E-Discovery

Avoiding **Post-Brexit** Multilingual Review Pitfalls

BY CHRISTOPHER C. O'BRIEN

© ISCTOCK

As the United Kingdom plans its exit from the European Union, dedicating time to fine tune legal and compliance discovery processes with multilingual capabilities will be increasingly important to companies and their outside counsel.

It's expected that the U.K.'s historic referendum to leave the EU will result in more cross-border litigation, investigations and regulatory oversight for U.S. and U.K.-based businesses with international operations due to additional complexities brought on by the farewell. Consequently, a potential influx of multilingual-document reviews await legal counsel. Here are a few reasons why:

• Brexit could have some impact on the enforceability of contracts governed under English law, and many companies are considering reviews of material contracts where they are likely to include provisions that may be triggered by Brexit.

• For financial institutions, there may be increased regulatory implications necessitating reviews.

• From an intellectual property perspective, there is uncertainty surrounding the Unified Patent Court system, as Brexit signals an end to the U.K.'s involvement in this "one stop shop" system, possibly weakening the attraction of U.K. courts as the venue to settle patent disputes.

• While English is the first choice for EU institutions, no country other than the U.K. has it registered as its primary language. Regulations (by unanimous EU adoption) would have to thus be changed in EU states to maintain the language, challenging the current ubiquity of English within EU government institutions and corporations.

Multi-language reviews are notoriously complicated. So until Brexit becomes more of a reality and can guide data privacy laws, understanding the impact foreign language will have on e-discovery, where the major pitfalls can occur—and how to avoid them—can make legal matters more compliant and cost-effective.

Identify Multilingual Documents Before Starting

Legal teams collecting documents from offices or subsidiaries based in the U.K. should anticipate that their data collections will contain multilingual language documents due to some of the factors discussed above. Otherwise, they'll invest countless hours and dollars in categorizing documents by search terms, only to later come across documents written in Arabic or Chinese that will require them to start the process anew to account for the multi-language documents.

Many e-discovery review platforms have the capability of detecting foreign languages. The software must be able to handle languages that do not use the Roman alphabet during the processing, search, and analytics phases of the review.

Predictive coding can work with any language, so long as the seed set is coded by a skilled attorney with the requisite knowledge, and can prioritize the documents most likely to be responsive for early review and cull non-responsive documents.

Organizations that use discovery software with predictive analytics that parses language at the sentence level, rather than at the document level, can identify which languages a data set contains as well as the percentage of each language in the collection. Armed with this information, they can choose the right software, tailor workflows, and marshal the necessary human resources for a successful review project.

Understand Complexities Of Foreign Languages

Foreign languages alone are complex. Instant messaging, SMS, social media, and other evolving channels—while revolutionizing how we communicate—have simultaneously complicated them more so.

For example, "Y do we O $? LMK UR thoughts," meaning "Why do we owe money? Let me know your thoughts," is difficult enough to handle in English. Now you must add the complexity of a foreign language to slang and text speak. Efforts to use search terms will almost certainly not capture the universe of potentially relevant information.

When foreign language combines with chat-speak or other obscure slang, how can a reviewer or computer algorithm detect legally significant innuendo?

Machine translation tools can handle mass volumes of data quickly and cheaply and give counsel a general understanding of the basic premise and relevancy of a document. However, the results will not always be precise, especially when documents contain unfamiliar jargon, nonstandard abbreviations, convoluted legal syntax, or sophisticated financial data that require accurate translation for defensible review. Typically, organizations will need to recruit resources to review these documents in the specific foreign language.

Engage Industry and Domain Experts

Once documents that are likely to be responsive are isolated, the next step is often a foreign-language review for tone, context, or idioms and jargon that machine translation tools can't assess.

Finding qualified native document reviewers abroad can be challenging. For this reason, many organizations look to service providers that have scalable foreign language and subject-matter experts readily available. The key is to find an organization with a roster of well-trained and managed local reviewers with the requisite skill set.

Language fluency is the bare minimum requirement, and proficiency should be verified through testing. Experience in the nuances of American discovery, privilege concepts, and the industry and subject matter of the underlying legal case or investigation are all highly desirable. More knowledgeable professionals can lend their insight in the development and refinement of search terms and syntax. They can also educate the rest of the review team on regional dialects, geographic-specific business terms, and conversational quirks, both formal and informal.

Service providers must be thoroughly vetted up front to confirm that they apply rigorous recruiting standards, train reviewers thoroughly and supervise them closely. The presence of strong on-site project management teams can also ensure greater consistency and more reliable performance.

Control Review Costs

With the size of today's data sets, translating and reviewing every document is wasteful and unrealistic. And linear review in any foreign language progresses more slowly than English-language reviews. Additionally, the fees for foreign language review can quickly escalate depending on a set of factors, such as the special skills and qualifications required, the language requiring review, the complexity of the task (i.e., simpler translation or more involved » Page 10

CHRISTOPHER C. O'BRIEN *is senior vice president of Xerox Legal Business Services (XLS) and is an expert in e-discovery, data privacy and cross-border litigation as it relates to discovery.*

E-Discovery Techniques to **Investigate** And **Mitigate** Insider Threats

BY BRIAN FOX, DOUGLAS BLOOM AND CAT CASEY

Each year PwC surveys approximately 10,000 CEO, CFOs, CIOs, CISOs and other executives in charge of information security from companies all over the world about the state of their information security and the threats facing their organizations.[1] Over the past few years, an interesting trend has emerged: The greatest increase in information security incidents has surrounded the theft of intellectual property (IP), including hard intellectual property, i.e., trade secrets. And the most common perpetrators? Insiders.

Law firms, compliance organizations and general counsel's offices have grown accustomed to regularly handling insider investigations involving the typical employee malfeasance: fraud, abuse, embezzlement and harassment. These groups leverage e-discovery tools to manage the document productions and review for the litigation that often follows these investigations.

These tools, though, should not be simply reserved for legal actions. When it comes to investigations into the theft of IP, the use of e-discovery tools as part of the investigation itself may significantly reduce the time required to uncover or rule out suspected bad behavior, while helping companies control the cost of what appears to be an increasingly common event.

Insider Intellectual Property Theft

Indeed, respondents in our Global State of Information Security Survey identified current employees (cited by 34 percent) and former employees (29 percent) as the largest categories of threat actors responsible for misappropriation and exfiltration of IP. The report also found that while employee, customer, and "soft" IP data are the top three targets of cyberattacks, theft of "hard" IP increased 56 percent overall in the past year and 183 percent in the financial services industry alone. For financial services organizations, 72 percent of security incidents involved a current or former employee, while third parties with trusted access were responsible for 41 percent of the detected security incidents. Sixty-two percent of security incidents at industrial product organizations involved a current or former employee.[2] » Page 11

BRIAN FOX *is a principal in the computer forensic and e-discovery practice at PwC and a member of its financial crimes unit.* DOUGLAS BLOOM *is a director of PwC's cyber crime and incident response practice and a member of its financial crimes unit.* CAT CASEY *is a director in the computer forensic and e-discovery practice.*


© ISCTOCK

Social Media Investigations: Digging Deep, Or Just Scratching The Surface?

BY DANIEL M. BRAUDE AND DANIEL E. LUST

Time and again, defendant corporations find themselves settling cases at inflated valuations simply to avoid the costs to preserve, review and produce substantial amounts of electronically stored information (ESI). In contrast, individual plaintiffs with very few documents to produce, if any, have been sitting back and relaxing throughout discovery.

This is changing as defendants increasingly use social media to turn the tables on plaintiffs. A well-known example involved the surviving husband in a wrongful death case in Virginia who shared a picture of himself on Facebook in which he was drinking a beer and wearing a t-shirt that read "I ♥ Hot Moms." His attorney instructed him to delete this picture, but not before it was spotted and retained by defense counsel, ultimately resulting in an adverse inference instruction to the jury and a fine of more than $700,000. *Allied Concrete v. Lester*, 285 Va. 295, 302 (2013).

Defendants can and should use photos, tweets, vines, snaps, emojis and whatever else can be pulled from a plaintiff's social media trail to potentially discredit the plaintiff and demonstrate that alleged damages are not based in reality. But are defense attorneys today properly digging through social media postings, or are they just scratching the surface?

New York's Social Media Authority

The creation of Facebook in 2004 kicked off the social media boom. But it was not until September 2010 that New York courts dipped a toe into the treacherous social media waters and addressed the issue of discoverability. In *Romano v. Steelcase*, 30 Misc.3d 426 (Sup. Ct. Suffolk County, 2010), the court granted access to the plaintiff's complete Facebook and MySpace accounts, including private and deleted content, following production by defendants of public postings from both accounts that depicted the plaintiff's "active lifestyle" in contradiction to her claims:

> [W]hen plaintiff created her Facebook and MySpace accounts, she consented to the fact that her personal information would be shared with others, notwithstanding her privacy settings. Indeed, that is the very nature and purpose of these social networking sites, else they would cease to exist. Since plaintiff knew that her information may become publicly available, she cannot now claim that she had a reasonable expectation of privacy….

In some situations, unfettered access to the private portion of a social media account could be characterized as a "fishing expedition." Yet, in *Romano*, the court focused on the existence of contradictory materials and determined that the defendants' right to discovery, specifically their need for materials hidden behind privacy settings, far outweighed the plaintiff's relative privacy interest. Two months later, the Appellate Division in *McCann v. Harleysville Ins. Co. of N.Y.*, 78 A.D.3d 1524 (N.Y. App. Div. 4th Dep't. 2010), articulated the standard that a party seeking social media content must establish "a factual predicate with respect to the relevancy of the evidence." Under this standard, access will likely be granted to a plaintiff's protected content where a defendant establishes a "factual predicate" by producing material found on "public" portions of social media platforms that sufficiently contradicts the nature and character of the plaintiff's claims or testimony.

Gaps in Social Media Authority and Guidance

The lasting impact from *Romano* and *McCann* is the commentary on plaintiff's diminished privacy interest and the application of the "factual predicate" standard to social media, respectively. This authority remains relevant and is still cited across courts in New York and around the country. See *Forman v. Henkin*, 134 A.D.3d 529, (N.Y. App. Div. 1st Dep't. 2015); *Breton v. City of New York*, 2016 WL 2897848 (Sup. Ct. New York Cty 2016); *Higgins v. Koch Dev.*, 2013 WL 3366278 (S.D. Ind. 2013); *Keller v. Nat'l Farmers Union Prop. & Cas. Co.*, 2013 WL 27731 (D. Mont. 2013). However, the rapid pace of innovation in social media has caused these 2010 opinions and » Page 10

DANIEL M. BRAUDE, *a partner in Wilson Elser's New York and White Plains offices, is co-chair of the firm's e-discovery practice and serves as an adjunct professor at Pace University School of Law.* DANIEL E. LUST *is an associate in the White Plains office and focuses on general liability and transportation litigation.*

Inside

Got Any Custodians? Go Fish!

Explore the pros and cons of a custodian-based approach to e-discovery.

© ISCTOCK

BY CHRISTOPHER JAGOE AND THOMAS FLEMING

When the authors were younger attorneys, back when dinosaurs roamed the earth, the practice to identify responsive, non-privileged documents for production involved dank, dimly lit warehouses, mountains of "bankers boxes" and countless paper cuts. That practice has gone the way of the mimeograph machine. Today, electronic discovery and terabytes of electronically stored information (ESI) rule the day. While the modern practice of lasering through the ESI, rather than paper documents, on its face sounds efficient and easy, in practice it is far from the case.

If you ask e-discovery experts they will gladly tell you that all that is required is for the parties to agree to limit the searches for responsive ESI to those in the electronic files and emails of a defined subset of employees ("custodians"), and that those documents would then be electronically searched by a group of agreed-upon keywords. This seemingly simple procedure suffers in the execution. How do you know which custodian to select, how do you check that your adversary had identified the correct custodians? How can you tell whether the search terms are adequate to uncover what it required? How can you be sure that you are not missing anything critical? What if your adversary won't agree to disclose search terms?

CHRISTOPHER JAGOE *and* THOMAS FLEMING *are partners in Kirkland & Ellis' intellectual property practice group based in New York.*

As to the last issue, in the recently decided *Burd v. Ford Motor Co.*, 2015 U.S. Dist. LEXIS 88518, (S.D. W. Va. July 8, 2015), defendant Ford refused to share its search terms with plaintiffs, the court disagreed and held that general objections to discovery are outmoded and unpersuasive, and ordered that Ford provide a 30(b)(6) witness to testify as to the search terms used. One of the advantages of modern-day electronic discovery is that more and more courts are familiar with the process and how the sausage is made. That being so, courts are more willing to assist litigants and to compel recalcitrant parties who are seeking to withhold relevant information. The system is, and continues to be, rooted in a professional's good faith: Still, trust but verify.

The problem facing litigants, particularly in complex litigation such as patent disputes, is that you cannot tell until you are well into the discovery process how "forthcoming" your adversary has been in identifying key custodians and search terms. As a matter of practice, there are several layers of the onion to peel away before one can be sure that it has done all it can to confirm that its adversary has been operating in the utmost good faith.

In most complex patent litigation, one or more of the parties will be large, multi-national corporations, whose day-to-day operations involve detailed and layered electronic data sources, email systems, structured and network databases, and multiple levels of shared networks and drives. Again, it all starts with the right custodians.

Employing a custodian-based system for parsing electronic discovery demands that the requesting party ensure that the producing party has identified all of the "non-custodial"-based data sources likely to contain relevant information. Indeed, the Local and Standard Rules for ESI in most jurisdictions require the parties to identify these data sources. One way to identify the relevant data sources is to question the custodians. They will know which share drives and network spaces they and their colleagues use, and where they regularly store relevant information. If your adversary is not willing to produce such information, courts are not reluctant to enforce their local rules and order the information to be disclosed. In *Viteri-Butler v. University of California, Hastings College of Law*, No. CV 12-02651 (N.D. Cal. Sept. 30, 2013), the plaintiff requested the defendant to "specify what information systems as to which it has placed a litigation hold and what information systems it has searched for documents responsive to Plaintiff's Rule 34 requests, as required under the [Northern District of California]'s Guidelines for the Discovery of Electronically Stored Information." The court ordered the defendant to provide an amended certification that identified the location and types of information systems with potentially discoverable ESI (including date ranges of the ESI available on each system) and the search methods (including search terms) used to identify discoverable ESI.

Employing **a custodian-based system for parsing electronic discovery** demands that the requesting party ensure that the producing party has identified all of the "non-custodial"-based data sources likely to contain relevant information.

So how do you know that your adversary has provided the names of the right custodians? In a patent case, named inventors and authors of publications on the technology should be custodians unless they have left the company long ago. Also, FRCP 26 requires a party to identify the names and subject matter of individuals upon whom the party may rely to prove its claims and defenses. Those people should also be custodians. It is also helpful to serve interrogatories asking for the 10 or more individuals who are most knowledgeable about certain subject areas in the particular interrogatory. Then cross-check those answers to see how they compare to the custodians identified by the adversary.

If doubt still haunts you, then see if your adversary will agree to an early sample production. In IP cases, this often involves invention documents, sales and licensing documents, product launch and commercialization documents. Often, the distribution or email chains from such documents will give an indication of who the key individuals were during a given phase of the dispute. Also, ask to add three more custodians after that preliminary production is made based on names revealed from those documents.

Courts are not unsympathetic to the "shot in the dark" type practice that custodian-based discovery can create. In *American Home Assurance Co. v. Greater Omaha Packing Co.*, No. 11-CV-270 (D. Neb. Sept. 11, 2013), the court remarked that it "cannot compel the production of information that does not exist," but then ordered the defendant to disclose the ESI sources it had searched or intended to search and, for each source, the search terms used. According to the court, this information would provide the plaintiff "an adequate opportunity to contest discovery of ESI."

Of course, an early 30(b)(6) deposition might work to provide much of the same information, but given the limitations on the number of depositions in cases today, doing so without document production may be a wasted bullet. As *Apple v. Samsung Electronics Co.*, No. 12-CV-0630-LHK (PSG), 2013 WL 1942163, at *2 (N.D. Cal. May 9, 2013) noted, case law suggests that search terms and choice of custodians used in the document collection and production process are not necessarily protected as attorney work product.

If all of this still concerns you, then simply do not agree to a custodian based process for collecting and producing documents in a litigation. However, in this age, it is likely that the court will impose some parameters nonetheless, so be prepared.

Social Media

« Continued from page 9

their progeny to become outdated.

Compared to 2010, the current social media landscape is almost unrecognizable, with many notable platforms, including Instagram, LinkedIn, Twitter and Snapchat, gaining prominence over the past several years. In addition, the very definition of "social media" has been blurred as quasi-social and third-party mobile apps, such as Waze (a GPS app) and Venmo (a digital payment app), have developed followings. This begs the question of whether these platforms fall within the social-media-specific "factual predicate" standard.

A larger question looms: Should demonstration of a factual predicate through social media material on one platform permit access to private material on other platforms? To date, New York courts have largely treated individual accounts as discrete locations on which data can be stored. Is this a workable approach in light of "linking" functionality where users on one platform simultaneously post identical content across multiple platforms? The intermingling of accounts creates a scenario where courts will likely treat a plaintiff's social media content as consisting of a single portfolio of material rather than discrete and unrelated accounts.

Rapid innovation also has caused a lack of guidance regarding counsel's ethical obligations. Snapchat's process for viewing another user's postings provides a unique example. Traditional platforms such as Facebook, Instagram, LinkedIn and Twitter offer publicly accessible landing pages for each user's profile while indicating whether certain content is accessible only to that user's "friends." This does not exist on Snapchat. Also, there is no traditional access ("friend") request where *mutuality* exists through an option to approve or deny the request. Instead, one's Snapchat postings can be viewed only by those that *unilaterally* "add" that user, a novel functionality not covered by the Social Media Ethics Guidelines of the Commercial and Federal Litigation Section of the New York State Bar Association, June 9, 2015. Once this "adding" occurs, the owner of the added account automatically receives a notification that he or she has been "added" by a certain user.

Could "adding" another user on Snapchat be considered an unethical communication with a person represented by counsel? The answer to this question *appears* to be no. A 2010 opinion of the New York State Bar Association's Committee on Professional Ethics (Formal Opinion No. 843), explicitly allowed an attorney to view publicly accessible portions of an opposing party's account. In addition, the American Bar Association's Standing Committee on Ethics and Professional Responsibility (Formal Opinion No. 466) explained in 2014 that LinkedIn's analogous page-view notification feature was not an impermissible communication, but only an innocuous communication between LinkedIn and the user. If this Snapchat "add" feature were deemed per se unethical, it would run contrary to these opinions. In fact, it would entirely prohibit viewing a user's publicly available content despite that user's lack of an expectation of privacy. This issue, among other social media-related ethical issues, has remained unanswered while Snapchat has grown into one of the most popular platforms. In any event, it is difficult to think that ethical guidance will be able to keep pace with social media's expansion.

Digging Deep

In contrast to the early days of Facebook, an individual's social media content is likely to be spread across multiple platforms. It is not enough to focus on Facebook and merely take screenshots from an easily identified account. This approach may overlook treasure troves of metadata, possibly pinpointing when and where a plaintiff visited a particular location, not to mention entire social media accounts that are not easily identified. In addition, the general population has increasingly implemented privacy settings and restricted access exclusively to approved "friends" or "followers." It also remains possible that some plaintiffs' attorneys may still follow the approach taken by counsel in *Lester v. Allied Concrete*, or at least recommend tweaks to their clients' privacy settings. Regardless, a proper social media investigation and forensic collection, which should be conducted early and often, will still frequently uncover useful material on anyone who maintains even a modest online presence.

In today's world, uncovering probative social media material requires much more than "Googling" a plaintiff's name and crossing your fingers. Attorneys must know the right questions to ask during discovery. This is not limited to straightforward questions about name-brand platforms such as Facebook and Twitter, but includes questioning designed to uncover the use of lesser-known platforms and third-party mobile apps or to confirm ownership of accounts using pseudonyms or misleading profile usernames.

A proper investigation does not stop with a plaintiff's accounts, but extends to friends and relatives whose profiles may not be hidden behind privacy settings. It is no longer enough to merely understand the law. Counsel today must develop a thorough understanding of a wide variety of social media platforms and third-party apps, or associate with one who does, especially when technology develops at a lightning pace and where fads come and (Pokémon) go in the blink of an eye.

Post-Brexit

« Continued from page 9

review), and the location of the review.

In any review, the best way to lower the discovery budget is to limit the amount of review time. This occurs in two steps: reducing the number of foreign language documents that require review and then increasing the speed of review.

As discussed earlier, when used at the inception of a project, machine translation can sample foreign language documents so review teams can make more informed decisions about relevance. In some cases, organizations may be tempted to proceed to native translation to gain a more precise understanding before review. However, given the exorbitant cost of human translation, it may make good financial sense for reviews with a high percentage of multi-language documents to have foreign language attorneys first review the documents in their native language and then only translate the documents that are relevant to the case.

To expedite review, organizations should choose a discovery suite with robust analytics tools capable of comparing concepts and relationships across documents regardless of language, so reviewers can target the most critical custodians and identify anomalous behavioral patterns. Keyword filtering is still viable with these documents, but it is critical that discovery specialists collaborate with linguistics experts, who can ensure that search terms account for local cultures, dialects and colloquialisms.

Predictive coding can work with any language, so long as the seed set is coded by a skilled attorney with the requisite knowledge, and can prioritize the documents most likely to be responsive for early review and cull nonresponsive documents. Tools such as email threading, deduplication, and near-duplicate identification can avoid the rework that occurs when multiple copies of identical or similar documents proliferate throughout a data set. Other analytics tools that cluster related documents can provide the context required to hasten understanding and review.

Keep in mind that the rules may change if a document collection contains digitized hard-copy documents. Analytics and machine translation tools are ideal for native electronic files, since they can access both the text and metadata of a document, but they are less effective with scanned files that must undergo optical character recognition.

Adhere to Data Privacy Rules

Until the U.K. formally withdraws from the EU, the U.K.'s Data Protection Act 1998, which implements the EU Data Protection Directive, is still the law of the land. While refining processes to better handle multi-language documents, organizations must still consider a host of issues to remain compliant, including how to set up proper access controls to the secured data; where to conduct the document review (either in-country, on site or elsewhere as allowed); and how to protect sensitive data to comply with privacy rules, such as by redaction. Records that require heightened protection include personally identifying information, payment card information, protected health information and geolocation data.

Many organizations form a cross-functional team that includes their data privacy officer, outside counsel and third-party discovery vendors. The team can then be tasked with the development of a defensible strategy that addresses the issues of legally acceptable data transfer and processing. In addition, organizations concerned about the sanctity of their data and reluctant to transfer their data offsite can opt for a mobile "backpack" solution, which will allow all processing to occur on site, within the organization's firewall.

Take a Proactive Approach To Compliance

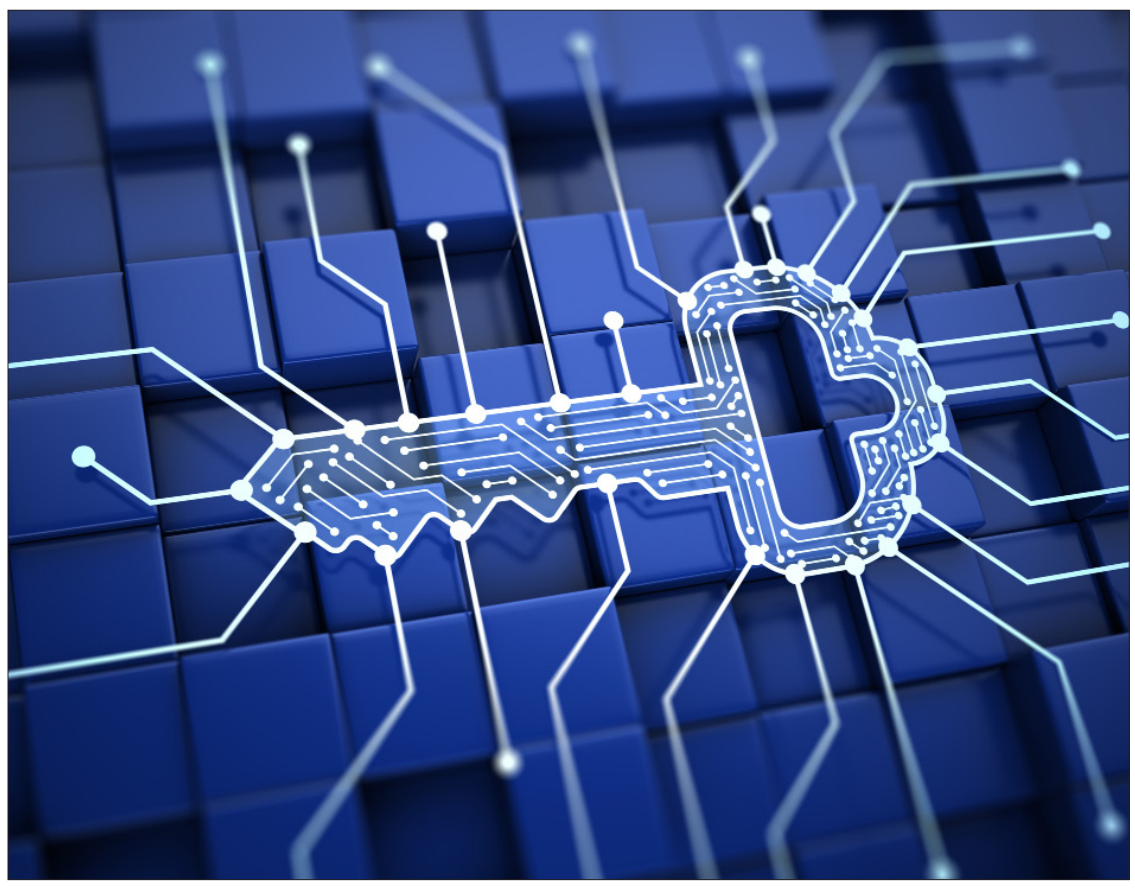
A large number of organizations still take a reactive approach to reviews, reviewing documents (including those in foreign languages) on a case-by-case basis after a legal matter or compliance review has commenced. When documents are parsed out to outside counsel for review, it can complicate a review if different coding designations are made and sensitive or private data is inadvertently disclosed through production.

So, many companies are now adopting analytics systems for ongoing compliance monitoring. Large amounts of data can be filtered to the important facts to help flag potentially "risky" activity on a real-time basis, identify isolated incidents and create alerts to systematic issues for further review (and remediation) by legal and compliance teams—before litigation hits.

Conclusion

Legal and compliance reviews are daunting enough on their own. Add the complications of an event like Brexit, and even the most reliable protocols and tactics for reviewing significant numbers of foreign language documents can snare the savviest counsel. By understanding the obstacles, applying the right technology and recruiting skilled personnel, organizations and their legal counsel can minimize the risks.

How Will NY Courts Handle **Encrypted Communications?**



© ISCTOCK

BY RONALD J. HEDGES AND KRISTEN B. WEIL

Encryption may soon be a recurring challenge for civil litigators. Encryption appears to be growing across electronic devices that create, store and transmit electronic information.

Public awareness of government surveillance and perceived invasions of privacy highlight the existence of encryption technologies and the perceived ability to use encryption to protect privacy. The conflict between privacy and law enforcement needs has been played out in disputes between the U.S. Department of Justice in the Northern District of California and the Eastern District of New York earlier this year. See, e.g., J.H. Koo, "Encryption Called Essential for Privacy, Security, Economy," 16 DDEE 246 (2016); J. DaSilva, "4th Amendment Should Balance Safety, Privacy: Panelists," 16 DDEE 287 (2016). Yet, the same devices that can be at issue in criminal investigations may well contain electronically stored information (ESI) relevant and therefore discoverable in civil litigation in New York state as well as federal courts. What arguments might be advanced in support of and in opposition to discovery requests for encrypted ESI? How might a court rule?

We are unaware of any New York state case law that addresses encryption in any context, civil or criminal. Nevertheless, we need to begin somewhere and that might be with *Forman v. Henkin*, 134 A.D.3d 529 (1st Dept. 2015). At issue in *Forman* was a lower court decision that had allowed discovery of Facebook postings made by the plaintiff, who brought a personal injury action arising out of a horseback-riding accident. Applying "settled principles" that govern discovery in the New York courts, the Appellate Division reversed:

> We conclude that defendant has failed to establish entitlement to either plaintiff's private Facebook photographs, or information about the times and length of plaintiff's private Facebook messages. The fact that plaintiff had previously used Facebook to post pictures of herself or to send messages is insufficient to warrant discovery of this information (see *Tapp*, 102 AD3d at 620 [the plaintiff's mere utilization of a Facebook account is not enough]). Likewise, defendant's speculation that the requested information might be relevant to rebut plaintiff's claims of injury or disability is not a proper basis for requiring access to plaintiff's Facebook account (see id. at 621 [the defendants' argument that the plaintiff's Facebook postings might reveal daily activities that contradict claims of disability is "nothing more than a request for permission to conduct a fishing expedition"] [internal quotation marks omitted]; *Pecile*, 113 AD3d at 527 [vague and generalized assertions that the information sought might conflict with the plaintiff's claims of emotional distress insufficient]). [footnote omitted].
>
> However, in accordance with standard pretrial procedures, plaintiff must provide defendant with all photographs of herself posted on Facebook, either before or after the accident, that she intends to use at trial. Plaintiff concedes that she cannot use these photographs at trial without having first disclosed them to defendant.

134 A.D.3d at 531, 22 N.Y.S.3d at 181.

There was a strong dissent in *Forman* that challenged the majority position that earlier case law should be reconsidered with regard to the discovery of social media. The majority and dissenting decisions also differed on the circumstances under which in camera review might be appropriate, the majority concluding that such review was in the discretion of the trial court. But, with these caveats in mind, *Forman* can guide consideration of how courts might approach encryption.

The first question is a threshold one: Is the encrypted ESI at issue discoverable? As *Forman* recognized, "CPLR 3101(a) provides that, '[t]here shall be full disclosure of all matter material and necessary in the prosecution or defense of an action.' In determining whether the information sought is subject to discovery, '[t]he test is one of usefulness and reason.'" 134 A.D.3d at 530, 22 N.Y.S.3d at 180 (citation omitted). Proceeding from this principle of broad discovery, *Forman* affirmed that the party seeking discovery bore the burden to establish a sufficient factual predicate of relevancy. This is where the defendant in *Forman* failed: He could only offer speculation that Facebook postings were relevant to the claims or defenses in the action. Consistent with *Forman*, a party seeking access to encrypted ESI would have the burden to establish relevance of what was sought and a party opposing access would argue that, absent some factual predicate, the requesting party was embarking on nothing more than a fishing expedition.

Assuming that the encrypted ESI is discoverable (and leaving for another day whether the ESI, once accessed, should be subject to an in camera review before production, whether the responding party should review the ESI and produce relevant portions, or whether the requesting party should be given the proverbial (decryption) key and allowed to "rummage" through *all* content), what happens if the producing party refuses to produce? If she simply declines to comply with a request, then the moving party can seek judicial assistance in the form of an order to comply. Noncompliance will presumably lead to some form of judicial compulsion.

In the criminal context, motions to compel a party to decrypt data have met mixed results. Several courts have concluded that compelling a party to produce an alphanumeric password to decrypt data is a testimonial communication that would violate the party's Fifth Amendment right against self-incrimination. See, e.g., *In re Grand Jury Subpoena Duces Tecum dated March 25, 2011*, 670 F.3d 1335 (11th Cir. 2012); *Commonwealth v. Baust*, 89 Va. Cir. 267 (Va. Cir. Ct. 2014); *State v. Trant*, No. CUMCDCR201502389, 2015 WL 7575496 (Me. Dist. Ct. Oct. 27, 2015). Such passwords are a product of one's mind.

> The *Baust* court, however, drew a distinction between alphanumeric passwords and biometric passwords such as fingerprints. The court likened alphanumeric passwords to the combination of a safe, whereas fingerprints were akin to a key. Disclosing alphanumeric passwords requires the party to divulge mental processes, but fingerprints were mere nontestimonial physical characteristics. Relying on this distinction, the *Baust* court concluded that compelling a party to decrypt data using fingerprints did not implicate the Fifth Amendment, but compelling a party to produce a password did. Civil courts may be inclined to adopt this same distinction.

In the criminal context, **motions to compel a party to decrypt data** have met mixed results. Several courts have concluded that compelling a party to produce an alphanumeric password to decrypt data **is a testimonial communication** that would violate the party's Fifth Amendment right against self-incrimination.

But what if the producing party's response is something like, "I don't remember the decryption key?" Presumably the judge presiding over the dispute will conduct a hearing and make a credibility determination. If the judge finds the party to be incredible, what should the judge do?

Here, a criminal law analogy might be appropriate. In *Commonwealth v. Gelfgatt*, 468 Mass. 512 (2014), the Massachusetts Supreme Judicial Court held that, under the facts before it, an individual could be compelled to decrypt several computers that law enforcement had seized. On remand, the individual argued that he could not remember the keys, was found incredible, and ordered to try to provide access again or else be held in contempt and remanded to custody. (Order dated Nov. 6, 2014, Mass. Sup. Ct. Suffolk Cnty.). Drawing the analogy suggested above, a judge might hold the producing party in civil contempt and remind him that he holds the "key to the cell" in his head. Alternatively, the judge might consider a case-dispositive sanction, perhaps deeming the encrypted ESI to be "lost," or a lesser sanction such as ordering an adverse inference, imposing monetary sanctions, or ordering a party to engage a vendor.

Assuming encrypted ESI to be lost, the parties should be expected to rely on *Pegasus Aviation I v. Varig Logistica S.A.*, 26 N.Y.3d 543 (2015). Pegasus held:

> A party that seeks sanctions for spoliation of evidence must show that the party having control over the evidence possessed an obligation to preserve it at the time of its destruction, that the evidence was destroyed with a "culpable state of mind," and "that the destroyed evidence was relevant to the party's claim or defense such that the trier of fact could find that the evidence would support that claim or defense" (*Voom HD Holdings LLC v Echostar Satellite L.L.C.*, 93 AD3d 33, 45 (1st Dept 2012), quoting *Zubulake v UBS Warburg LLC*, 220 FRD 212, 220 (SD NY 2003)). Where the evidence is determined to have been intentionally or wilfully destroyed, the relevancy of the destroyed documents is presumed (see *Zubulake*, 220 FRD at 220). On the other hand, if the evidence is determined to have been negligently destroyed, the party seeking spoliation sanctions must establish that the destroyed documents were relevant to the party's claim or defense (see id.).

Consistent with *Pegasus*, the parties should be expected to contest the state of mind of the responding party and the relevance of the encrypted ESI. The court would then make findings of fact and, depending on a number of considerations, exercise its discretion and impose an appropriate sanction.

This article is an introduction to encryption in civil proceedings. There are other topics that could be addressed, including whether a third-party provider might be asked or compelled to break into an encrypted device. But that and other topics are for another day!

RONALD J. HEDGES *is senior counsel at Dentons in New York.* KRISTEN B. WEIL *is a senior managing associate at the firm.*

Techniques

« *Continued from page 9*

Organizational resources devoted to the mitigation of cyber exposure often focus on external threats including state actors and organized crime. However, insider threats may pose a disproportionate risk to an organization, because those insiders, including employees and contractors, are in a position of trust with access to and an understanding of where key company information resides. At the same time, this threat is extremely difficult to combat because the principal tool used is the access itself, granted by the organization for authorized business activities. Curtailing that access can impact productivity and business operations, while misuse of that access can be masked as legitimate activity.

Investigating Insider Threats

When a company is confronted with the suspected theft of IP (hard or soft) by an insider, the first course of action is to identify the key actor(s), isolate the relevant data sources and determine what data may have been compromised. Unfortunately, this is often easier said than done. The evidence necessary to determine what, if anything, the suspected insider had done rests in emails, calendars, text messages, and other forms of electronic communication across a vast array of systems. The data that he or she had access to is often equally dispersed. Despite a company's best efforts, we have often encountered organizations whose IP resides not only in controlled data stores, but in unauthorized shared drives, emails, laptops, and on mobile devices. Critically, it is often comingled with other information in a difficult-to-search format.

While not the traditional use of e-discovery tools, these mechanisms, combined with computer forensic activities typically associated with cyber breach investigations, can be exceedingly useful for quickly determining the extent, if any, of a loss of IP. Document review systems are, at their heart, about managing a substantial amount of unstructured data and finding relevant evidence within that mass of information. They are adept at taking substantial amounts of data from multiple sources and making it searchable. More importantly, they can perform data analysis, helping to visually depict who was communicating with whom, in what frequency and with regard to which topics. This information can be used to identify individuals for interview, validate the scope of email and calendar review, and potentially open or close avenues of investigation. In addition, traditional e-discovery search and review tools can ease the breach notification process through their built-in abilities to search potentially leaked information for Personally Identifiable Information (PII) and Personal Health Information (PHI).

By employing these tools, it has been discovered that an employer's suspicions about a particular employee were founded, but not for the reasons originally thought. For instance, by imaging and ingesting data stores and employee computers into e-discovery tools, we have on more than one occasion discovered that the IP that the employer thought the insider had developed and, therefore, had access to was, in fact, immature or completely undeveloped. By collecting and—using standard document review platforms—reviewing masses of email communications between suspected employees, we have also been able to isolate communications of interest, identify participants to conversations, and have on occasion discovered that the suspected malfeasance did not occur; but other fraudulent acts had. Given the amount of information involved, the tasks would not have been possible in the tight timeframe required by an insider investigation without the assistance of these tools—designed not for investigation, but litigation.

Conclusion

Attorneys often consider their e-discovery needs in the midst of litigation. However, the same tools that help frame your case, meet your discovery obligations and prepare for hearings, depositions and trials can pay dividends when investigating internal fraud, corruption and IP theft. You should not leave these tools on the shelf simply because litigation has not been filed. By employing them in the midst of your investigations, you may discover that a suspicion was misplaced, or that your client was right to be worried—just for the wrong reason.

1. 2016 PwC Global State of Information Security Survey, available at https://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html.
2. Id. at 24-30, appendix, Financial Services Industry Data.