accelerated pace holds promise for the future. The main concern, however, rests in ensuring that government attorneys and agencies integrate these changes into their litigation planning. The challenges for litigators confronted with either a client agency or organization using cloud computing for data storage are best addressed by developing E-Discovery strategies at the earliest stages of the case. Agencies should also plan ahead by proactively incorporating litigation and discovery needs into their agreements with cloud providers. By embracing and adjusting to these changes, agencies will have the proper tools and procedures in place and thus be better prepared to aid litigators when litigation arises.

As part of the effort to "jump start" agency adoption of cloud computing, the Office of Management and Budget (OMB) will continue to exercise an important role in this transformation. When OMB evaluates funding and options for new IT deployments, it "will require that agencies default to cloud-based solutions, whenever a secure, reliable, cost-effective option exists." *OMB Announces "cloud first" policy for agencies*, FEDERAL CLOUD BLOG (Nov. 23, 2010), http://fedcloud.wordpress.com/tag/omb/. In November, OMB promulgated a policy that is triggering the movement of additional government entities into the cloud. The policy stated that starting with the 2012 budget process, agencies would be required to consider using cloud computing options first when formulating their budgets. *See* Office of Management and Budget, www.whitehouse.gov/blog/2010/11/19/driving-it-reform-update. Consequently, both agency data and documents needed by Department of Justice attorneys for litigation and discovery are moving to the cloud.

Several agencies have already started this migration. For example, the United States Department of Agriculture (USDA) announced that it would move to a Microsoft cloud for email, web conferencing, document collaboration, and instant messaging. Press Release, USDA, USDA Moves to Microsoft Cloud (Dec. 8, 2010). USDA stated that in implementing the plan it would consolidate 120,000 users who were spread across 21 email systems. *Id.* Other agencies that embrace the cloud are the GSA, the Department of Treasury, the Securities and Exchange Commission, and the Department of Veterans Affairs. *See generally* FEDERAL CLOUD COMPUTING CASE STUDIES, http://info.apps.gov/content/federal-cloud-computing-case-studies (profiling several projects from agencies as varied as the U.S. Forest Service to the Federal Labor Relations Authority).

The movement to the cloud, however, is not unique to the government. Cloud migrations are also expanding at private companies, many of which the government investigates and litigates against. Among the largest group of early adopters for cloud services are financial services and manufacturing industries. *See* Gartner Says Worldwide Cloud Services Market to Surpass $68 Billion in 2010, http://www.gartner.com/it/page.jsp?id=1389313. Companies such as Genentech and Virgin Atlantic have publically disclosed their utilization of cloud computing for certain business functions. Moreover, an extensive survey of company CIOs revealed that cloud computing was their top priority. *See* Gartner Executive Programs Worldwide Survey of More Than 2,000 CIOs Identifies Cloud Computing as Top Technology Priority for CIOs in 2011, http://www.gartner.com/it/page.jsp?id=1526414. As a result, the data and potential evidence needed from these companies may now be in the cloud.

By its very nature, the information found in the cloud is electronic. Consequently, discovery in the cloud will require litigators and courts to rely on E-Discovery law, strategies, and processes. E-Discovery entails the identification, preservation, collection, review, production, and presentation of documents and data originally found in electronic form, and/or documents originally found in hard copy but converted to electronic form for review and production. While E-Discovery has evolved with changes in both the law and technology, the cloud still presents new complications.

IV. E-Discovery challenges and opportunities in the cloud

One challenge presented by cloud computing rests in the discovery issues that have yet to be addressed by the courts. The courts have not resolved how the very nature of cloud computing may complicate the preservation, collection, or production of data stored in the cloud.

Another challenge involves cloud providers. Providers constantly move the data in the cloud to different geographic locations to take advantage of savings found, for example, when data is moved to a different server location because the new location has less network traffic during certain times of day. The ability to preserve data may be complicated by the constant movement of information in the cloud. Further, the data to be preserved and collected is physically with a third-party and may not easily be in the agency's or the company's reach. Collecting data and its associated metadata from the cloud may be challenging because many cloud providers may not provide access to the original metadata.

In the civil context, at the very start of a case or when litigation is reasonably anticipated, a litigation hold must be issued to prevent the spoliation of potential evidence. *See, e.g.*, *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212 (S.D.N.Y. 2003). In the criminal context, the triggers for preservation may be different but organizations will have certain preservation obligations. These obligations may be statutory. The Sarbanes-Oxley Act of 2002, 18 U.S.C. § 1519 (2002) provides, for example, that

> [w]hoever knowingly alters, destroys, mutilates, conceals, covers up, falsifies, or makes a false entry in any record, document, or tangible object with the intent to impede, obstruct, or influence the investigation or proper administration of any matter within the jurisdiction . . . of the United States . . . or in relation to or contemplation of any such matter . . . shall be fined . . . [or] imprisoned not more than 20 years, or both.

Id. It remains unclear how courts will interpret and litigators will implement these preservation requirements given how cloud providers store and move data. It is also unclear how the collection and production of data from the cloud will affect the development of law regarding the production of metadata in response to discovery requests in litigation. *See, e.g.*, *Aguilar v. Immigration and Customs Enforcement Div. of the U.S. Dep't of Homeland Security*, 255 F.R.D. 350 (S.D.N.Y. 2008) (observing the relationship between a document and its metadata for production); *Williams v. Sprint/United Mgmt.*

Co., 230 F.R.D. 640, 652 (D. Kan. 2005) (explaining that metadata is an inherent part of an electronic document). Depending on the system configuration and cloud services, the original metadata for data stored in the cloud may no longer technically exist. A further discussion of the practical effect that cloud computing has on a litigator's practice continues below.

V. Potential opportunities for litigators in the cloud

In the search for evidence, several potential benefits are available for litigators if a client agency or investigation target uses cloud computing to store their information. First, email and data in the cloud will be centrally located as opposed to dispersed across different systems, programs, organizational divisions, and physical locations. As a result, subpoenas, civil investigative demands, or document requests seeking information from these centralized systems should yield faster responses. Collecting email, for example, will start at a centralized entry point instead of beginning with an exhaustive search through multiple, isolated systems.

Second, but not wholly unrelated to the first, data stored in the cloud should lend itself to faster and easier electronic searches. Instead of an agency searching each sub-agency email system separately, it will be able to perform one top level search over all agency email. The email software would also be consistent organization-wide, rather than one department using Microsoft Outlook, one using GroupWise, and another potentially using Lotus Notes. Further, if the cloud systems are originally configured with E-Discovery in mind, the cloud technology may have built-in search capabilities. Consequently, the amount of time and effort saved searching for evidence could be substantial. The litigator may want to inquire about the search functionality of the system in advance of issuing discovery or an inquiry so that search requests can be more effective.

A third potential advantage for litigators is that the data will be held by a third-party, the cloud provider. In some circumstances the investigator or requestor may be able to obtain that data without notice to the data owner. *See* Stored Communication Act, 18 USC §§ 2701-2708 (2010). *But see United States v. Warshak*, No. 08-3997, 2010 WL 5071766, at *14 (6th Cir. Dec. 14, 2010) (holding that "a subscriber enjoys a reasonable expectation of privacy in the contents of his emails 'that are stored with, or sent or received through, a commercial ISP.'").

Fourth, a user may have less ability to actually destroy or alter evidence because the data now sits with a third-party. Cloud providers may establish processes that control what and how a person may, for example, delete a document. The cloud provider's disaster recovery and back up procedures may prevent a culpably-minded person from permanently destroying electronic evidence in the cloud. The cloud provider's procedures may aid a litigator in capturing and locating potential evidence that might have otherwise been lost if the data solely resided with the user or an interested party.

Finally, more data, and therefore more evidence, may be accessible to litigators. In addition to the move towards information remaining actively and more easily accessible online, as opposed to being removed and placed on a disaster recovery system such as back up tapes, cloud computing may feed into users natural tendencies to store more than necessary. The cost to store data in the cloud will continue to decrease; therefore, the motivation to only create and store what is absolutely needed will also decrease. Consequently, more information may be generated and retained, depending on the existence and compliance with an organization's records management policies.

VI. Potential disadvantages of cloud data storage for litigators

The many benefits of cloud data storage are nonetheless accompanied by potential disadvantages for litigators. First, an organization using cloud computing for storage may not have the knowledge or ability to implement a hold on data that may be potential evidence. If document retention needs were not addressed by an organization when developing their terms and requirements with the cloud provider, their attempts to preserve information may be undermined by the cloud provider's normal data recycling processes and procedures, despite potential good faith efforts by the users. The cloud providers may not be able to suspend their own procedures because such suspension may affect other unrelated users. The evidence may be gone before the litigator even knows it existed unless the user takes proactive preservation steps to avoid loss of important data or evidence.

Second, debate over what information the agency or organization has custody or control over may substantially increase. This debate may be both factual and legal. In the past, an organization's email, for example, was found on the organization's computers, network, and servers because the organization owned and controlled the physical location of the information. With the rise of cloud computing and with the data being stored by a third-party's system, more debate as to whether the data is within the control of the company may naturally arise.

Case law suggests, however, that courts may find the data in the control of the company even if it is found with a third-party. In *Flagg v. City of Detroit*, 252 F.R.D. 346 (E.D. Mich. 2008), the court held that the Stored Communications Act did not preclude discovery of a city's relevant, non-privileged electronically stored communications that were maintained by a non-party service provider but remained within the city's control. The court evaluated whether control existed under FED. R. CIV. P. 34(a), which states that a party may request disclosure by another party of information that the responding party has within its "control." *Id.* at 358-66. The court concluded that control under FED. R. CIV. P. 34(a) existed because the city had a contract with the service provider. It based its reasoning in large part on the fact that the city could permit disclosure by granting consent because it could "block" disclosure by withholding consent. *Id.* at 355.

The extent of control under FED. R. CIV. P. 34 by a person or entity may depend on other statutes. For example, in *Tomlinson v. El Paso Corp.*, 245 F.R.D. 474 (D. Colo. 2007), pension plan participants sued their employer under the Employee Retirement Income Security Act (ERISA) and moved to compel the production of electronically stored information (ESI). *Id.* at 476. The ESI was stored with a third-party that refused to produce part of the ESI, arguing that part of it was proprietary. *Id.* at 475. The court examined the concept of control under FRCP 26(a)(1)(B) and compelled production under FRCP 34(a), stating that "Rule 34(a) enables a party seeking discovery to require production of documents beyond the actual possession of the opposing party if such party has retained any right or ability to influence the person in whose possession the documents lie." *Id.* at 476-77. The court reasoned that because a duty arose under ERISA to maintain records, the employer was in possession of the documents and may not "delegate [its] duties to a third-party under ERISA." *Id.* at 477.

Even without a statute, courts will likely construe the concept of control broadly. In *Goodman v. Praxair Services, Inc.*, 632 F. Supp. 2d 494 (D. Md. 2009), the court stated that "Rule 34 'control' would not require a party to have legal ownership or actual physical possession of any documents at issue." *Id.* at 515. Instead, documents are considered to be under a party's control when that party has "the right, authority, or practical ability to obtain the documents from a non-party to the action." *Id.* (quoting *In re NTL, Inc. Sec. Litig.*, 244 F.R.D. 179, 195 (S.D.N.Y. 2007) (a securities litigation case where the district court found that successor entities still had "control" over ESI arising from a cooperative file-sharing system)).

While some may argue that the data remains within the organization's control when the data is in the cloud, legitimate factual arguments may exist suggesting that the evidence sought is not actually in the organization's control. The outcome may depend on how the services are arranged with the third-party. For example, Twitter allows users to retrieve only up to 3,200 of their last tweets. Twitter retains all tweets sent by a user in its archived system but the user only has access to the last 3,200 messages. *See* TWITTER HELP CENTER, http://support.twitter.com/entries/13920-frequently-asked-questions. Therefore, organizations may not be physically able to reach the evidence even if it exists in the possession of a third-party.

Third, if the data in the cloud is difficult to manage or retrieve for litigation purposes, courts may be disinclined to sympathize with discovery difficulties. Courts may view cloud computing as a normal business function where the data cannot be made inaccessible when the organization should have known of potential E-Discovery needs when incorporating cloud computing into their systems. In *Radian Asset Assurance, Inc. v. Coll. of the Christian Bros. of N.M.*, No. CIV 09-0885 JB/DJS, 2010 WL 4928866 (D.N.M. 2010), Plaintiff, Radian Asset, sought production of ESI from the Defendant College. The college had sold its assets, including ESI on backup tapes, to a third-party. College subpoenaed the third-party to produce the ESI. The third-party proceeded to produce, but Radian Asset argued that the format of the ESI was not the same format as the "usual course of business" under FRCP 34(b)(2)(E). *Id.* at *1-2. The district court disagreed and found that it was common for businesses to transfer ESI to backup tapes. The district court stated that:

> Businesses commonly store data in increasingly less accessible formats as the data loses currency, and the data is retained primarily for archival purposes. It is common to move data from on-line storage, where it is quickly accessible through networks, to near-line storage robotic storage devices - where data can be retrieved after a short delay, and eventually to offline or archival storage, such as tape backups.

Id. Courts may not be receptive to hearing from organizations whose data has, in the normal course of business, been sent to the cloud but is not easily accessible.

Finally, although access to a large amount of information may be beneficial, the volume of data may actually be a hindrance depending on which side of the request the litigator is on. When defending an agency that has moved its data to the cloud, the potentially voluminous data must still be reviewed and produced in some way in response to a discovery request. The more data a cloud stores, the more work to determine relevancy and privilege. One terabyte of data can cost less than $100 to store but more than $1 million in litigation costs to collect, processes, review, and produce. A caveat to this concern is that with advances in technology, smarter automated tools will be able to help alleviate this problem by increasing efficiency when reviewing large volumes of information in the cloud. The potential help these tools provide becomes available if one has access to these resources. The investment in and access to litigation technology in handling the data in discovery may, however, very well lag behind the rise in storing data in the cloud.

The challenges that litigators face with either a client agency or organization using cloud computing for data storage are best addressed by taking a proactive position on this new movement and developing E-Discovery strategies at the earliest stages of the case.

VII. Suggestions for the twenty-first century litigator facing the cloud

In this changing world, litigators must learn how to adapt. Given these cloud computing challenges and opportunities, several practical steps are available for litigators to take in adjusting to these changes. First, attorneys need to work closely with IT and technical staff to understand what is stored in the cloud, what the terms of that storage agreement are, and the options for retrieving that data. To learn about where the evidence is, the litigator may have to issue a document request or subpoena for the cloud terms and data policies or, in the civil context, seek a Fed. R. Civ. P. 30(b)(6) deposition of the relevant IT personnel.

Second, attorneys may want to notify the organization to preserve the potentially relevant information in the cloud at the very outset of the case. Litigation holds should not be overly broad, but rather should be accurate in scope and related to the inquiry. As discussed, the challenge with data in the control of a third-party is that it may not be retained or easily retained after time has elapsed. By notifying the client agency, for example, of the need to preserve the relevant data in the cloud, the agency will activate the preservation steps they hopefully negotiated with the cloud provider in the contract, before normal data management procedures delete the information. In contrast, in investigations and affirmative litigation, if a litigator notifies the target organization up front that any relevant data in the cloud must be preserved–depending on the strategy for providing notice of the ongoing investigation–then the organization risks potentially serious ramifications, such as an obstruction of justice charge, if the data is destroyed.

Third, the best way to deal with many of the challenges caused by cloud computing is to reach an early understanding with opposing counsel. Litigators should negotiate the scope of discovery to reflect what is needed because the volume of potential data in the cloud may be large. Consequently, the need to process and review that data may threaten to slow the investigation or litigation. In the defensive context, the attorney will want up front and early limitations on discovery, potentially limiting the searches by custodian, time frame, location, or topic, so that preservation, search, and collection can be done by the agency in a more streamlined and cost-efficient manner. In the civil context, the concept of discovery effort being proportional to the case is becoming a more acceptable argument used to limit the scope of discovery. *See e.g.*, Sedona Conference®, Commentary on Proportionality in Electronic Discovery, October 6, 2010. *But see Orbit One Communications, Inc. v. Numerex Corp.*, No. 08 Civ. 0905 (LAK) (JCF), 2010 WL 4615547 (S.D.N.Y. Oct. 26, 2010). In the affirmative context, the litigator needs to understand the proper scope for their request so that they are not buried in irrelevant or unusable data.

Fourth, litigators should be prepared for arguments regarding the burden and cost of discovering data from the cloud and be prepared to educate the court and opposing counsel. Litigators, both requesters and responders to discovery, must educate themselves on the technology employed at their client agency or target or the litigator risks missing valuable opportunities and evidence. A partnership between the litigator and their litigation technology or IT resources is essential for litigators to make persuasive and accurate arguments.

Finally, a litigator may consider being more involved in the early stages of discovery by engaging in reviews of sample sets of data or search results. This will help to determine early on if the discovery strategy is accurately capturing and producing the evidence requested from the cloud.

VIII. Conclusion

In the twenty-first century, electronic evidence is rapidly moving to the cloud as companies, local governments, and federal agencies embrace cloud computing. As a result, potential evidence is being stored with third-parties in virtual warehouses. Those who litigate against or on behalf of organizations using cloud computing should adapt their discovery strategies and leverage the technological advances to their advantage when confronted with this new technology. In the final analysis, the question remains the same: Where is the evidence?❖

ABOUT THE AUTHORS

❑**Allison C. Stanton** is the Director of E-Discovery for the Civil Division of the U.S. Department of Justice. Among her responsibilities, Ms. Stanton develops E-Discovery policies, practices, and training for the Civil Division, works with the other Department Divisions on E-Discovery initiatives, advises federal agencies on E-Discovery matters, and provides guidance on proposed changes to procedural rules, regulations, and legislation affecting E-Discovery. Ms. Stanton is also the Chair of the D.C. Bar E-Discovery Committee. She is an established author and has spoken at national and international E-Discovery conferences.

❑**Andrew J. Victor** joined the Department of Justice in 2010 through the Honors Program as a Trial Attorney with the FTCA Staff of the Torts Branch. He handles a range of FTCA litigation matters and is an E-Discovery Coordinator for his office.✠