Warner Norcross + Judd

FALL 2019

DISCOVERY CENTER

A DATA ANALYTICS + eDISCOVERY NEWSLETTER

Preparing for the California Consumer Privacy Act

By Norbert F. Kugele and Kelly R. Hollingsworth

The California Consumer Privacy Act (CCPA) becomes effective on January 1, 2020. While the governor of California has recently signed into law amendments to the CCPA, the law remains fundamentally unchanged, except now there is a one-year carve out for employment data and business-to-business contact information. Companies should take steps now to ready themselves for the CCPA before the January 1 deadline.

TABLE OF CONTENTS

Who Must Comply With the CCPA?

The new law casts a wide net. It applies to any for-profit business (including entities that control or are controlled by the business and share common branding with the business) that:

1. Collects information about California consumers or households (defined as "personal information");
2. Determines the purposes for processing the personal information, alone or jointly with others;
3. Does business in California or with any California resident; and
4. Meets any one of the following requirements:
   a. has annual gross revenues in excess of $25 million;
   b. alone or in combination, annually buys, sells, receives or shares personal information of 50,000 or more California consumers (or 50,000 or more devices or households); or
   c. derives 50% or more of its revenue from selling California consumers' personal information.

A business that is not directly subject to the CCPA may still have compliance obligations if it handles personal information about California residents or households on behalf of another business. This is because the term "sale" is broadly defined under the CCPA to include any sharing of data with another business or third party for monetary or other valuable consideration.

If a business subject to CCPA uses a third party to handle any personal information about California residents or households, the business must obtain certain contractual promises from the third party so that the third party's handling of the data will not be deemed a sale for CCPA purposes. Specifically, the contract with the third party must prohibit sale of the information or use in any manner other than to provide the agreed upon services to the business and must also include a certification that the third party understands and will comply with those restrictions.

What Are a Business's Obligations Under the CCPA?

The CCPA gives California residents certain rights with respect to their data. These rights will vary, depending on whether a business merely collects and processes information about California residents and households or if it also "sells" the information.

Any business that is subject to the CCPA must disclose to California residents at or before the point of collection the categories of personal information that it has collected over the last 12 months, the purposes for which it uses the personal information and with whom it shares the personal information. If the business also sells (or is deemed to be selling) personal information, then it must also disclose the fact that the information may be sold and include a "Do Not Sell My Personal Information" button on the homepage of its website and in its privacy policy.

All businesses subject to CCPA must have a website privacy policy that includes an explanation for California residents of their rights under the CCPA, which are:

The right to request disclosures of data collected about the California resident (also known as the "right to know").

The right to access the personal information that the business has collected about the California resident.

The right to seek deletion of data that the business has collected, with certain exceptions (also known as the "right to be forgotten").

The right to opt out of any sale of information—to the extent that the business sells (or is deemed to be selling) personal information.

The right not to be discriminated against with respect to the available goods and services or costs of goods and services if the California resident exercises any rights under the CCPA (also known as the "right to equal services").

Rather than including the above information (such as a "Do Not Sell My Information" button) on the business's general website and privacy policy, a business may comply with its disclosure obligations by redirecting California residents to a California-specific home webpage and a California-specific privacy policy.

If a California resident seeks to exercise any of his or her rights, the business must generally respond free of charge within 45 days – which includes any time needed to verify that the request is legitimate. The 45-day deadline can be extended an additional 45 days, provided the business provides notice to the individual within the original 45-day time period.

How to Prepare for the CCPA

A business subject to the CCPA should take the following steps to become compliant:

Map Your Data 1

Understanding the personal information your organization collects, retains and shares is a critical first step in assuring CCPA readiness. You should be able to answer the following questions:

What personal information does your organization collect from California consumers?

How does it collect this information and from what sources?

Where and how is the information stored?

With whom is the information shared?

Why is the information shared (e.g., provision of services, a "sale")?

Because employee data and business-to-business contact information is carved out for 2020, you can prioritize your compliance efforts by first focusing on consumer data.

Review Your Current Security Controls 2

The CCPA allows individuals to file a lawsuit and obtain statutory damages if certain personal information is breached due to a business's failure to utilize reasonable security

practices and procedures. Now is the time to review and update your data security and privacy policies and practices to help mitigate the risk of a data breach and subsequent litigation.

3 Develop a Process for Handling Requests to Exercise Individual Rights

Given the short, 45-day response window, you should develop procedures for responding to individual requests and establishing rules for when to deny such requests. Your process should also include appropriate methods to verify that the request comes from the data subject or from an authorized representative of the data subject, taking into account the nature of the information involved in the request. Although the CCPA does not allow you to require that an individual set up an account on your website to exercise his or her individual rights, recent amendments to the CCPA allow you to require that any individual who has set up an account must submit his or her request through that account. Furthermore, you should ensure your process allows for requests to be honored. For example, if an individual opts out of the sale of information, you must be able to implement that request throughout your business and with those vendors and affiliates with whom you have shared that information.

4 If You Sell Personal Information About Children Under Age 16, Develop an Opt-In Process

While adults can opt out of the sale of their information, the CCPA requires an opt-in process for children under age 16. Children who are at least 13 years of age can opt in for themselves, but parents must opt in for children under age 13.

5 Update Your Vendor Agreements

To avoid having data transfers classified as a "sale" of information, businesses need to ensure their agreements with third parties, and even affiliated entities, meet certain CCPA requirements. You will likely need to update your current agreements (or create new agreements if they are not already in place) with any organization that handles personal information about California residents on your behalf. If you do not update these agreements before January 1, 2020, you may be deemed to be selling information, which implicates opt-out obligations (and opt-in obligations for children under age 16) and requires the use of the "Do Not Sell My Information" button.

6 Ready Your Website

You should determine ahead of time whether to develop a California-specific landing page or integrate CCPA requirements into your general website. Furthermore, you will need to update (or develop) your website privacy policy so that it clearly details all of the following:

The types of personal information you collect;

How you collect the information;

With whom you share the information;

Whether or not you sell personal information (and, if so, how individuals can opt out of the sale); and

How individuals can exercise their rights under the CCPA, including two or more designated methods for consumers to submit requests (at a minimum, a toll-free telephone number and a website address).

In addition, if you sell (or are deemed to be selling) personal information, you will need a clear, conspicuous link on your homepage (or on the homepage for California consumers), titled "Do Not Sell My Personal Information." This link must take consumers to a page where they can opt out of the sale and where children under the age of 16 and parents of children under the age of 13 can opt into the sale.

7 Train Your Employees

Finally, begin training your employees on the key aspects of the CCPA, how to respond to individual requests, and the importance of following the organization's data privacy and security policies and procedures.

The CCPA is a data privacy game-changer within the U.S. and it imposes significant obligations on a large swath of businesses. While the obligations and individual rights under the CCPA are similar to obligations and individual rights granted under the European Union's General Data Protection Regulation (GDPR), the two laws are not identical and compliance with the GDPR does not mean you are automatically compliant with the CCPA. Thus, your business will still need to develop policies, disclosures and contractual provisions that are specific to the CCPA.

Non-compliance with the CCPA will be costly.

The California Attorney General is authorized to enforce the CCPA with penalties of up to $2,500 per consumer violation. Additionally, consumers whose data is the subject of a data breach can sue for between $100 and $750 per incident if the business failed to implement reasonable security procedures. The CCPA expressly voids any arbitration provision or class action limitation on this right. If your business meets the statutory thresholds noted above, compliance efforts should be started well in advance of January 1, 2020.

By Nathan W. Steed

Recent Data Privacy & Security Enforcement Actions: Lessons Learned

The Department of Health and Human Services (HHS) Office for Civil Rights (OCR) continues to pay close attention to those companies in the health care industry and how they use patient information, specifically in the context of the Health Insurance Portability and Accountability Act (HIPAA). OCR has announced its first ever enforcement action and settlement agreement related to its Right of Access Initiative. The Initiative was announced earlier in 2019 and is focused on enforcing individuals' rights to receive copies of their medical records (or their minor children's records) in a timely and cost-friendly manner.

The settlement arose out of an OCR investigation into a hospital after a woman complained that the hospital did not provide access to records about her unborn child. As a result of the investigation, the hospital provided the woman with the records more than nine months after her request. Under the settlement, the hospital paid OCR $85,000 and is required to develop information access policies and procedures, provide employee training on the policies and to be monitored by OCR for one year. This recent settlement reflects just how seriously OCR is taking its Right of Access Initiative. Healthcare providers should become familiar with and comply with HIPAA's right of access rules. These require providers to provide access to personal health information within 30 days of the request and to make sure fees for record copies are reasonable and cost-based.

OCR also recently announced its settlement with Medical Informatics Engineering, Inc. (MIE), an Indiana company that provides medical record services to health care providers. In 2015, MIE notified OCR that hackers accessed personal health information of over 3.5 million people. OCR then investigated and discovered MIE

had never conducted a comprehensive risk analysis to determine risks and vulnerabilities with respect to the company's personal health information. As part of the settlement, MIE paid OCR $100,000 and must implement a corrective action plan to help MIE comply with HIPAA rules.

It is imperative for companies entrusted with personal health information to conduct risk assessments. HIPAA rules specifically require companies to "conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic protected health information" held by the company. Failure to do so can lead to enforcement actions and leaves businesses open to data breaches.

In May, OCR announced that Touchstone Medical Imaging (Touchstone), a company providing diagnostic medical imaging services, agreed to pay $3,000,000 and adopt a corrective action plan to settle potential HIPAA violations.

In 2014, both the FBI and OCR notified Touchstone of a data breach allowing uncontrolled access to Touchstone patients' personal health information. While Touchstone initially denied any health information was exposed in the breach, OCR later discovered health information of over 300,000 people was exposed and available online. OCR's investigation revealed a number of other issues including Touchstone's failure to seriously investigate the breach until months after notice from both the FBI and OCR, failure to notify individuals affected by the breach in a timely manner, failure to conduct a comprehensive risk assessment and a lack of HIPAA required agreements between Touchstone and their third-party vendors.

The Touchstone incident reflects how a complete lack of preparation in the data privacy and security context can lead to disaster. As the OCR Director has stated, a failure to identify personal health information risks and vulnerabilities "opens the door to breaches and violates HIPAA." When a data breach occurs, businesses must take them seriously to not only minimize the risk of the affected individuals, but also to minimize risk for themselves. Failure to do so, as Touchstone has learned, can be quite costly.

Enforcement actions are not limited to health information. The Federal Trade Commission (FTC) enforces data privacy and security rules through its role to protect consumers and prevent unfair trade practices.

The FTC recently settled charges against an automotive dealer software provider, LightYear Dealer Technologies (LightYear). LightYear's software collected large amounts of personal information (such as names, addresses, social security numbers, credit card numbers and

bank account information) about dealership customers and employees. The FTC alleged LightYear stored this information "in clear text, without any access controls or authentication protections, such as passwords." LightYear also used a backup storage device without any steps taken to ensure it was set up safely and securely. The failure to implement even basic security measures, the FTC alleged, led to a breach exposing the personal information of approximately 12.5 million people.

Under the settlement, unless LightYear develops and implements a comprehensive program to protect personal information, they are prohibited from sharing, collecting or maintaining personal information. Additionally, the settlement requires LightYear to have a third party assess its security programs every two years and for a LightYear senior corporate manager to certify every year they are complying with the FTC's order. When collecting, storing or sharing sensitive personal information, it is imperative to take reasonable steps to secure and protect that data.

Businesses should make sure they understand the type of data they collect, store or share; how it is used; and the risks and vulnerabilities to that data. Doing so enables businesses to develop, maintain and revise policies to best protect consumers' data. The failure to do so can lead to devastating data breaches and costly regulatory investigations and actions.

The FTC has also announced a proposed record-breaking settlement where Google, and its subsidiary YouTube, agreed to pay $170 million to settle allegations that they violated the Children's Online Privacy Protection Act (COPPA) by collecting children's personal data without parental consent. The FTC alleged YouTube used technology on its child-directed channels to track users on the internet (i.e., cookies) to deliver targeted ads without notification of such practices and subsequently obtaining parental consent.

Child-directed websites and online services should familiarize themselves with COPPA requirements.

Further, third parties, such as advertisers, need to know where their data is coming from – as those with knowledge that the information they collect is from users of child-directed platforms are also subject to COPPA rules.

Before child-directed platforms collect personal information from children under the age of 13, they must provide notice of the business's personal information policies and practices and to obtain parental consent.

This summer the FTC announced its proposed settlement with Unrollme Inc., a company that helps users manage their emails. The FTC alleged that despite assuring its users they would not access or use their personal emails (instead only clearing out user inboxes, unsubscribing them from unwanted email subscriptions, etc.), Unrollme accessed personal emails containing electronic receipts and shared them with its parent company who then used and sold the information in its market research products. The settlement requires Unrollme to notify certain users of their information collection and sharing policies, bars Unrollme from misrepresenting their data policies and requires both Unrollme and its parent company to delete the information collected from the electronic receipts unless they obtain express consent from the Unrollme users to keep the data.

Businesses must be honest about their data collection and use policies. To do so, businesses should comprehensively understand their policies and communicate them to customers in a clear, conspicuous way.

Warner Associate Alexandra Woods contributed to this article.

Getting Redactions Right Matters Now More Than Ever

By B. Jay Yelton III

Lawyers routinely handle thousands of records, both hard copy and electronic, that contain privileged or otherwise confidential information. And, while lawyers have always had an obligation to protect client confidences, the heightened global concern over data privacy and proliferation of legal regulations to safeguard private personal information has minimized the margin for error when handling client records—especially when those records need to be shared in response to discovery requests or government investigative demands.

Yet, despite the ethical and legal obligations to protect privileged and confidential data, mistakes in handling privileged and confidential information continue to make headlines.

These are just a few examples:

In January 2019, Paul Manafort's lawyers filed an improperly redacted response to Special Counsel Robert Mueller's determination that Manafort had breached his plea agreement. The improperly redacted PDF file revealed Manafort's contacts with Konstantin Kilimnik, a Ukrainian the FBI believes to be a Russian intelligence agent.

In November 2018, Facebook's lawyers submitted an improperly redacted document in its litigation with Six4Three, an app for finding bikini photos. The improperly redacted PDF file revealed that Facebook had considered charging the company for access to its user data.

In August 2018, the United States Postal Service, in response to a Freedom of Information request, produced an unredacted copy of the entire civilian personnel file of Congresswoman Abigail Spanberger, a former CIA officer, who at the time was a Congressional candidate. The file contained her SF-86 security clearance application with her social security number and answers to highly personal background questions over such matters as drug and alcohol use and health information.

A lawyer's failure to properly redact information can result in the disclosure of a client's privileged or highly personal and potentially embarrassing information. Serious repercussions can result: waiver of attorney-client privilege, a malpractice lawsuit and possible professional disciplinary action that can lead to suspension or disbarment.

Given these high stakes, what should lawyers do to get redactions right?

Everything they can, of course.

First, recognize that confidential information, privileged or otherwise, is likely to be found in any collection of documents received from a client. So, there needs to be a process in place for identifying confidential information, properly redacting it (or, in some cases and especially with privileged information, withholding it) and conducting a quality control check before production to an opposing party or government agency.

Second, build available technology into the process. Standard eDiscovery software can assist with the identification and redaction of confidential information. Keyword searches can be used to identify potentially privileged information as well as other types of confidential information. For example, searches can be set up to look for firm names, firm email domains, individual attorney names, and other words or phrases that could implicate privilege or work product, such as "Work Product," "Attorney-Client Privileged," "Lawsuit," etc. As for confidential search terms, possible search terms would be "social security," "SS#," "DOB," "telephone number," etc. If the case involves protected health information, searches could be set up for doctor names, hospital names, related email domains and any known medical conditions. These terms can also be highlighted in the documents to assist human review.

With respect to certain types of personally identifying information, eDiscovery software can also be used to automatically redact that information when it is found. Social security numbers, telephone numbers and dates of birth have a standard pattern. Most eDiscovery software allows for what is in essence a sophisticated keyword search known as "regular expressions," or "regex." These searches look for patterns like ###-##-#### for social security numbers or ###-###-#### for telephone numbers. Once found, the software will automatically redact these patterns. Also, with standard forms, the software can be instructed to redact information in the same location on every form. Using these auto-redaction features saves both time and money.

Where auto redaction is not possible, eDiscovery software facilitates the redaction process by providing tools that easily allow for the drawing of redaction boxes. These redaction boxes can be customized to include text such as "Redacted," "Attorney-Client/Work Product," or "Personal Identifying Information," or whatever else might be appropriate for the case. The software also allows for one-click "full page" redactions, one-click "full document" redactions, and one-click removal of redactions — all of these features are tremendous time savers to which anyone who did redactions in the early age of eDiscovery can attest.

Finally, conduct a rigorous quality control before any documents are produced. All documents that are marked for production that contain hits for the privileged/confidential keyword searches but do not contain redactions, should be subjected to human review. eDiscovery software can be used to quickly segregate these documents for the quality control (QC) process.

A random sample of documents marked for production that do not contain hits for keyword searches should also be subjected to human review. Keyword searches can be both overinclusive and underinclusive. This QC step provides the opportunity to find where the searches have been underinclusive. Again, the eDiscovery software can be used to quickly segregate these documents and create a random sample for human review.

To complete the QC process, a random sample of documents marked for production and containing redactions should be subjected to human review. This QC step will allow the opportunity to double check how well the eDiscovery software did in the case of auto redactions and how well the human reviewers did with manual redactions. As in the previous QC step, the eDiscovery software can be used to quickly segregate these documents and create a random sample for human review.

Another step that does not depend on technology should also be taken in every case where there is a likelihood that confidential information will inadvertently be disclosed. A protective order should be entered that allows the producing party to "clawback" any documents that should have been withheld or redacted. The protective order should also provide that non-producing parties may not argue waiver based on the production of privileged information. In federal court, the parties should ask the court to enter an order under Federal Rule of Evidence 502(d). A 502(d) Order provides that the unintentional production of privileged information shall not operate as a waiver in the current proceeding or *any subsequent federal or state proceeding*. This precludes any satellite litigation over whether the production was inadvertent or not. However, the 502(d) Order does not cover the situation where a party intentionally turns over privileged information — for example, where there is a strategic advantage in doing so — and then later invokes the 502(d) Order to preclude further use of the information. Nor will the Order preclude a nonproducing party from arguing that information is not truly privileged. In state court proceedings, the parties should attempt to get an order similar to the 502(d) Order with the understanding it will not have the same binding effect outside of the current proceeding as the 502(d) Order does.

One parting thought. As much as lawyers need to embrace technology to assist them with the more mundane, tedious tasks involved in the practice of law, in the case of redaction of confidential information, it is unlikely that the human element will be obviated any time soon. There just is no substitute for human review during the quality control process. Moreover, because it is the human lawyer who has the ethical obligation to protect the client's confidential information and the human lawyer who may be subject to disciplinary or other legal action for disclosing the client's confidential information or that of another individual, the human lawyer should be reluctant, at best, to stake their reputation and livelihood solely on technology.

Article III "Standing" in Private Actions Based on Data Breach

By Kenneth J. Treece

One issue that has arisen repeatedly in cases where private individuals sue for damages based on data breach is standing. In the federal system, standing goes to the very power of the court to adjudicate a case.

Under Article III of the United States Constitution, federal courts are only empowered to hear cases over which they have "subject matter" jurisdiction. Generally, when rights arise under federal law, a federal court has subject matter jurisdiction over a case. And, under certain circumstances, a suit between citizens of different states can be heard in federal court as "diversity of citizenship" also bestows subject matter jurisdiction on the court.

These general rules have been limited by the United States Supreme Court under the "Case or Controversy" clause of Article III, which provides that the federal judicial power only extends to actual "cases or controversies." One of the jurisdictional limiting doctrines that has grown out of the Court's interpretation of the "Case or Controversy" clause is that of "standing." As the Court recently explained, "standing" under Article III requires that the plaintiff has: "(1) suffered an injury-in-fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision." *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547 (2016).

In *Spokeo* the plaintiff learned that the "people search engine," Spokeo, had collected and then disseminated information about him that was untrue. The plaintiff filed a class action suit against Spokeo for violation of the Fair Credit Reporting Act (FCRA). The FCRA requires "consumer reporting agencies" to "follow reasonable procedures to assure maximum possible accuracy of" consumer reports, and provides that "[a]ny person who willfully fails to comply with any requirement [of the Act] with respect to any [individual] is liable to that [individual] " for either "actual damages" or statutory damages, costs of the action, attorneys' fees and potentially punitive damages. The district court dismissed the complaint citing the plaintiff's lack of standing, but the Ninth Circuit reversed on appeal, finding that the plaintiff had alleged that "Spokeo violated his statutory rights, not just the statutory rights of others" and the plaintiff's "personal interests in the handling of his credit information are individualized rather than collective." Based on these findings, the Ninth Circuit concluded the plaintiff had adequately alleged injury-in-fact.

The U.S. Supreme Circuit disagreed and remanded the case for further proceedings. The Court noted that injury-in-fact "requires a plaintiff to allege an injury that is both 'concrete and particularized,'" but the Ninth Circuit's analysis only addressed "particularity," not "concreteness." The Court further explained:

> **For an injury to be "particularized," it "must affect the plaintiff in a personal and individual way."**
>
> **A "concrete" injury must be "de facto"; that is, it must actually exist. When we have used the adjective "concrete," we have meant to convey the usual meaning of the term – "real" and not "abstract."** (citations omitted)

With respect to the FCRA, the Court held that the plaintiff could not satisfy the standing requirement by alleging a "bare procedural violation." The Court gave the example of a credit reporting agency providing an erroneous zip code in a credit report. "It is difficult to imagine how the dissemination of an incorrect zip code, without more, could work any concrete harm."

The Supreme Court has not addressed the question of standing directly in a case involving a data breach. The circuit courts that have addressed the issue of standing in the data breach setting since *Spokeo* have issued conflicting opinions. See *Galaria v. Nationwide Mutual Ins. Co.*, 2016 WL 4728027 (6CA Sept 12, 2016) (standing requirement satisfied in a data breach class action where the plaintiffs were placed "at a continuing, increased risk of fraud and identity theft" and a "sufficiently substantial risk of harm" beyond just a "possible future injury"); contrast *In re Supervalu, Inc.*, 870 F.3d 763 (8CA 2017) (standing requirement was not met in the data breach class action because the plaintiffs could not "manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending" but allowing one plaintiff to proceed with his claims because he alleged that fraudulent charges had been made to his payment card account following the incident).

As a result of this split, a plaintiff's ability to meet the standing requirement may depend on the circuit in which the case is brought. In jurisdictions where the federal courts have adopted a narrow interpretation of *Spokeo*, this leads to a strange result: plaintiffs may only be able to pursue federal rights in state court as state courts are not bound by the "standing" requirement under Article III. Something close to this happened in a recent Seventh Circuit case.

In *Collier v. SP Plus Corp.*, 2018 WL 2186786 (CA7, May 14, 2018), the plaintiffs filed a state court class action lawsuit alleging that the defendant, the operator of public parking lots at Dayton International Airport, printed receipts that included the expiration date of their credit or debit cards in violation of the Fair and Accurate Credit Transaction Act (FACTA). Because the plaintiffs' claims arose under federal law, the defendant removed the case to federal court and promptly moved to dismiss on the grounds that the plaintiffs lacked standing to sue rendering the federal court without subject matter jurisdiction. The plaintiffs agreed and moved the court to remand the action to state court because it was improperly removed in the first place.

The district court denied the plaintiffs' motion and gave the plaintiffs time to amend their complaint to cure the standing defect. When the plaintiffs did not amend their complaint, the court dismissed the complaint with prejudice. Because the dismissal with prejudice acts as an adjudication on the merits, the plaintiffs could not refile in state court. The plaintiffs appealed the dismissal.

On appeal, the Seventh Circuit Court first noted that the party invoking federal court jurisdiction, in this case the defendant, has the responsibility to make sure that all requirements of that jurisdiction are met. If the defendant did not believe the plaintiffs had standing to sue, it was improper for them to remove in the first instance. Next, the Court noted that under the removal statute, a case must be remanded to state court if "at any time … it appears that the district court lacks subject matter jurisdiction." Examining the complaint, the Seventh Circuit Court agreed that the plaintiffs lacked standing to sue.

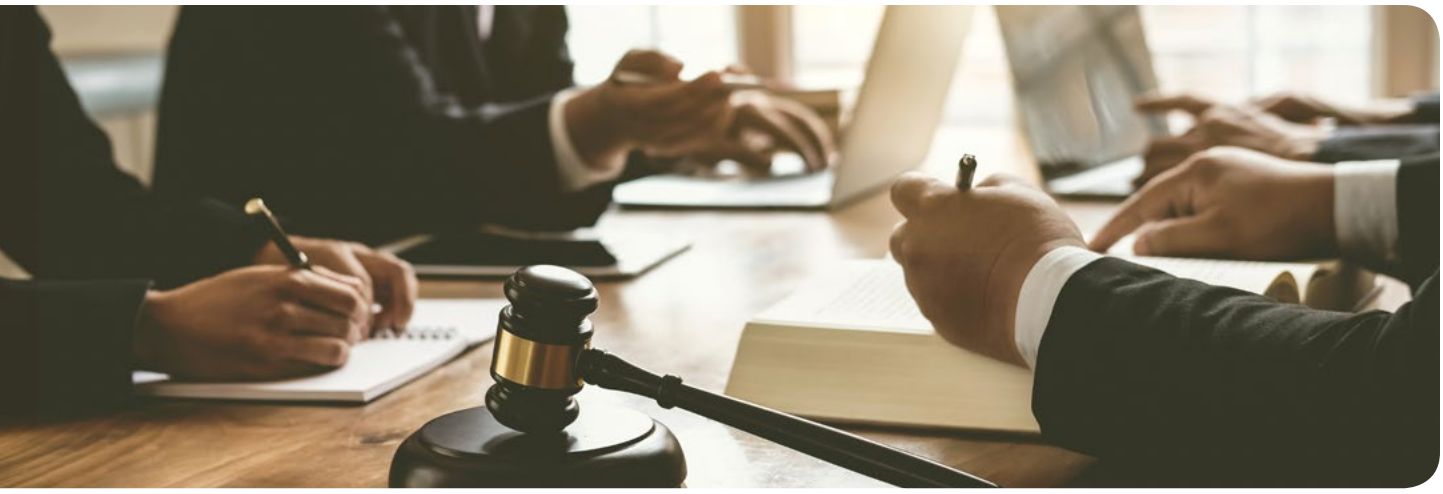
Here, it is clear that Collier and Seitz's complaint did not sufficiently allege an actual injury. A mere reference to "actual damages" in the complaint's prayer for relief does not establish Article III standing. The single reference here falls far short of an allegation that the plaintiffs suffered a concrete harm or appreciable risk of harm apart from the statutory violation. (citations omitted)

Defendants argued that it would be unfair to remand the case because the plaintiffs might then amend their complaint "after it is too late" for removal, and requested the Court to direct the plaintiffs to amend their complaint to support their allegations of actual damages or strike those allegations from the complaint. The Seventh Circuit Court declined the request. "This is impossible. We have no basis to order these plaintiffs how to plead their case in state court after remand. Further, a state's standing doctrine is 'the business' of its own courts; 'it is not for [this court] to venture how the case would there be resolved.'" (citations omitted) The Court also noted that if the plaintiffs amended their complaint or served any other papers in the state court that conferred subject matter jurisdiction on the federal courts, the defendant would have 30 days from service to remove the case to federal court.

While *Collier* turned on the specificity of the pleading, this scenario could arise in a case where a plaintiff alleges damages based on the increased risk of injury from a data breach. That case would be removable in the Sixth Circuit, but not in the Eighth Circuit. In the Eighth Circuit, that case would have to be pursued in state court.

A similar anomaly would occur in a case where the plaintiffs sue for data breach under state law which might be brought in federal court based on diversity of citizenship. The state law might create a private right of action for "bare procedural violations" or for "increased risk of harm." However, since standing is a constitutional question in federal court, the plaintiff would still need to satisfy Article III's "injury-in-fact" requirement. So, the plaintiff's ability to file originally in federal court or the defendant's right to remove might be dependent on the circuit in which the case can be brought.

Standing is a significant issue in data breach cases. Standing can determine whether a case may be brought originally in or removed to federal court. Until the United States Supreme Court clarifies the standing doctrine in private data breach actions, plaintiffs and defendants must know the standing requirements in whichever circuit they find themselves regardless of whether the claim arises under federal or state law.



Fall 2019 eDiscovery

Case **BRIEFS**

Progressive Emu Inc. v Anderson Weidner LLC
2019 WL 3798494 (11th Cir Aug 13, 2019)
The plaintiff's counsel waited until the last business day before trial to serve overbroad "trial subpoena" on the defendant's parent corporation requiring compliance the next business day and outside the 100-mile limitation of Fed R Civ P 45(c)(1)(A). The appellate court upheld an award of attorney fees under Rule 45(d)(1) against the plaintiff's counsel and added an award of attorney fees against the plaintiff's counsel for pursuing a frivolous appeal under Fed R App P 38.

Anokiwave, Inc. v Rebeiz
2019 WL 3935778 (SD Cal Aug 20, 2019)
Despite the district court's acknowledgment that the non-party had agreed to produce subpoenaed records and the defendant's lack of standing to quash the subpoena, the court modified the subpoena based on the defendant's overbreadth and relevancy objections.

Lotus Industries, LLC v Archer
2019 WL 2247793 (ED Mich May 24, 2019)
The district court shifted the cost of uploading subpoenaed records to an eDiscovery review platform plus five percent of the anticipated attorney fees for privilege review and privilege log compilation to the plaintiff pursuant to Fed R Civ P 45(d)(2)(B)(ii). In addition, it required prepayment of the costs based on the plaintiff's past failures to pay sanctions in related litigation.

Casun Invest, A.G. v Ponder
2019 WL 2358390 (D Nev June 4, 2019)
In quashing the defendant's subpoena and awarding sanctions against the defendant pursuant to Fed R Civ P 45(d)(1), the district court noted that where the non-party objects to a patently overbroad subpoena, the issuing party has the duty to either substantially limit and modify the subpoena or withdraw it.

In re Schaefer
2019 WL 2336698 (WD Pa June 3, 2019)
The government's subpoena to non-party was quashed pursuant to Fed R Civ P 45(d)(3)(A)(iv) and 45(d)(3)(B)(ii) to compel expert testimony concerning a report she authored for the RAND Institute regarding the effects and feasibility of the service of transgendered individuals in the U.S. military where report disclosed its sources, data and methodologies and could be impeached by the government's own experts and where compelling experts' testimony would harm her reputation and RAND's reputation for objectivity and independence.

Bellamy v Wal-Mart Stores, Texas, LLC
2019 WL 3936992 (WD Tex Aug 19, 2019)
The defendant filed a motion pursuant to Fed R Evid 502(b) to clawback an inadvertently produced litigation file. The court's *in camera* review of the file revealed that the defendant's expert had conceded the defendant's liability early on in the case. While the court allowed the defendant to clawback its litigation file, the court used the concession to strike the defendant's comparative negligence defense

on the plaintiff's motion for spoliation sanctions under Fed R Civ P 37(e), finding that the plaintiff had been prejudiced by the defendant's loss of a video recording of the plaintiff's accident.

Cruz v G-Star Inc.
2019 WL 2521299 (SDNY June 19, 2019)
The defendant's duty to preserve attached prior to the lawsuit, and it failed to initiate a timely litigation hold and permanently deleted the plaintiff's email account in violation of its own internal retention policy. Even after initiating a litigation hold and subsequent to the plaintiff filing suit, the defendant later deleted the plaintiff's SAP account. The court determined that the defendant's spoliation evidenced an "intent to deprive" under Fed R Civ P 37(e)(2) and awarded the plaintiff an adverse inference jury instruction to cure prejudice from the loss of ESI.

University Accounting Service, LLC v ScholarChip Card, LLC
2019 WL 2404512 (D Ore June 7, 2019)
An individual defendant admitted to intentionally deleting information on his personal computer's hard drive and in his personal backup cloud account after receiving a subpoena in related litigation in which he was a non-party because it was "exactly the type of damning information that [plaintiff wanted] to catch [him] with." The court granted the plaintiff's motion for sanctions under Fed R Civ P 37(e)(2) and would instruct the jury that if it found that the individual defendant acted with the intent to deprive the plaintiff of the deleted information's use in litigation, it could presume that the deleted information was unfavorable to the defendant.

Stimson v Stryker Sales Corporation
2019 WL 2240444 (ND Ga Jan 24, 2019)
The plaintiff was unable to produce all text message exchanges with a coworker, and there were discrepancies between those he did produce and those produced by the coworker. The court denied the defendant's motion for case terminating sanctions under Fed R Civ P 37(e)(2) because regardless of the plaintiff's loss or alleged alteration of text messages, the text messages were available to the defendant via the coworker.

Karsch v Blink Health Ltd.
2019 WL 2708125 (SDNY June 20, 2019)
A plaintiff's duty to preserve triggered when he sent a demand letter threatening to sue the defendant despite not filing a suit until 23 months later as the time of filing was wholly within his control. His failure to preserve an email server containing relevant information resulted in sanctions under Fed R Civ P 37(e)(1), which included allowing the defendants to present evidence to the jury concerning the plaintiff's spoliation and permitting the jury to consider that evidence in evaluating credibility and making its decision.

Incardone v Royal Carribean Cruises, Ltd.
2019 WL 3779194 (SD Fla Aug 12, 2019)
A defendant only preserved ninety-one minutes out of a possible 14,400 hours of video recording of a cruise ship being battered by hurricane force winds. The court denied the plaintiffs' motion for spoliation sanctions under Fed R Civ P 37(e), and found that the preserved video was sufficient to show the impact of the storm on the ship. The plaintiffs suffered no prejudice, especially where the plaintiffs claimed damages for psychological, not physical, injury and during the worst part of the storm, the plaintiffs were confined to their cabins and no video cameras recorded the interior of the cabins.

Thompson v H.W. Clarke
2019 WL 4039634 (WD Va Aug 27, 2019)
The court denied the plaintiff's motion for spoliation sanctions under Fed R Civ P 37(e), holding that even if the defendant acted with an "intent to deprive" the plaintiff of the use of lost video recordings, it would not award sanctions against the defendant due to the video recordings' lack of relevance.

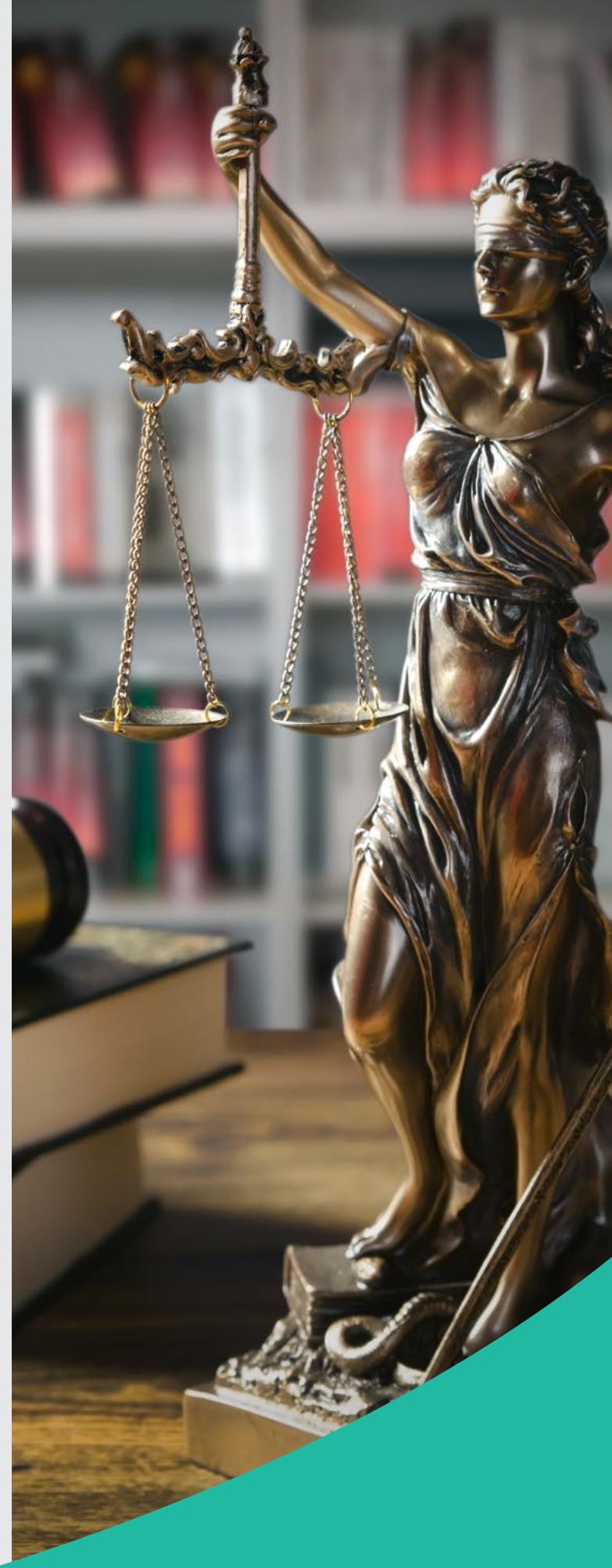
U.S. v Carter
2019 WL 3798142 (D Kan Aug 13, 2019)
Petitioners filed motions pursuant to Fed R Crim

P 41(g) for return of property and pursuant to 28 USC §2255 for post-conviction sentencing relief. The motions were ancillary to criminal proceedings and civil in nature, and the court held that issues concerning spoliation of electronic evidence would be governed under Fed R Civ P 37(e) and the defendant's destruction of relevant ESI in willful violation of numerous court preservation orders constituted "intent to deprive," potentially triggering sanctions that could include adverse inferences.

Woods v Scissons
2019 WL 3816727 (D Ariz Aug 14, 2019)
A defendant's employer, a municipality and non-party in plaintiff's §1983 civil rights action, deleted relevant ESI under its exclusive control after the defendant's duty to preserve had attached. The court imputed the non-party employer's actions to the defendant since the municipality had no sovereign immunity under the Eleventh Amendment and its agreement to indemnify the defendant against any judgment aligned their interests in the preservation of the evidence.

Zhang v City of New York
2019 WL 3936767 (SDNY Aug 20, 2019)
Despite finding that the plaintiffs had established relevancy and prejudice for the defendant's loss of video surveillance footage and telephone recordings, the court limited sanctions under Fed R Civ P 37(e)(1) to attorney fees and costs associated with bringing spoliation motion because the plaintiffs could obtain (and had obtained) other evidence, such as testimony and medical records, to prove their case.

Heartland Food Products, LLC v Fleener
2019 WL 2501862 (D Kan June 17, 2019)
Parties had agreed to produce via PDF format in response to "targeted requests for email communications" and that "no open-ended ESI reviews [would] be required." The court would not order the plaintiff to reproduce a TIFF production of emails where the defendant issued open-ended, not targeted, requests for the emails, the emails were produced as kept in



the usual course of business as allowed under Fed R Civ P 34(b)(2)(E)(i) and the requests did not otherwise specify the format for production under Fed R Civ P 34(b)(2)(E)(ii).

Homeland Ins. Co. of New York v Health Care Serv. Corp.
330 FRD 180 (ND Ill 2019)
In a declaratory judgment and breach of a contract action concerning coverage under a second-layer excess insurance policy, the court denied a plaintiff's motion to compel production of a settlement agreement between the defendant and the primary coverage provider, as the defendant had made no request for coverage under a second-layer policy, making evidence regarding "exhaustion of coverage" irrelevant to the proceedings.

Keim v ADF Midatlantic, LLC
2019 WL 2298787 (SD Fla May 30, 2019)
The court granted the defendants' motion to compel production of email exchanges between the plaintiff's counsel and counsel for non-parties regarding the modification, scope and execution of subpoenas as the emails were relevant and proportional to the needs of the case under Fed R Civ Pro 26(b)(1), given the defendants' strong interest in ensuring the validity and reliability of the documents subpoenaed from the non-parties and were not a protected attorney work product.

Olsen v Owners Ins. Co.
2019 WL 2502201 (D Col June 17, 2019)
Neither Fed R Civ P 26(a)(1) nor 26(b)(1) required plaintiff to produce a total amount for his non-economic and impairment damages as they were for garden-variety emotional distress and permanent physical impairment and such damages are not typically suitable to a precise calculation.

Laub v Horbaczewski
2019 WL 3492402 (ED Cal July 30, 2019)
In a case based on diversity jurisdiction, a court finds that state law controls procedure for determining whether a document is privileged and declines *in camera* inspection request based on prohibition in California Evidence Code 915.

Ciesniewski v Aries Capital Partners, Inc.
2019 WL 2869671 (SD Ind July 3, 2019)
Where one defendant acted as agent for other defendants in the hiring of attorneys to file debt collection actions nationwide, under Fed R Civ P 37 court would not compel defendant-principals to produce records regarding debt collection actions where the plaintiff could simply request defendant-agent since it had only direct contact with attorneys.

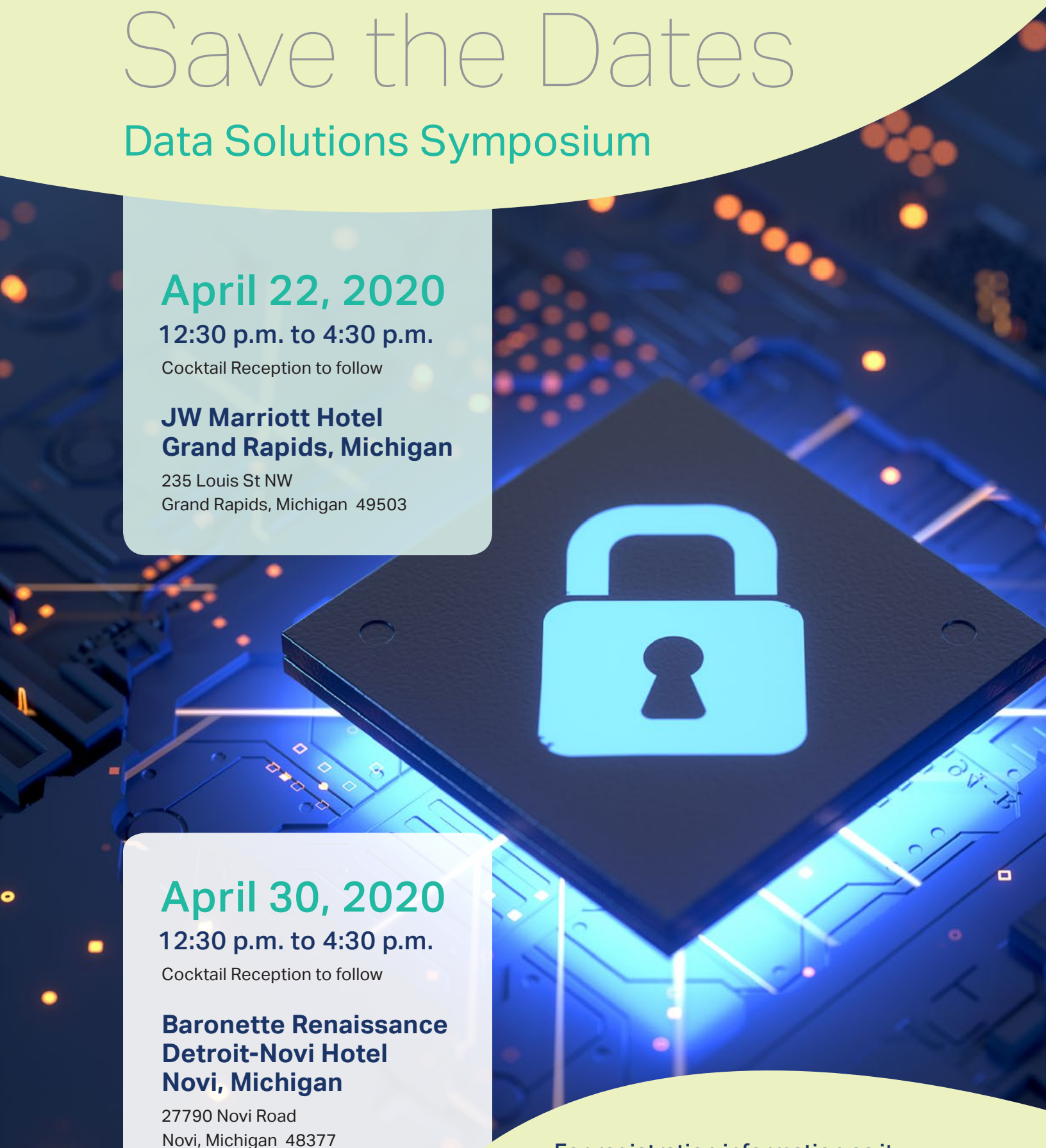
Wang v Omni Hotels Mgmt. Corp.
2019 WL 3852590 (D Conn Aug 16, 2019)
Court compels production of video recording of plaintiff's "slip and fall" accident at the defendant's hotel, but only after plaintiff's deposition, finding that video recording is "surveillance video" and it would lose its impeachment value if disclosed to plaintiff prior to her deposition.

Dixon v Bank of America, N.A.
2019 WL 3767097 (SD Fla Aug 9, 2019)
In denying a non-party's motion to quash subpoena under Fed R Civ P 45(d)(3) on grounds raised by the non-party, the court would not *sua sponte* raise issues of relevancy and proportionality despite having genuine concerns about both where neither the non-party nor the other party to proceedings raised those issues, and the court therefore deemed those issues waived.

Johnson v Soo Line Railroad Co.
2019 WL 4037963 (ND Ill Aug 27, 2019)
Before ruling on defendant's motion to compel production of a plaintiff's tax returns, the court would apply proportionality factors under Fed R Civ P 26(b)(1) and weigh the defendant's need for the returns with the burden that compelled production of income tax returns may impose on voluntary self-reporting of income under federal tax system during the court's *in camera* review of the tax returns.

Save the Dates

Data Solutions Symposium



April 22, 2020

12:30 p.m. to 4:30 p.m.

Cocktail Reception to follow

JW Marriott Hotel
Grand Rapids, Michigan

235 Louis St NW
Grand Rapids, Michigan 49503

April 30, 2020

12:30 p.m. to 4:30 p.m.

Cocktail Reception to follow

Baronette Renaissance Detroit-Novi Hotel
Novi, Michigan

27790 Novi Road
Novi, Michigan 48377

For registration information as it becomes available, please go to wnj.com/events

Warner Norcross + Judd

These materials are for educational use only. This is not legal advice and does not create an attorney-client relationship.

401 EAST MICHIGAN AVENUE, SUITE 200, KALAMAZOO, MI 49007-5842

ADDRESS SERVICE REQUESTED

PRSRT STD
U.S. Postage
PAID
Grand Rapids, MI
Permit # 564

Warner Discovery Center

Jay Yelton, Partner	jyelton@wnj.com
Myra Willis, Senior Project Manager	mwillis@wnj.com
Adam Cefai, Litigation Support Manager	acefai@wnj.com
Zach Nevenzel, Staff Attorney	znevenzel@wnj.com
Jeremy Nufer, Staff Attorney	jnufer@wnj.com
Bruce Olson, Staff Attorney	bolson@wnj.com
Todd Rooze, Staff Attorney	trooze@wnj.com
Kenneth Treece, Staff Attorney	ktreece@wnj.com
Ashley Tyler, Project Manager	atyler@wnj.com
Tim Winslow, eDiscovery Support Specialist	twinslow@wnj.com

next issue:

We will focus on a topic of growing importance:

AUGMENTED INTELLIGENCE + SOCIAL MEDIA

The Warner Norcross + Judd Discovery Center offers wide-ranging eDiscovery and Data Analytic services. Our discovery professionals have 100+ years of combined expertise in discovery practice with a special emphasis on electronic data.

We are available to answer your questions regarding the discovery process and will work with you to develop a customized suite of services that fits your needs and your budget.

our services include:

- Data Intake
- Data Processing
- Data Hosting
- Data Review
- Data Production
- Data Analytics
- Early Case Assessment
- Project Management
- Discovery Dispute Mediation
- Discovery Management & Consulting

wnj.com