MAYER·BROWN

Electronic Discovery & Information Governance

2018 TIPS OF THE MONTH - A Compilation

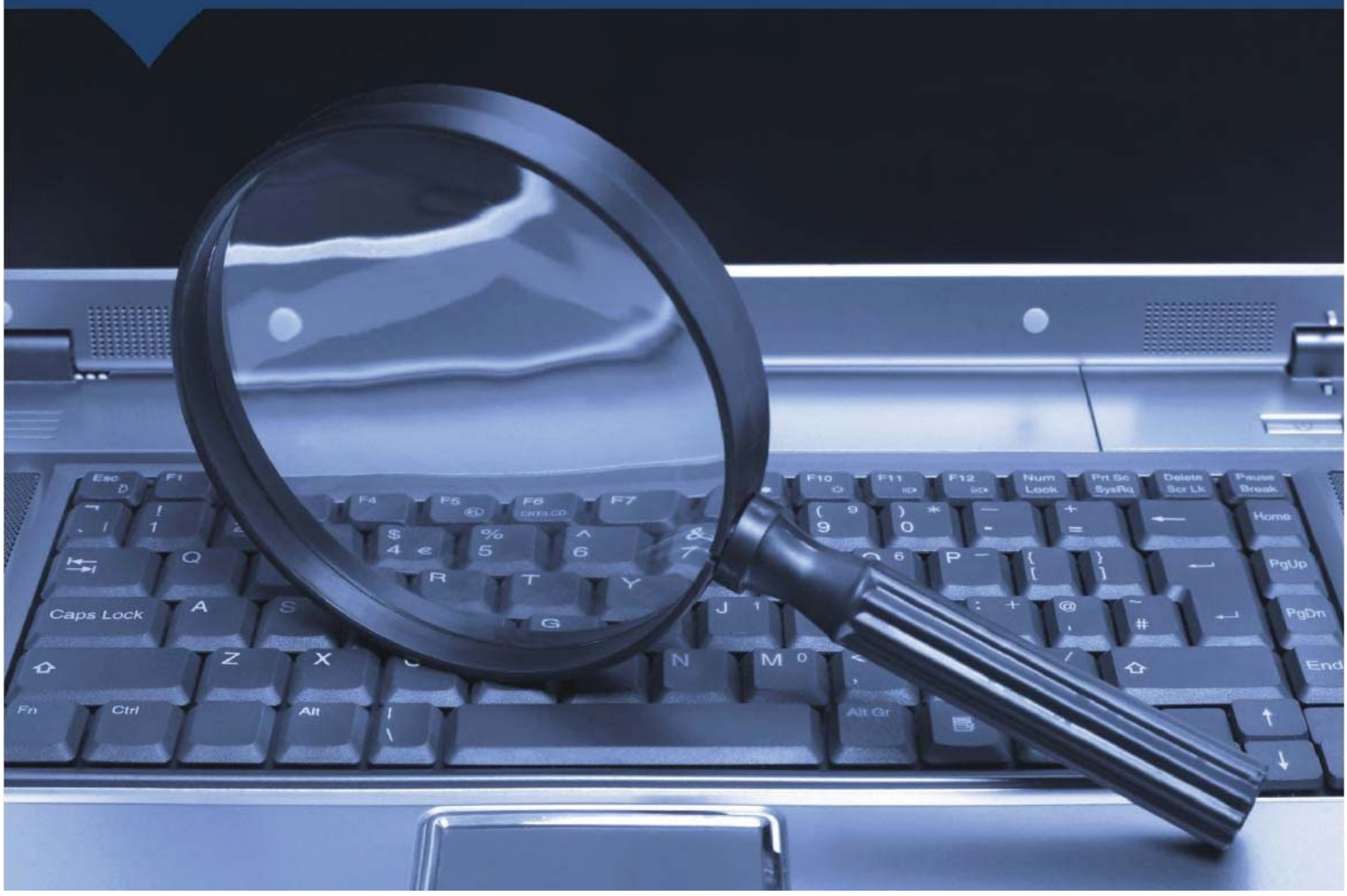
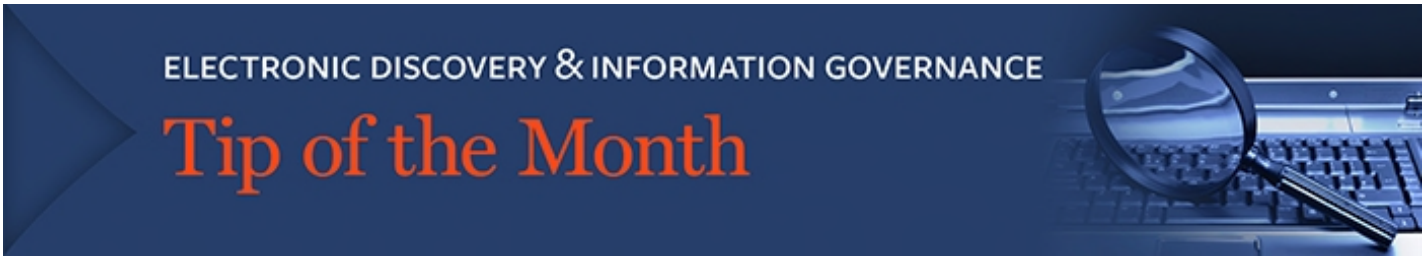


TABLE OF CONTENTS



Introduction

2018 continued a trend of significant vendor consolidation in the e-discovery and information governance space, return to form in delaying the time to answer the complaint and in triggering other discovery options after a motion to dismiss is filed under the Northern District of Illinois' Discovery Pilot Program and a growing conversation around BYOE (Bring Your Own Email) versus BYOD (Bring Your Own Device). However, the most significant events of 2018 involved the implementation and enactment of the General Data Protection Regulation ("GDPR") by the EU; passage of the US Clarifying Lawful Overseas Use of Data Act (the "CLOUD Act"), mooting Microsoft's challenge to the extraterritorial application of the Stored Communications Act in the Supreme Court; and the continued grappling by US courts and litigants on how to apply the 2015 Amendments to the Federal Rules of Civil Procedure.

Each of these three seminal topics was discussed in Mayer Brown's Electronic Discovery & Information Governance Practice Tips of the Month series in 2018 and are recapped below. We begin with the enactment of GDPR in May 2018 and the initial investigations and fines issued. Next, we move to the CLOUD Act and its implications on cross-border seizure of data. Finally, we discuss the renewed focus on proportionality and further consideration of defensible disposition as a consequence of changes to Rule 37(e) as part of the 2015 Amendments.

GDPR Comes to Life. In 2019 individual EU member states will continue to flex GDPR muscle as they will likely go after larger and more well-known companies. Below is a look back at GDPR actions and fines in 2018 since the regulation took effect on May 25, 2018:

- In July, Portugal's Commissao Nacional de Proteccao de Dados ("NCPD") hit a hospital with a 400,000 Euro fine for allowing employees indiscriminate access to patient data.
- In September, the UK's regulator, the Information Commissioner's Office ("ICO"), accused AggregateIQ, a Canada-based company, of using names, email addresses, and other personal data to target UK individuals with political advertising messages on social media. The ICO ordered the company to erase any UK individuals' personal data retained on its servers.
- In October, Austria's Osterreichische Datenschutzbehorde ("DPA") issued a 4,800 Euro fine to a retail company that used a surveillance camera that captured too much of the sidewalk. The DPA cited that the retailer lacked the GDPR's required notice and transparency.
- In November, France's CNIL found that Vectuary, a mobile ad network, illegally obtained the consent of more than 67 million people. CNIL ordered the company to change its consent practices and purge all data collected on the basis of the invalid consent obtained.

- Later in November, Germany's Data Protection and Freedom of Information Baden-Wuettemberg ("LfDI") issued a fine of 20,000 Euros after a data breach at a social media company, in which a hacker stole and published passwords.

SCA and the CLOUD Act. Courts continue to be faced with questions regarding whether certain communications are properly within the realm of the Stored Communications Act (the "SCA") and just what constitutes being retained "for backup protection." The biggest development in this area was the passage of the CLOUD Act, which the Supreme Court found mooted Microsoft's challenge to the extraterritorial application of the SCA. The overall impact of the CLOUD Act remains to be seen, but, for SCA purposes, it is now clear that the government can obtain data stored overseas in certain circumstances.[1]

Court's Application of 2015 Federal Rule Amendments. The courts' continued application of the amended rules in 2018 consumed much of the year in e-discovery. Two areas of continued focus were Rules 26(b)(1) (proportionality) and 37(e)(spoliation sanctions).

- **Focus on Proportionality.** The 2015 Amendments to the Federal Rules of Civil Procedure noted that in some cases discovery of relevant information may not be proportional to the needs of the case, which refocused attention on the role of proportionality in discovery. Since December 2015, many courts have sought to apply the proportionality factors to determinations of the appropriate scope of discovery in the particular case at issue. Under Amended Rule 26(b)(1), the scope of discovery is limited to documents and information that are both relevant to the claims and defenses in the specific matter and proportional to the needs of the case. The responsibility to ensure that discovery is proportional to the needs of the case is on all parties and the court. However, in recent practice, much of the effort to establish that certain discovery is disproportionate falls on the responding party or the judge, as requesting parties too often shoot for the moon. While in some cases the court can determine that specific requests are facially disproportionate, in other instances, the court looks to the producing party to demonstrate with specificity why specific requests are not proportional to the needs to the case. In these situations, most responding parties (including third parties) attempt to argue undue burden and/or cost. In such cases, the producing party needs to offer more than just boilerplate objections and instead provide actual costs and/or realistic estimates. In addition, there are certain types of discovery that are generally not proportional without a showing of a deficiency in the producing party's production, such as (1) discovery-on-discovery, (2) unfettered direct access to the responding party's ESI and (3) requests for searches of all company databases when the case involves only a narrow issue or specific set of custodians. In 2019 and beyond,

[1] *See United States v. Microsoft Corp.*, 138 S. Ct. 1186 (2018).

parties need to be aware of attempts to improperly expand the scope of discovery and the need to educate the court on the specific burden the producing party faces.[2]

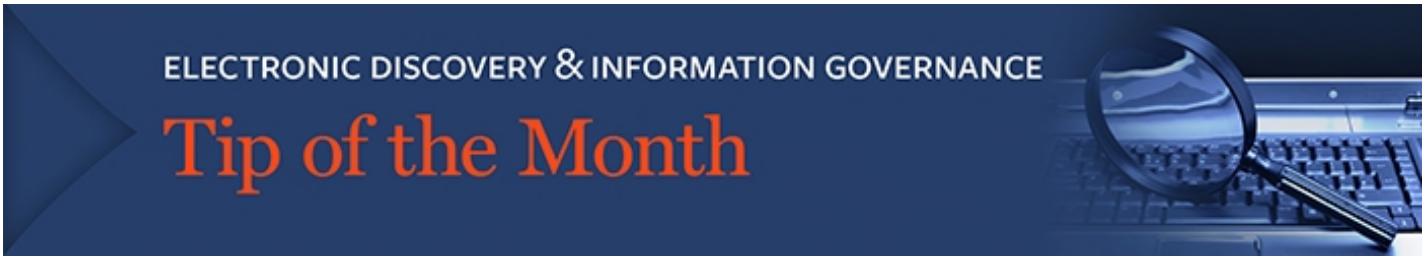
- **Changing World of Spoliation Sanctions Under Amended Rule 37(e).** Overall Rule 37(e) appears to have had its intended impact in terms of lessening the threat of or use of spoliation motions as a tactical weapon in the context of civil litigation. Courts are finally focusing on the predicates to the Rule that require, before sanctions/curative measures can be imposed, that (i) there was a loss of ESI, (ii) the ESI is relevant and proportional to the claims and defenses, (iii) the party in question failed to take reasonable steps to preserve the ESI and (iv) the ESI could not be replaced from other sources. We have seen that courts are increasingly inventive in their use of "curative measures" short of "severe" sanctions. One important outstanding question is whether courts can, or should, apply the Rule 37(e) approach to spoliation of tangible things and/or hard copy documents.[3] This more reasoned approach to Rule 37(e) sanctions has led to many companies considering resuming on-the-books but not strictly enforced document retention policies and seeking defensible means of disposing unneeded data.

For inquiries related to this Tip of the Month, please contact author Oral D. Pottinger.

To learn more about Mayer Brown's Electronic Discovery & Information Governance practice, contact Michael E. Lackey, Eric B. Evans or Ethan A. Hastert.

[2] For two such examples of proportionality-related decisions, *see Bell v. Pension Committee of Ath Holding Co., LLC*, (S.D. Ind. June 14, 2018) (where the court granted motion to compel production of Facebook messages, noting that the plaintiff's testimony established the messages' relevance to the parties' claims and defenses and that the plaintiff had not presented any evidence that it would be burdensome for the messages to be collected) and *Brewer v. BNSF Railway Co.*, 2018 WL 882812 (D. Mont. Feb. 14, 2018) (where, the court upheld a magistrate's decision denying discovery-on-discovery, stating that the plaintiff's request still needed to be proportionate to the needs of the case, and found the Sedona Conference Commentary on Defense of Process: Principles and Guidelines for Developing and Implementing a Sound E-Discovery Process persuasive, noting that "[a] party should not be required to provide discovery about its e-discovery without good cause" and that "[a] party seeking discovery on discovery ('meta discovery') must show a specific deficiency in the other party's production").

[3] One example where the pursuit of spoliated evidence went wrong was in *Klipsch Group, Inc. v. EPRO E-Commerce Ltd.*, 880 F.3d 620 (2d Cir. 2018). While certainly courts have an interest in deterring "recalcitrant parties from the cavalier destruction of concealment of materials that the law requires them to retain and disclose," amended Rule 1 also places on both the parties and the court a responsibility to efficiently resolve cases. In light of that responsibility, the drafters certainly did not intend any party to run up a $2.7 million legal tab in pursuit of spoliated evidence in a case with $20,000 at issue, as the plaintiffs did in *Klipsch*.



Impact of New EU Privacy Law on US E-Commerce Businesses

27 February 2018

Scenario

A company headquartered in the US uses its online store to sell products to customers located in the European Union ("EU"). Prices are displayed in euros, and the company offers international delivery to the EU. The US-based general counsel wants to know more on how the company's e-commerce activities will be affected by the EU General Data Protection Regulation.

What is the EU General Data Protection Regulation?

The General Data Protection Regulation ("GDPR") introduces a new privacy framework in the EU and will come into force on May 25, 2018. The GDPR will replace existing EU data protection laws and bring about significant changes and requirements that will have a wide-ranging impact worldwide on the way organizations handle and use data.

The GDPR is a real game changer for e-commerce businesses and online stores. Those companies, by their nature, receive and process a vast amount of personal data and have cross-border activities.

GDPR considerations for e-commerce businesses

The main issues that companies engaged in e-commerce should take into account when implementing policies and procedures in compliance with the GDPR are related to:

1. **The territorial scope**

   The GDPR will apply to organizations established outside of the EU when they process personal data in connection with: (a) the offering of goods or services to an individual in the EU and/or (b) the monitoring of the behavior of an individual in the EU. As a consequence, companies that offer products and services to individuals in the EU via their websites or other online platforms will now have to comply with EU data protection rules.

   The mere accessibility of the company's website from the EU will not be sufficient to trigger the application of the GDPR. For the new regulation to apply, the company must clearly intend to offer services to individuals located in the EU, for instance by mentioning EU currency, by referencing EU customers or by presenting ordering information in an EU language (when this is not the language generally used in the country where the company is based).

2. Legal basis for processing

Companies will need to identify a legal ground for their processing activities. In this regard, the main change introduced by the GDPR relates to consent, which now requires a clear affirmative action by the data subject—silence, pre-ticked boxes, inactivity, failure to opt-out or other such mechanisms will not be enough to qualify as valid consent.

E-commerce businesses should keep in mind that the GDPR allows for processing of personal data on other legal grounds, including if the processing is necessary for the performance of a contract with the data subject. This legal basis applies to data required to process an online payment or deliver the purchased product. In such cases, there is no need to get consent.

Companies seeking to rely on such alternative grounds should conduct a necessity test to determine if only the information necessary for the purposes of the contract is being collected. When requiring other personal data (e.g., personal data for use beyond the primary purpose of processing a payment, filling an order, delivering the purchased good, etc.), the company will need to identify another legal basis (e.g., consent or legitimate interest). This is especially relevant when customer data are used for marketing or advertising purposes.

3. Retention periods

Under the GDPR, personal data should not be retained longer than necessary. As a consequence, companies should delete personal data when the purpose of the processing has been achieved. For example, personal data collected when a good is purchased should be deleted at the end of the contract. However, companies might want to keep all or some of the data. In those circumstances, companies should find other grounds for keeping the data—for example, the need to retain to comply with legal requirements that might apply under national law.

4. Privacy notices

The GDPR requires companies to inform data subjects on how their personal data are being processed. Specific information must be provided, such as the purpose and the legal basis for processing, whether personal data are shared with third parties, if the company conducts profiling activities, etc. E-commerce businesses will have to provide data privacy notices at the time personal data are obtained. For this purpose, a link to the terms and conditions and to the privacy notice of the company should be displayed when the customer purchases goods online, and privacy notices may need to be updated to comply with the GDPR.

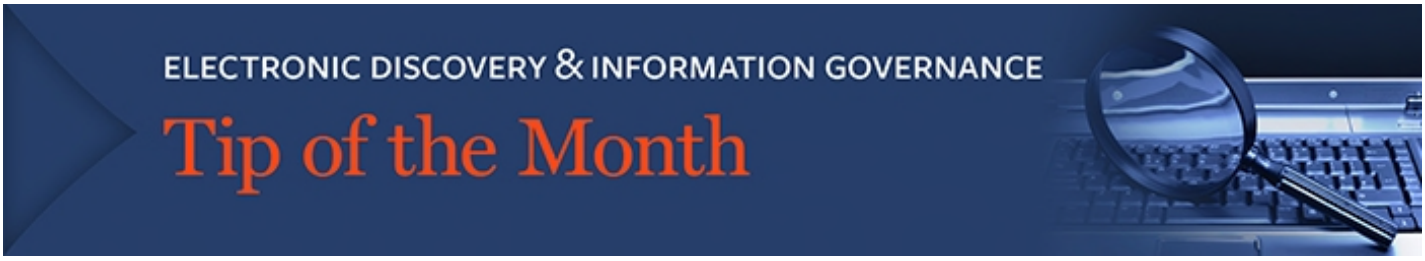
5. **Data subjects' rights**

   The GDPR strengthens data subjects' rights. It introduces new rights such as the right to be forgotten, the right to data portability and the right to restrict the processing. Companies should also allow their customers to exercise these rights. And to comply with their obligations, online stores and e-commerce businesses should ensure that customers are in control of their personal data, being able to access and modify the data. To facilitate meeting these requirements, companies should provide information on whom customers can contact regarding their data privacy concerns.

6. **Contracts with third parties and international transfers**

   Companies involved in e-commerce activities often outsource components of these activities, such as payments, marketing or IT. Under the GDPR, whenever a data controller (the e-commerce company) uses a processor (a third party who processes personal data on behalf of the controller), the controller needs to have a written contract in place that includes certain specific terms such as data processed and duration, obligations such as data breach reporting and audit assistance, use of technical measures, etc. Outsourcing agreements should be reviewed and, where necessary, renegotiated to ensure that companies are appropriately supervising the manner in which they process personal data and that the specific required provisions are included. When service providers are located outside the EEA (European Economic Area), legal mechanisms for carrying out personal data transfers should also be identified.

For inquiries related to this Tip of the Month, please contact authors Charles-Albert Helleputte or Diletta De Cicco or contributors Mark A. Prinsley, Lei Shen, Oliver Yaros or Kendall C. Burman.



The Thin Cyber Line — Be Aware of an ESI Custodian's Personal Email Accounts

30 March 2018

Scenario

A company is a party to long-running complex commercial litigation. The case's fact discovery deadline is a month away when opposing counsel alerts the company's outside counsel to a series of recently produced emails. The emails show that several of the company's custodians used personal Gmail email accounts for business purposes. Citing discovery obligations, opposing counsel demands the Gmail accounts be collected and reviewed for relevant materials. The company's general counsel asks outside counsel what are the risks of refusing to collect and review the Gmail accounts and why the accounts were not previously identified as potential sources.

The Pitfalls of "Bringing Your Own Email" to Work

In some companies, employees engage in "Bring Your Own Email" ("BYOE"), using personal email accounts to conduct business. BYOE poses different risks, costs and discovery consequences than "Bring Your Own Device" ("BYOD")—using, with the employer's permission, a personal mobile device to access the employer's information systems and applications for work purposes.

The business and practical reasons for distinguishing between BYOE and BYOD are clear. BYOD can increase employee productivity, enhance IT functionality by catering to user preferences and cut costs. BYOD decentralizes a company's information governance regime but through a secure, controlled electronic platform that is engineered to protect and preserve the company's data. Companies can—and do—live with that cost-benefit tradeoff.

Often done without the employer's knowledge, BYOE, on the other hand, can result in potentially relevant electronically stored information ("ESI") sources and discoverable information being inadvertently overlooked. Such a scenario exposes companies to increased eDiscovery and litigation risks and costs and may create information governance risks implicated by BYOE concerning the security, control and privacy of company and client data.

Employee's Personal Email Files Can Be Discoverable in Certain Cases

Courts have held that a party's employees' personal email accounts may be discoverable when used for work purposes—and not just where employees are a named party alongside their employer.

Competing Legal Standards Create a Risk of Discoverability

Courts are split on what test applies when determining whether an employer has sufficient possession, custody or control of an employee's personal email account under Rule 34(a). Some courts apply the liberal "practical ability test" while others apply the more restrictive "legal right test."

Under the "practical ability test," courts conduct a fact-intensive balance inquiry to determine if a party can realistically obtain the discovery sought from its employees, directors, agents or affiliated non-parties. The factors courts consider under this analysis include whether the individual is subject to firing from the employer.

Courts conducting a "legal right test" take a narrower view of possession, custody or control under Rule 34(a). For example, courts consider factors such as whether a contract or other legal right exists entitling the party to access its employees' personal email files.

The Impact of Employees Being Named Parties

Not surprisingly, where the employee is also a party, courts have held that neither the company nor the employee can shield a personal email account from discovery simply by contending that their business emails and documents were searched for relevant materials. Rather, the employee bears the obligations of a party under Rules 26 and 34, and personal email accounts are not protected from discovery simply because they are personal email accounts.

Strategies and Best Practices for Addressing BYOE

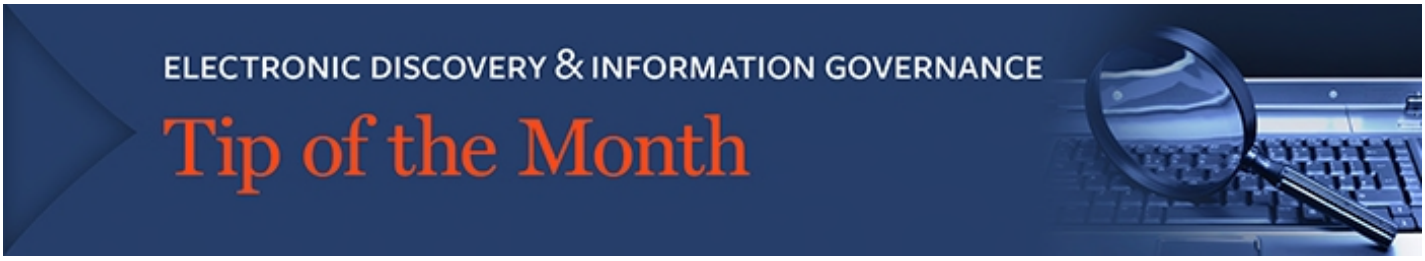
The practice of employees conducting business on personal email accounts can present challenges in the litigation discovery context that in-house and outside counsel should be aware of. Companies and their counsel should consider taking appropriate steps to minimize the cost and risk associated with BYOE, including:

- Understanding their employees' BYOE practices and considering rules prohibiting employees from using personal email accounts for work purposes.
- Considering requiring that employees obtain BYOE approval from company compliance personnel or in-house counsel and/or agree to make personal email accounts available to the company for business or litigation purposes.
- Addressing BYOE in litigation holds by directing employees to identify to in-house or outside counsel whether the employees use BYOE for any purpose and requiring employees to preserve business-related data in their personal email files.
- Addressing BYOE practices during pre-collection, custodial interviews.

Conclusion

Whether a court will observe and respect the thin cyber line dividing our work and personal lives depends on how well we ourselves observe that line. When we use our personal email for work, opposing counsel and courts are less likely to be swayed by a privacy argument. BYOE is an extension of our BYOD business culture. But it comes with much different risks, costs and discovery consequences—and also implicates other paramount corporate information governance concerns (e.g., data security, control and privacy). Companies and their lawyers are well-advised to be aware of BYOE.

For inquiries related to this Tip of the Month, please contact author Joshua A. Faucette.



US Customs and Border Protection Searches of Electronic Devices: Ethical Issues for Lawyers

2 May 2018

Scenario

Waiting to pass through customs is a tedious but unavoidable part of international travel. But US Customs and Border Protection (CBP) policies also introduce complex ethical headaches for lawyers crossing the US border.

The outside counsel for a multinational company that is the defendant in a lawsuit is traveling to a country outside the United States. The company's general counsel asks the outside counsel, "What will you do if a US customs agent asks to see your email? There are lawyer-client communications in there."

CBP Guidelines for Searches

CBP has the authority to search electronic devices—without a warrant—at ports of entry, such as international airports, road and rail crossings at the border, and within 100 miles of the border. While these searches are rare, CBP can review content saved on devices, but cannot search cloud data.

Earlier this year, CBP issued a directive, CBP Directive No. 3340-049A, January 4, 2018 ("CBP Directive"), to provide guidance on how CBP intends to use its power to conduct searches of electronic devices. The CBP Directive:

- Provides that devices may be "presented" or "detained" for inspection. "Presentment" means a response to a Customs agent's demand to inspect an electronic device.
- Permits searches of both inbound and outbound travelers.
- States that a search "include[s] an examination of only the information that is resident upon the device." This is an important restriction on the scope of a search by CBP.
- Describes both "basic" searches, which examine the device and its contents, and "advanced" searches, which may involve forensic equipment and copying.
- Provides that device searches will usually occur in the device owner's presence.

The Duty of Confidentiality

For many travelers, the requests above raise no ethical issues. But lawyers' computers and phones often contain lawyer-client communications and clients' confidential information. And state bar ethical rules impose a duty not to disclose privileged and client-confidential information. Statutes and regulations

may also require lawyers to protect a client's personal data. There is no customs-search exception to this duty.

In general, lawyers should make sure that any customs search does not violate these obligations. The NY City Bar Association's Formal Legal Opinion 2017-510 suggests how to balance these obligations with CBP regulations.

The opinion states that:

- A lawyer has a duty to take reasonable steps to protect client confidences;
- A lawyer may comply with a demand by a border officer with lawful authority;
- But a lawyer should make reasonable efforts to dissuade the border officer from reviewing a client's confidential information or to limit the extent of that review.

Reasonable Efforts to Keep Client Information Confidential

"Reasonable efforts" in this context might include:

1. Putting devices in airplane mode before approaching a border area. The CBP Directive clarifies that only information resident on the device may be searched. Airplane mode cuts off network connections, which cuts off access to remote information.
2. Remaining polite, professional and truthful.
3. Being aware that a Customs agent may physically search a device. For example, an agent may search for contraband in the battery compartment.
4. Being prepared for the agent to ask for passwords or access to the device.
5. If an agent asks for a password:
    a. Confirming the authority of the border officer and the purpose of the search; and
    b. Confirming that the agent is requesting voluntary consent to search the device.

As discussed above, a lawyer's duty of confidentiality may require that the lawyer refuse. In most cases, the lawyer must take reasonable steps to protect a client's confidential information, taking into account the sensitivity of the information on the device and other relevant considerations.

If the client-confidentiality interest is strong and the agent persists, the lawyer should inform the agent of the lawyer's profession and that the device contains confidential information covered by lawyer-client privilege. For the former purpose, the lawyer should carry some form of professional

identification, such as a business card or a bar membership card. Some suggested language to inform the agent of the latter:

> I am a lawyer and this device contains information that is confidential and privileged. I am not permitted to show that information to anyone else, including you. I therefore cannot provide you with the [device/passwords] you are requesting. Under s.5.2 of CBP Directive 3340-049A, I request that you contact [your/CBP] counsel before proceeding.

If the agent insists on searching the device even after being informed of the lawyer's profession and duty to protect lawyer-client privileged information, what the agent can do depends on the lawyer's citizenship:

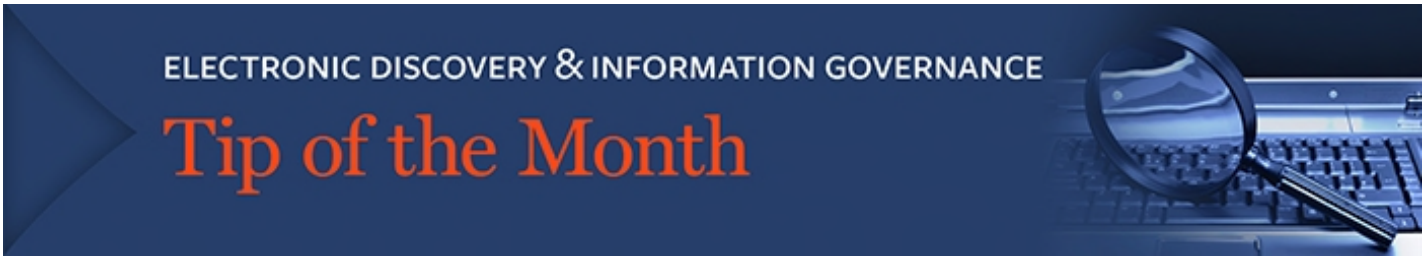
1. **A US citizen cannot be prevented from entering the United States**, even if they don't provide a password. However, not providing a password may result in delay and detention of the device.
2. **A Non-US citizens may be detained or denied entry**, and the agent may detain the device.

Next Steps

At this point, the border officer may escalate the matter to CBP legal counsel.

If CBP detains the device, the lawyer will receive a custody receipt. Devices are generally returned within five days.

For inquiries related to this Tip of the Month, please contact the author Eric B. Evans.



Illinois Ethics Guidance Warns Against Lawyers' Use of Snooping Software

31 May 2018

Scenario

An Illinois-based technology company is in settlement negotiations to resolve a lawsuit. The company's general counsel is considering using email tracking software in electronic communications with opposing counsel to determine when counsel opens any email attachments—such as a draft settlement agreement—and how much time opposing counsel spends reviewing each page of those attachments. Before moving ahead, the general counsel wants to know whether this use of email tracking software violates any professional conduct guidance.

State Bars See Ethical Perils in Email Tracking Software

Email tracking software has been earning the ire of an increasing number of state bar associations. The Illinois State Bar Association issued a Professional Conduct Advisory Opinion in January 2018 in which it concluded that a lawyer may not use this software in electronic communications with other lawyers or clients without first getting the consent of all recipients, citing threats to the attorney-client relationship and other ethical concerns.

The Illinois opinion followed similar conclusions reached by the state bar associations of Alaska, New York, and Pennsylvania, bringing the tally to at least four states that have found lawyers' use of email tracking software under various circumstances to be ethically impermissible.

What Is Email Tracking Software?

The Illinois opinion considered software applications that allow an email's sender to covertly monitor how recipients handle the email and its attachments. This tracking software will typically insert an invisible image or code into an email message, and the recipient will unknowingly activate that image or code upon opening the email.

The software then provides the email sender with information that may include:

- when the email was opened;
- the kind of device used to open it;
- how long the email was open;
- whether and what attachments were opened or downloaded;
- how long any attachments were opened;

- whether, when and to whom the email or attachments were forwarded; and
- the "general geographic location" of whatever device received the forwarded materials.

The Illinois State Bar Association specified that it was not concerned with the "read receipt" function offered by many email applications. That function lets an email recipient notify the sender of receipt. But by not providing information about what happens to an email after receipt, a read receipt does not present the same ethical issues as other tracking functions, according to the Illinois opinion.

Dishonesty and Deceit

The Illinois State Bar Association found that, at a minimum, the undisclosed, concealed use of email tracking software by a lawyer amounts to "dishonesty" and "deceit" under Rule 8.4 of the Illinois Rules of Professional Conduct, which provides that it is professional misconduct to "engage in conduct involving dishonesty, fraud, deceit, or misrepresentation."

"Any competent lawyer receiving an email from an opposing counsel would obviously wish to know that the opposing counsel is acquiring instantaneous and detailed private information concerning the opening and subsequent handling of the email and its attachments," the Illinois opinion recognized.

Invading the Attorney-Client Relationship

The undisclosed use of email tracking software also carries implications for attorney-client relationships. In examples cited in both the Alaska and Illinois opinions, a lawyer's surreptitious use of this software in email correspondence with another lawyer, while representing a client, would invade the relationship between the receiving lawyer and that recipient's client.

One example involved a client who had moved and did not want to disclose where she was now living. Email tracking software could enable opposing counsel to email that client's lawyer an attached document for the client's signature and would uncover the client's general location when she opened the forwarded email with that document.

In another example, the Alaska and Illinois bar associations both noted that using this software provides the sending lawyer with access to "protected information and extraordinary insight as to which sections of a document the lawyer and her client found most important."

Further, the Illinois State Bar Association found that communications between a receiving lawyer and insurers, co-counsel, co-clients, experts, investigators, accountants and other consultants involved in the matter can also result in intrusion into a lawyer's client representation. Illinois Rules 1.6(a) and 1.9(c)(2) protect the details of those communications—which qualify as confidential information related to a client representation—from disclosure by the lawyer, the Illinois opinion explained. Secretly obtaining that information should therefore be considered "an unwarranted intrusion in the client-lawyer relationship," according to that opinion. Here, the Illinois State Bar Association pointed to Illinois Rule

4.4(a), which bars a lawyer from using methods of obtaining evidence that violate a third person's legal rights.

Contrary to Rationale of Rule on Inadvertent Disclosures

Approving the undisclosed use of email tracking software would also violate the rationale of Illinois Rule 4.4(b), which requires lawyers who receive confidential client information and know that the information was inadvertently sent to promptly notify the sender to allow that person to take protective measures. The Illinois Rules should not allow a lawyer to obtain that same kind of information by stealth, the opinion said.

The Illinois State Bar Association has also concluded that a lawyer who finds out that opposing counsel has inadvertently transmitted confidential information, and learns this before opening the transmitted materials, should return those materials without examining them. The January 2018 opinion explained that if reading those inadvertently disclosed materials is improper, then it must also be improper for a lawyer to collect that information using undisclosed tracking software.

Key Takeaways

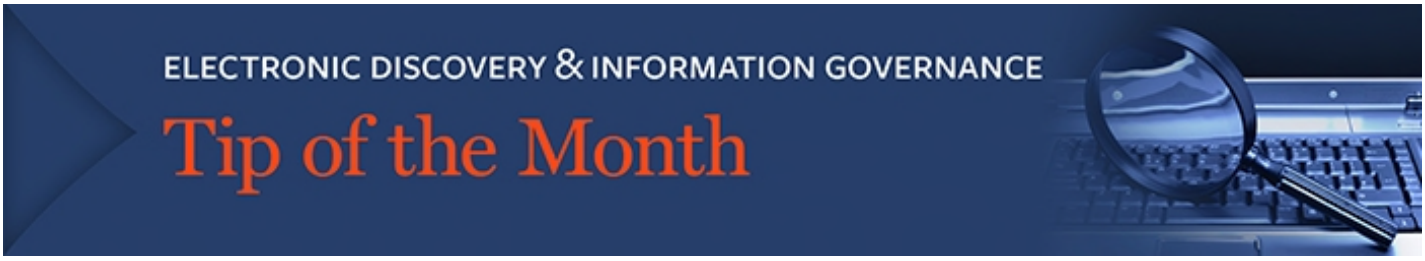
While finding the covert use of this software impermissible, the Illinois State Bar Association acknowledged that there does not appear to be any generally available, reliable program that can detect and defeat the use of tracking software. It also would be unworkable to force all lawyers in Illinois to keep tabs on various tracking programs as they become available and then immediately buy and install defensive software or devices—should they become available—to protect themselves, the Illinois opinion explained.

The Illinois State Bar Association directed that lawyers wanting to use tracking software when emailing another lawyer in connection with a client representation must first receive the informed consent of the receiving lawyer and any affected client. According to the Illinois opinion, an email seeking that consent must:

- Not contain tracking software;
- Contain no other substantive content; and
- Provide a "clear, explicit, and non-technical plain language explanation" regarding the features of the specific software that the lawyer wants to use.

Lawyers must also obtain the informed consent of their own clients to be able to use tracking software in communications with them, the Illinois opinion directed.

For inquiries related to this Tip of the Month, please contact the author Megan E. Stride.



Obtaining Evidence from Foreign Jurisdictions for Use in US Proceedings

28 June 2018

A multinational corporation with offices in both the United States and Great Britain has filed suit in the United States against the American subsidiary of a French competitor. The general counsel is unsure how to compel the production of relevant data stored on the defendant's servers in the European Union and is seeking advice as to the appropriate mechanisms for obtaining evidence from foreign jurisdictions.

The same multinational corporation is a defendant in British proceedings brought by a British competitor. Aware that much of the data relevant to this litigation is stored on the multinational corporation's American servers, the general counsel seeks to understand the scope of its production obligations when a foreign plaintiff seeks to compel evidence located on American soil for use in foreign proceedings.

Obtaining Evidence from Abroad

Through the Federal Rules of Civil Procedure

Pretrial discovery in the United States is famously expansive, particularly by comparison to foreign civil law jurisdictions. Under the Federal Rules of Civil Procedure, any party to US federal litigation can compel the discovery of evidence located in a foreign jurisdiction so long as the evidence requested is in the responding party's "possession, custody, or control." American discovery emphasizes the importance of "truth-seeking" in pretrial disclosure, and it is in this spirit that US courts construe "control" broadly. Depending on where its US facilities are located and details of its organizational structure, a party may be deemed to have control if it has the legal right, authority and/or practical ability to obtain the materials.

Through the Hague Evidence Convention

US litigants may seek discovery from foreign entities through the Convention on the Taking of Evidence Abroad in Civil or Commercial Matters ("Hague Evidence Convention"). This multilateral treaty (to which more than 50 countries, including the United States, are signatories) streamlines procedures for seeking evidence abroad by allowing US courts to request evidence directly from designated authorities within foreign states.

The extent to which parties to a US litigation are able to rely on the Hague Evidence Convention depends on the local discovery rules of the country in which discovery is sought. It is not unusual for contracting countries to limit the types of information that can be requested pursuant to the

Convention, and thus, if possible, it is advisable for parties to pursue discovery through the Hague Evidence Convention in conjunction with other avenues of obtaining foreign evidence.

Through Letters Rogatory

In addition to the Hague Evidence Convention, letters rogatory provide a mechanism through which US parties may seek to compel the production of overseas evidence in US-based litigation. A letter rogatory is essentially a formal request from one court, in which an action is pending, to a foreign court, asking for assistance in performing a judicial act.

If a non-US jurisdiction isn't a signatory of the Hague Evidence Convention or some other treaty regarding judicial assistance, letters rogatory may be the only means by which a party can compel evidence from a foreign non-party, unless the foreign non-party is subject to the personal jurisdiction of the US court ordering discovery.

Unfortunately, obtaining documents by letters rogatory is costly, and it can take longer for parties to procure evidence through this method than via the Hague Evidence Convention.

Personal Jurisdiction

Finally, US courts will compel the production of documents located abroad when the custodian of the documents is subject to the court's personal jurisdiction. Indeed, even a non-party foreign corporation may be compelled to produce evidence pursuant to a US court subpoena if that entity, or in some cases its corporate parent, is subject to the court's personal jurisdiction.

An Impediment: Blocking Statutes

Several European countries—most prominently, France—have enacted blocking statues intended to protect their sovereignty and prevent disclosure of their citizens' personal data during US pretrial discovery. Generally, US courts regard blocking statutes with the trademark skepticism reserved for foreign legislation seeking to limit the United States' power to bind the parties before them, and American courts often require production of relevant data regardless of a blocking statute.

It is important to note, however, that companies in violation of foreign blocking statutes may face serious consequences in those jurisdictions. The French blocking statute, for example, criminalizes the act of obtaining discovery from France for use in litigation or investigations outside of the country, unless the discovery is sought through the Hague Evidence Convention.

Obtaining Evidence Through 28 U.S.C. § 1782

28 U.S.C. § 1782 permits US district courts to order discovery in the United States for use in foreign proceedings. The potential scope of discovery under § 1782 is far-reaching: In order to avail itself of § 1782, the party seeking discovery must simply demonstrate that: (1) the request has been made either by "a foreign or international tribunal" or "any interested person"; (2) the request seeks evidence, whether an individual's "testimony or statement" or the production of "a document or other thing"; (3) the evidence is "for use in a proceeding in a foreign or international tribunal"; and (4) the person from whom discovery is sought resides or is found in the district of the United States District Court ruling on the application for assistance.

Though these requirements have been interpreted broadly by US courts across many different types of litigation, the law is not settled on whether § 1782 can reach documents within a US entity's "possession, custody, or control" if those documents are physically located overseas.

Judicial Discretion Applying 28 U.S.C. § 1782

Once each of these statutory requirements has been met, the court ordering discovery has discretion to determine how broad the discovery order will be. US courts tend to weigh multiple factors, including (1) whether the person from whom discovery is sought is a participant in the foreign proceeding, (2) how receptive the foreign government has been to US federal-court judicial assistance, (3) whether the discovery request conceals an attempt to circumvent otherwise applicable discovery restrictions and (4) whether the request is unduly intrusive or burdensome.

Tips for Parties Facing Cross-Border Litigation

Obtaining evidence from abroad through the Hague Evidence Convention or letters rogatory can be a time-consuming, labyrinthine and expensive process. Early on in the discovery process, US counsel facing cross-border discovery should make the court and opposing counsel aware of the potential legal barriers and costs associated with collecting foreign data.

Multinational corporations should be aware of the types and location of electronically stored information ("ESI") under their control, and develop cross-border discovery strategy (and discovery defense strategy) accordingly. For example, if a company's ESI is located in several European Union member states, each subject to the same data privacy framework, it may make sense to transfer the relevant data to one central location within the EU for storage and document review.

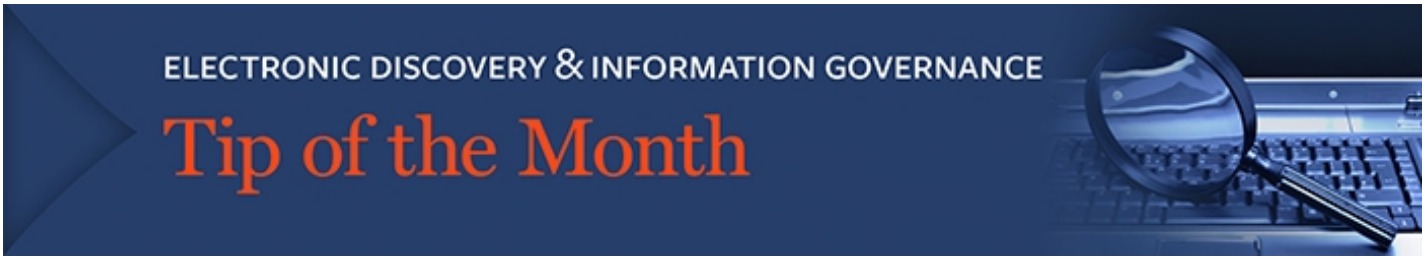
Companies collecting foreign data relevant to a US litigation should consider conducting document review in the jurisdiction where the data is located or a jurisdiction to which it can be transferred without implicating local data protection laws. An on-site review, coupled with targeted collection procedures and narrowly defined requests for production, may significantly reduce the volume of data

that has to be transferred to the United States and lighten the burden of complying with data privacy restrictions.

Because US discovery laws require broader disclosure in the pretrial phase than corresponding discovery laws abroad, companies would be well advised to work with local counsel to avoid falling foul of a foreign jurisdiction's data privacy regulations and blocking statutes.

International corporations should be aware that US discovery rules may directly conflict with foreign blocking statutes and data privacy regulations. Although US courts have shown greater deference to restrictions arising from data privacy laws than those arising from foreign blocking statues, companies must keep in mind the possibility that the failure to comply with US discovery obligations out of concern for foreign laws could lead to US courts imposing considerable sanctions.

For inquiries related to this Tip of the Month, please contact the author Alessandra Crawford.



Special Masters and Complex E-discovery Questions

31 July 2018

Scenario

A multinational corporation is served with an antitrust class action alleging that the corporation cooperated with other players in its industry to set prices. It soon becomes apparent that the plaintiffs' counsel has also sued all of the other players, each in the US judicial district where a major place of business is located. The cases are eventually consolidated in a single US district court that does not have robust local rules governing e-discovery. A major competitor's counsel proposes that the parties seek the appointment of a special master to handle e-discovery because the counsel fears that otherwise the plaintiffs will be essentially free to set the scope and depth of e-discovery more or less unilaterally. The general counsel requests an assessment of this suggestion.

Special Masters and Complex E-discovery Questions

In 2016, over a dozen food producers faced this dilemma when they were served with an antitrust lawsuit alleging multi-year collusion over pricing. Perhaps predictably, given the complex allegations and litany of defendants, discovery got messy quickly. Denying the defendants' motion to dismiss, the judge explained that "[t]his is not a simple case of obvious injury with obvious defendants. Rather, many dots need to be connected in context to draw a picture of conspiracy."

After a year of wrangling between the parties over discovery protocols, the judge appointed a law professor and e-discovery expert as special master to oversee technology-assisted document review. She issued a comprehensive search methodology framework to guide electronic discovery, defining both the substantive scope of discovery and an elaborate multi-state procedure to encourage "cooperation" between the parties.

But for now, the jury is out on whether court-appointed special masters such as this one help or hinder e-discovery. Certainly the trend has been toward appointing special masters. A series of changes to the Federal Rules of Civil Procedure between 2003 and 2006 have greatly facilitated their appointment. Evaluating these changes, one judge with the Southern District of New York wrote that she "firmly believe[s] that court adjuncts in this field are both necessary and desirable."

Reflecting specifically on the special master's work in the complex antitrust case involving the food producers, some have hailed it as a "terrific protocol" that "will certainly be referenced for a long time." Even so, as one mediation expert has explained, "[j]udicial officers, lawyers and clients are becoming more comfortable with e-discovery and how it's used in litigation," so these special masters may increasingly play a less meaty role in ironing out e-discovery wrinkles. If judicial officers and the parties

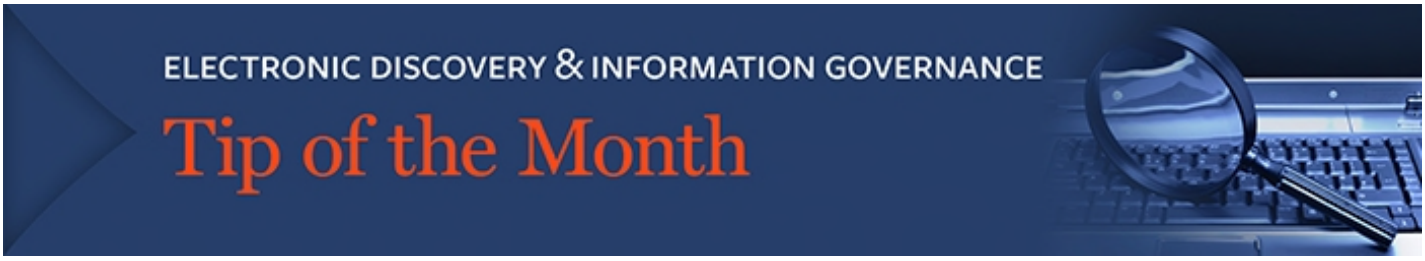
themselves have sufficient capacity to conduct e-discovery, a special master may just add another layer of complexity and rigidity to an already contentious phase of litigation—complexity that comes at the expense of judicial discretion and authority. Some commentators also have voiced concern that the position adds gratuitous costs to litigation, costs that come at the expense of parties themselves and accrue to the benefit of a small handful of qualified repeat players. As magistrate judges hone their e-discovery expertise, they offer a compelling alternative—bringing greater impartiality, a broader scope of knowledge and a stronger working relationship with the district judge without compromising significantly on specific expertise in e-discovery protocols.

So should you move to appoint a special master in your matter?

Certainly special masters can offer greater sophistication, coordination and organization throughout the discovery phase of litigation—a particular boon in high-stakes, unwieldy cases like the ongoing food industry antitrust matter. Yet they bring increased costs, greater rigidity and potentially undesirable delegations of judicial authority. In deciding whether to move for a special master appointment, consider factors such as the number of parties and volume of documents at issue, relative comfort level of parties' counsel and judicial officers with e-discovery, your litigation budget, and the speed at which discovery must proceed to achieve your goals.

In short, special masters can be a powerful tool in a litigator's case management arsenal– but they may not be appropriate for *all* disputes.

For inquiries related to this Tip of the Month, please contact the authors Eric B. Evans, Ethan A. Hastert or Kim A. Leffert.



Defensible Disposition of Data: Guidance from the Sedona Conference Scenario

30 August 2018

Scenario

In response to defending periodic litigation in the early 2000s, a company implemented an information governance policy that emphasized the retention of nearly all electronic data and documents. At the time, the volume of data was not excessive, and the cost of retention was comparatively minimal. Over time, however, the company and the volume of data has grown. Storage costs have ballooned, and the company leaders have decided to reconsider their "packrat" strategy. In-house counsel has warned, however, that routinely deleting data may mean that something relevant to litigation will be lost, and the company may have to defend its practices against a spoliation claim. The company therefore wants to ensure that any new policy is defensible.

The Risks and Costs of Retaining All Electronic Data

Spoliation—the destruction, alteration or mutilation of evidence—is a common fear in litigation, particularly for large corporate defendants. In the past, conventional wisdom held that storage was cheap, and so it was prudent to save everything rather than risk deleting something that might later prove relevant in a lawsuit. However, as the volume of electronic data has exploded, many organizations have realized that developing and implementing a reasonable and defensible records retention program that provides for the regular deletion or expiration of electronic data is often cheaper and less risky than holding on to every scrap of electronic data.

- First, in reality, no organization actually saves *everything*. When data is lost in violation of a policy or practice that says everything must be preserved, it can be more difficult to defend against a spoliation claim.
- Second, storage costs are often not cheap. Storage hardware might not be particularly expensive on its own, but all of the associated information technology infrastructure can be extremely costly.
- Third, discovery costs can account for 75 percent or more of litigation expenses, and those costs can skyrocket as data volumes increase.
- Fourth, the percentage of an organization's data that is needed for business, legal or regulatory purposes is often relatively small in comparison to the total amount of data being retained. As the volume of data retained increases, so can the difficulty of finding what's truly important.

That can impact not only litigation expenses but also the ability of the business to function efficiently.

Developing a Defensible Disposition Policy

The 2015 amendments to the Federal Rules of Civil Procedure substantially revised the rules in federal court relating to spoliation of electronically stored information ("ESI"). Most significantly, the revised Rule 37(e) allows courts to impose sanctions for the failure to preserve ESI only if the party "failed to take reasonable steps" to preserve the information. (Fed. R. Civ. P. 37(e).)

Developing and implementing a reasonable policy for handling ESI—including deleting it when appropriate—can help defend against a spoliation claim. Courts have yet to develop clear standards for what constitutes "reasonable steps" or what a reasonable policy might look like. However, the Sedona Conference—a leading e-discovery research and analysis group—recently issued draft *Principles and Commentary on Defensible Disposition* to help organizations devise appropriate data disposition policies.

The Sedona Conference proposed three guiding principles that organizations can use to develop their policies:

1. Absent a legal retention or preservation obligation, organizations may dispose of their information;

2. When designing and implementing an information disposition program, organizations should identify and manage the risks of over-retention; and

3. Disposition should be based on information governance policies that reflect and harmonize with an organization's information, technological capabilities and objectives.

The first principle reflects the basic—and often forgotten—fact that there is no underlying legal requirement to preserve all data. Preservation obligations arise when litigation or an investigation is pending or reasonably anticipated or as required by statute or regulation. Absent one of those circumstances, organizations are free to let their business needs guide their document retention and destruction practices. While routine disposition practices often must be suspended in the face of internal or governmental investigations or litigation, those practices need not be focused in the first instance on the fear of a spoliation claim.

The second principle recognizes that there are risks to over-retention. Not only are organizations not required to preserve everything, but doing so may be affirmatively detrimental both to the operations of the business and to the successful and efficient conduct of litigation. Organizations should consider the risks of over-retention when developing their disposition policies.

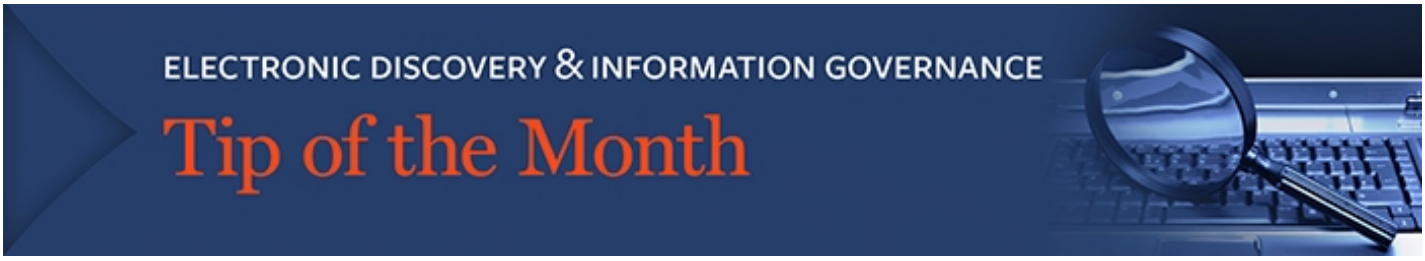
The third principle acknowledges that appropriate disposition policies will vary between organizations. Policies must take account of the types of data at issue, the subject matter of the data (including regulatory requirements), the technical capacities of the organization and the organization's own goals in retaining data. This requires organizations to undertake an internal assessment of what information they have, what they are capable of doing with it and, most importantly, why it might be valuable to keep that information. This will often be an ongoing process. As organizations evolve, the types of data they hold, their technical capabilities and their goals change. An organization's disposition policy should, therefore, be periodically reviewed to make sure that it is keeping up with the realities of the organization.

Benefits of Having a Defensible Disposition Policy

Organizations that take the time to develop and implement a disposition policy focused primarily on the realities of their business, while taking account of any applicable legal and regulatory requirements, are more likely to be successful in defending a claim of spoliation. Furthermore, discovery costs can be significantly reduced because of the decreased volume of materials that need to be collected, searched and reviewed.

Perhaps more importantly, significant business advantages may be gained: Not only will the organization spend less money retaining data unnecessarily, but the data that it does retain is more likely to be useful to the business and easier to find when needed.

For inquiries related to this Tip of the Month, please contact the authors, Kim A. Leffert or Corwin J. Carr.



The California Consumer Privacy Act: Possible E-Discovery Implications

1 October 2018

Scenario

You're the director of E-discovery Services at a major social networking company. The company's headquarters and main development facilities are in Santa Clara County, California, but its servers and operations are spread over the entire world. Many of the company's developers and customers are European Union residents. The company recently revised its e-discovery processes to account for the EU General Data Protection Regulation ("GDPR").

The general counsel walks into your cubicle and drops an article on your desk. It's titled "California Enacts GDPR-Like Consumer Privacy Protections: What You Need to Know." She then asks you, "We just finished the GDPR e-discovery update. Now do we need to do something about this?"

California's New Privacy Law

On June 28, 2018, California Governor Jerry Brown signed Assembly Bill 375, the California Consumer Privacy Act of 2018 ("CCPA" or "the Act"). Barring further amendment, the CCPA will go into effect January 1, 2020. The CCPA will give California residents control over how companies collect, store, use and disclose their personal information. The CCPA covers for-profit companies doing business in the state of California that:

1. Have annual gross revenues of more than $25 million (as adjusted);
2. Buy, receive, sell or share for commercial purposes the personal information of 50,000 or more consumers each year; or
3. Derive 50 percent or more of revenue from selling consumers' personal information.

Unlike earlier state and federal privacy laws, which tend to focus on a specific sector or type of personal information, the CCPA arguably applies to all businesses that meet these requirements. The CCPA, however, includes explicit exceptions to ensure that it doesn't come into conflict with pre-existing privacy laws such as the Gramm-Leach-Bliley Act and the Health Insurance Portability and Accountability Act (HIPAA).

GDPR Compliance Does Not Translate into CCPA Compliance

While the CCPA and GDPR both focus on consumer rights, companies should not assume that being GDPR-compliant means that they're already CCPA-compliant. Although companies with a GDPR

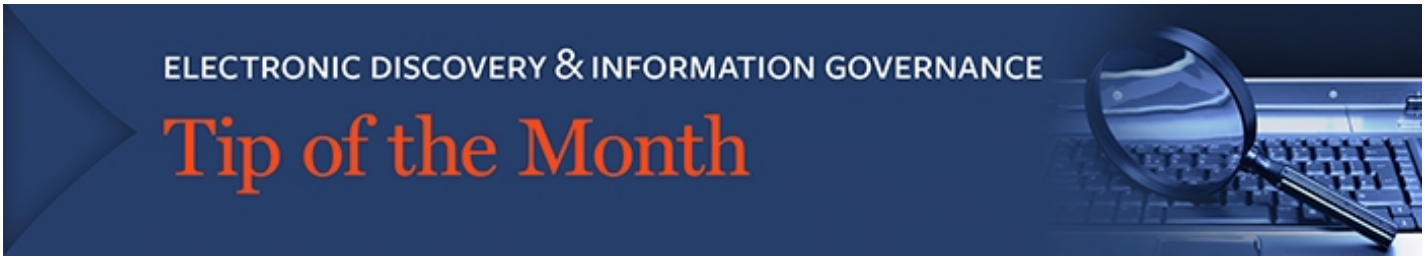
compliance program have a head start on CCPA compliance, these businesses subject to the law should ensure that they have the operational, technical and contractual ability to comply with the CCPA for any personal information they collect about California residents.

Several CCPA Provisions Raise Issues for E-Discovery Professionals:

The CCPA's broad definition of "personal information" implicates information routinely disclosed in discovery. The CCPA defines personal information as “information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.” Personal information specifically includes unique identifiers, biometrics, geolocation data, browsing and search information, “inferences drawn” from personal information to create a profile about a consumer and “[p]rofessional or employment-related information.” Companies cannot avoid disclosure of employee "personal information"—especially “professional and employment-related information” to service providers and litigation adversaries in discovery. It may be advisable to add terms to vendor agreements and protective orders specifying the recipients' obligations to comply with the CCPA.

The CCPA gives consumers the right to demand that companies delete their personal information. The CCPA requires companies to delete personal information “collected from the consumer” on demand. There are certain exceptions to this, including data collected to protect against fraud or other illegal activity, enable internal uses that are reasonably aligned with consumer expectation, complete a business transaction with the consumer and "comply with a legal obligation." (Sec. 1798.105(d)(8).) Retention obligations and litigation holds would likely qualify as "legal obligations," but companies that make operational changes to how they store and process personal information will need to ensure that these changes don't lead them to delete personal information that's subject to litigation holds.

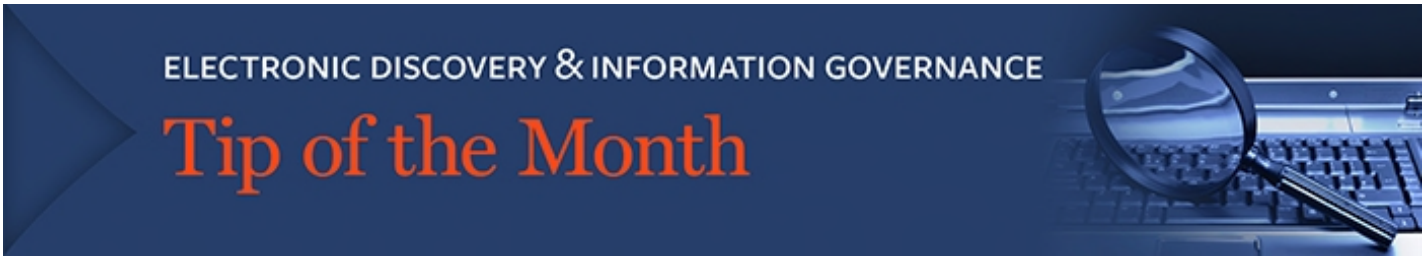
The CCPA gives consumers a private right of action for "disclosure" of personal identity information. Under the CCPA, California consumers get a private right of action for "disclosure" of names—in combination with any of the following: (i) Social Security numbers; (ii) driver’s license and state ID numbers; (iii) financial account numbers, passwords, and access codes; (iv) medical information; or (v) health insurance information—"as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices." (Sec. 1798.150(a)(1).) The plain language of this section could cover, for example, inadvertent public filing of consumers' names and account numbers in litigation. While many argued that this surprisingly common kind of error already violated California privacy law, the existence of a private right of action, with meaningful statutory damages, gives plaintiffs' attorneys an incentive to pounce on any publicized inadvertent disclosure.



The CCPA May Still Be Further Amended

The precise details of the CCPA may yet change. The CCPA was passed quickly to keep a more stringent initiative on privacy from appearing on the ballot in November. As a result, the CCPA has gaps and provisions likely to cause unintended consequences. Amendments have already begun. Governor Brown signed a first round of amendments, embodied in Senate Bill 1121, on September 23, 2018. But given the stakes for major technology players, it's reasonable to expect further attempts at amendment. Once the CCPA goes into effect, there are also likely to be legal challenges.

For inquiries related to this Tip of the Month, please contact the authors, Eric B. Evans or Kendall C. Burman.



US Companies with "Sufficient Connection" to UK Must Produce Documents to UK's Serious Fraud Office

29 November 2018

Scenario

A US company has a subsidiary based in the United Kingdom. It recently learned that its subsidiary is under investigation by the UK's Serious Fraud Office (SFO). The US company has received a notice to produce documents related to that investigation. The general counsel of the US company wants to know if it can challenge the request for documents on the grounds that the parent company's documents are located in the US and are therefore beyond the jurisdictional reach of UK authorities.

English Court: Documents Held by Foreign Company Must Be Produced If "Sufficient Connection" Between Company and UK's Jurisdiction

In September 2018, in *R (KBR Inc) v. Serious Fraud Office [2018] EWHC 2012 (Admin)*, the English High Court held that a foreign company that has a "sufficient connection" to the jurisdiction must produce documents to the SFO even when the company does not conduct business in the UK.

In that case, the US company KBR Inc. had received notice pursuant to an English statute—section 2(3) of the Criminal Justice Act of 1987 (CJA)—to produce certain documents to the SFO. The SFO sought the documents as part of its investigation into KBR's subsidiary, which was registered in the UK. KBR challenged the request for documents on numerous grounds, including arguing that the statute could not operate extraterritorially to apply to KBR's documents located outside the UK.

The court held, *inter alia*, that the relevant provision of the statute *could be* applied extraterritorially to foreign companies that held documents outside the UK in situations where there is a ***sufficient connection*** between the company and the jurisdiction. Although it did not set forth a clear test, the High Court outlined several factors that would aid in the determination of what would entail such a "sufficient connection." Importantly, the court noted that what did assist in establishing a sufficient connection to the UK were the facts that the payments central to the SFO's investigation of the UK subsidiary, as well as the underlying contracts and arrangements at issue in the investigation, were required to be approved by the parent company (KBR) and that the payments were actually paid by the parent company through its US-based treasury function.

By contrast, the court also noted that the following facts did not assist in establishing a connection to the UK:

- The mere fact that KBR was the parent company of the UK subsidiary;

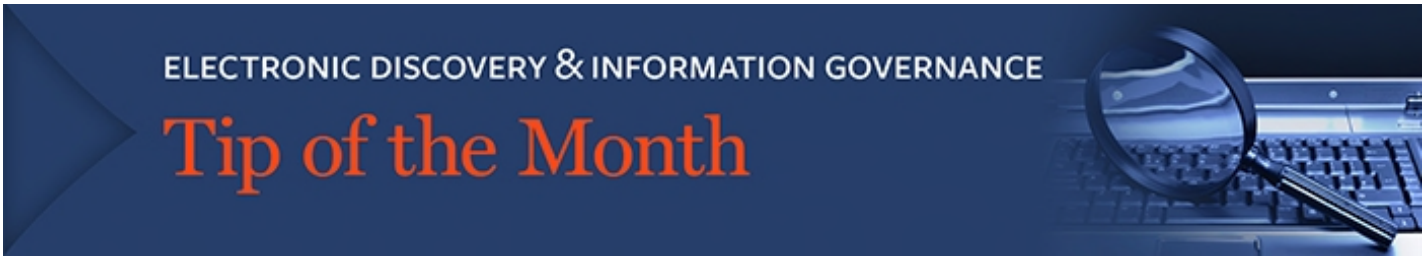
- That KBR cooperated to a degree with the SFO's request for documents and remained willing to do so voluntarily (i.e., KBR would apply SFO search terms across data held in the US); and
- That a senior representative of KBR met the SFO in the UK as part of the investigation.

Ultimately, the court ruled that—in the circumstances of this case—there was a sufficient connection and that, therefore, the US parent could not quash the request for documents on jurisdictional grounds. The court relied on the fact that the parent had to approve the payments and transactions at issue in the SFO's investigation and that the payments were made through the parent. The court also noted that a corporate officer of the US parent was actually based in the UK and appeared to carry out his functions from the UK. The court did not say whether this was itself enough to establish a "sufficient connection", but it was a factor that was given weight in its overall analysis.

Strategies and Best Practices

As noted above, whether or not a US company would be deemed to have "sufficient connections" to compel the production of documents to the SFO in the UK is a highly factual question. The key principle appears to be that the parent company must have performed certain actions that are central to the investigation (e.g., approving the core payments or transactions at issue in an investigation by the SFO). However, the question of whether affirmative actions (rather than mere omissions) are required by the parent for such a connection to exist and to what degree such actions relate to issues that are central to an SFO investigation will inevitably be questions of fact that any company will have to evaluate carefully before taking any steps in response to receiving a notice to produce documents under section 2(3) of the CJA.

For inquiries related to this Tip of the Month, please contact the authors, Anne M. Selin or Kim A. Leffert.



Revisions to the MIDP in the Northern District of Illinois

27 December 2018

Scenario

A manufacturing company was recently served with a complaint filed in the United States District Court for the Northern District of Illinois. The company litigated a similar case in 2017 in the Northern District under the court's Mandatory Initial Discovery Pilot Program ("MIDP"), and the company's general counsel has asked whether the same rules will apply to the recently-filed case.

The Mandatory Initial Discovery Pilot Program

In mid-2017, the District of Arizona and the Northern District of Illinois began participating in the Federal Judicial Center's MIDP. The MIDP radically changed the scope of parties' initial disclosures, and the timing of discovery more generally, and applied (with limited exceptions) to all civil cases.

Three crucial changes brought about by the MIDP at the time were:

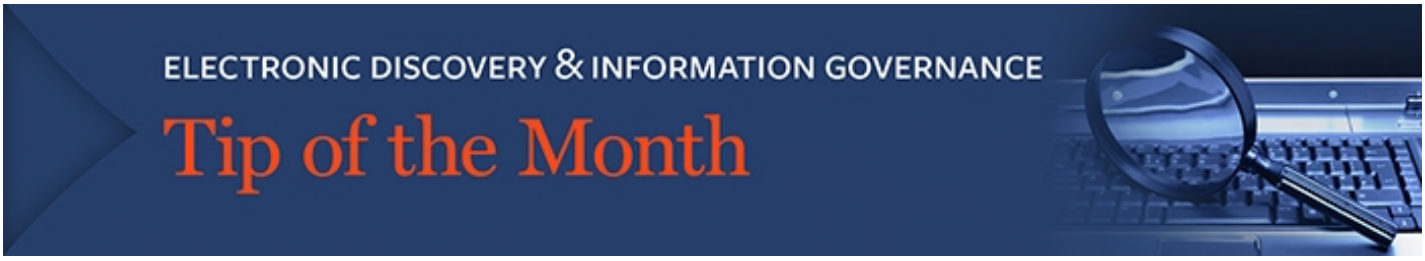
1. A motion to dismiss generally would no longer delay the time to answer the complaint;
2. With limited exceptions, 30 days after a responsive pleading is filed, the parties were to serve an expanded set of initial disclosures; and
3. Absent a court order, ESI was generally to be produced within 40 days of serving a party's initial disclosures, and parties were to meet and confer regarding the disclosure and production of ESI, including with respect to each party's preservation obligations, custodians, search terms, the use of technology-assisted review and the form in which ESI will be produced.

Updates to the MIDP in the Northern District of Illinois

As a pilot project, the Northern District of Illinois has evaluated both the litigants' and the court's reactions to the MIDP for the past year and a half. Effective December 1, 2018, the Northern District of Illinois amended its implementation of the MIDP on the basis of comments from the legal community. The Northern District's amended Standing Order now provides that filing a motion to dismiss does delay the time to answer the complaint, restoring the traditional time periods set forth in Federal Rule of Civil Procedure 12(a).

Under the amended Standing Order, filing a motion to dismiss will also delay the time to produce the MIDP's expanded set of initial disclosures.

The court does, of course, retain discretion to depart from the amendment and order that answers be filed or that initial disclosures be exchanged earlier.



Impact

The revision to the MIDP is a welcome change for defense counsel and their clients. Defendants facing even frivolous claims that could easily be dismissed were nevertheless forced to incur sometimes extensive costs to provide mandatory initial disclosures and produce documents. Now, while a motion to dismiss is pending, discovery will generally not commence, and litigation costs can be reduced significantly as meritless cases are weeded out.

For inquiries related to this Tip of the Month, please contact the authors, Kim A. Leffert or Corwin J. Carr.