JS|HELD

PERSPECTIVES

Utilizing Digital Forensics Expertise in Intellectual Property, Copyright & Trade Secret Matters

Our perspectives feature the viewpoints of our subject matter experts on current topics and emerging trends.

INTRODUCTION

Intellectual property and trade secrets in the modern era are predominantly stored as electronic records, or electronically stored information (ESI), which in turn increases the potential for misappropriation, exfiltration, or theft of these sensitive documents to unauthorized parties or entities outside the company domain. Historically, these electronic records have been saved to hard drives, file servers, emails, and external media such as thumb drives.

As emerging tech continues to become more prominent, however, we've observed claims of IP / trade secrets content theft within a broader range of repositories and media, such as cloud-based and / or chat collaboration platforms, various forms of source code and AI-based systems, and 'virtual reality' domains. There also has been a recent uptick in GenAI-related copyright infringement claims, alleging unlawful copying of content to train AI models.

In particular, the increased prevalence of cloud-based data sources for communications and storage offers users with additional opportunity for data proliferation and flight. Ironically, while the format of these electronic records may increase the ease with which the sensitive data may be transferred, it also heightens the potential for leaving an electronic trail—artifacts and traces of attempts to exfiltrate and transfer documents outside an organization's domain. For these reasons, among others, a digital forensics expert can be an invaluable ally in matters involving allegations of data exfiltration and / or misappropriation.

When such allegations present themselves, a trusted digital forensics expert can offer critical support and guidance throughout the course of an investigation, from the initial scoping and discovery phases – which may occur pre-litigation during an internal investigation – to the production of key findings, and when necessary, expert testimony.

This article focuses on key considerations for attorneys and primary stakeholders within an organization requiring digital forensics expertise from the early stages of determining the extent of a digital forensic expert's involvement to the different phases of IP and trade secret investigations.

NEED ASSESSMENT, VETTING, AND IDENTIFICATION OF A RELIABLE EXPERT IN THE DIGITAL FORENSICS PROCESS

Whether your organization is looking for advisory and expert support for an internal investigation into allegations of exfiltration, or outside counsel is preparing a client for pending litigation, specific needs may vary.

Digital forensics services for these types of matters can be broad-ranging; from overtly technical (e.g. deep-dive recovery of fragmentary deleted data, intensive review of source code for indications of replication, or exporting mailbox data from a journaled email server archive), to more advisory in nature. This would include working with counsel and / or key stakeholders to help develop ESI protocols, legal hold provisions, or other forms of strategic advice.

Law firms and in-house stakeholders need to assess their specific requirements and look for that level of expertise when aiming to retain a forensics consultant. Trusted experts retained through referrals by other law firms or organizations should consider a vetting process that includes a review of credentials, including prior experience specific to IP and trade secret theft investigations, as well as related expert testimony.

The following sections delve more deeply into certain would-be scenarios that may aid in determining the extent of a forensic consultant's involvement.

PRELIMINARY ASSESSMENT, SCOPING, DATA PRESERVATION, AND COLLECTION

In matters involving allegations of misappropriation or exfiltration of sensitive documents such as copyrighted material, trade secrets or other IP, there may be an initial internal investigation conducted by in-house counsel (though outside counsel may also be involved in these early stages) with support from other key stakeholders (HR, chief technology officer, etc.).

Depending on the extent of in-house experience in conducting such investigations, it can be beneficial to retain a forensics consultant during these early stages to determine the viability of the allegations made and offer guidance on exploring the possibility that data flight may have occurred. These initial steps may lead to a more formal scoping exercise, where key individuals and date ranges of interest are fleshed out, along with a better understanding of the information technology (IT) infrastructure in place within the organization. This is often accomplished through brief scoping calls with key stakeholders or questionnaires, though in certain contentious scenarios, scoping information may be limited, and the forensic expert may need to proceed with readily available information.

During this phase, those tasked with the initial investigation can gather information on any existing litigation holds or preservation notices in place or otherwise discuss implementation of new preservation holds and suspension of normal deletion or retention policies once litigation or a formal inquiry is anticipated.

A forensic consultant can help assess current policies to develop a sound preservation plan or work with in-house stakeholders or outside counsel (or both) in recommending adjustments that may be prudent. This is often a critical step, as failure to properly assess and revise existing policies may lead to spoliation and subsequent sanctions.

This is exemplified in a recent matter in which the failure to identify and disable an auto-delete setting on the company's email server led to a company-wide destruction of emails and resulted in significant sanctions related to the discovery process.[1]

In another case, a defendant deleted documents from his laptop after receiving numerous preservation demands, as well as after the court explicitly ordered the preservation of all data on the defendant's electronic devices. This case[2] resulted in a default judgment as a sanction.

As illustrated by these examples, sound preservation of ESI is crucial in trade secret cases, as it often revolves around whether or not sensitive documents were accessed or transferred outside an organization's domain. For that reason, it is vital to preserve key metadata attributes such as date and author name.

In addition to proactive preservation of electronic records, scoping and matter circumstances may require that additional data collections be performed. Particularly when in support of litigation, data collection must be a defensible process that maintains the integrity of the source data. Source data must be preserved without alteration, verified as an exact bit-by-bit duplicate. The resultant preserved capture can later be vetted by an opposing expert and / or law firm. Collection steps include setting up proper chain-of-custody and related documentation of the data sources with the anticipation that the procedures employed, and related documentation, will likely require presentation in court.

There are several ways ESI can be collected, each with its own risk profile. In certain instances, an organization may opt to have in-house IT, or perhaps even the custodians of interest, self-collect electronic records for the purpose of litigation. This may be a viable option depending on in-house IT's prior experience performing such collections. Even when an organization employs IT with requisite experience and credentials for performing data captures, it may prefer to avoid the liability of an in-house employee potentially testifying in court.

[1] *WeRide Corp. v. Kun Huang* (N.D. Cal. 2020).
[2] Roadrunner Transp. Servs., Inc. v. Tarwater (C.D. Cal. 2014).

To offset this concern, in certain instances the parties involved may opt to perform self-collection but with oversight or guidance or both from a forensic expert on the collection steps to be performed by IT and also to corroborate the steps taken. This approach offers the benefit of placing the responsibility of formal court reporting and testimony on the expert.

The forensic expert may also be retained to perform all of the services required for the litigation, including data preservation, analysis, reporting, and related consulting or advisory services. This may be preferred for high-profile matters or matters anticipated to be contentious.

The above considerations should be weighed against the specifics of a given matter to determine the best course of action to minimize the potential for sanctions and increase the odds of a satisfactory outcome.

FORENSIC ANALYSIS, TESTIMONY, AND REMEDIATION

Once data sources, such as mobile devices, computers, cloud-based repositories, etc., are preserved and collected in a defensible manner, the forensic analysis phase is critical to both identifying indications of exfiltration or misappropriation, as well as fleshing out the viability (or identification) of spoliation claims.

In matters involving allegations of data theft, a trained expert can analyze electronic records to uncover evidence of mass deletion of documents, usage of data-wiping software, transfer of data to external USB devices, cloud-based repositories, or personal webmail accounts, or remote access to company documents, among other artifacts that may be deemed to be of evidentiary value, all of which can assist counsel in bolstering a case for data exfiltration and spoliation claims. During this phase, as in nearly all phases of these types of matters, open discussion of preliminary findings and how these findings affect the next steps or case strategy are often key differentiators in the outcome. A seasoned forensic expert can provide timely and detailed findings, discuss the potential ramifications and evidentiary value of the findings with counsel and stakeholders, collaboratively develop recommended next steps, and prepare expert reports, declarations, and affidavits that may later lead to in-court testimony.

Depending on the scale of the need or other strategic factors, workflows during the analysis phase may also include utilization of eDiscovery or data governance review platforms, which may be implemented on-premise as part of “in-place” indexing and searching protocols, or otherwise via externally hosted review platforms. This is particularly helpful when search terms are incorporated into the analysis in scenarios where, for example, there are details available about the document names, parties involved, electronic communications among parties of interest, or other notable information associated with the alleged misappropriation of data – or otherwise as such information is discovered during forensics analysis. In such scenarios, search term responsive content is reviewed within an eDiscovery review platform, typically by the attorneys, to determine responsiveness, exclude false-positive hits, and / or ascertain merits of the claims among other benefits. The results of this review will generally inform the subsequent legal strategy and / or agreements between the parties involved.

After analysis and / or review of documents is completed, and depending on the findings, there may be a remediation phase, whereby parties agree that documents wrongly or erroneously exfiltrated from one organization to another can be identified and defensibly disposed of or quarantined. Remediation measures may also benefit from the use of on-premise or other indexing tools, including custom scripts to help identify documents of potential interest. These tools help identify and remediate (e.g., defensibly purge or quarantine) the documents of interest, which typically culminates in a report summarizing steps performed by the forensic expert overseeing the remediation. As with the other procedures discussed, companies should conduct a proper vetting of qualifications and prior experience when considering a forensic expert for such remediation.

Additionally, depending on the outcome of the digital forensics investigation, damages and valuation experts may be retained later to assess the value of the misappropriated / exfiltrated information. They can aid

in establishing a foundation of liability and quantifying the financial impact, including lost profits, unjust enrichment, or market harm.

The factors involved in determining the type of expertise required, and at what point, can vary depending on the case's specifics. For instance, if the misappropriation is already blatant, the focus shifts quickly to valuing the harm. But generally, digital forensics services are typically engaged in the first instance to establish the extent of harm(s) caused.

CONCLUSION

These considerations are by no means exhaustive but can help to guide an organization in determining the need for the services of a digital forensics expert to obtain the best possible outcome of a case. Data exfiltration, misappropriation, and related allegations are serious matters that require experts who can provide technical and advisory support to both internal investigations and pending litigation. Such experts can help in the early stages of such matters, including understanding existing litigation holds or preservation notices, thereby avoiding sanctions. They also can aid in the collection and preservation of data as well as help determine the evidentiary value of findings with counsel and stakeholders. Digital forensic experts can help develop recommended next steps, prepare expert reports and affidavits that may later lead to in-court testimony and also provide information that helps determine damages and remediation.

As technology continues to evolve with data being stored in new and innovative formats, the services of a digital forensic expert increasingly have become a necessity for any organization seeking to protect their intellectual property and trade secrets.

Acknowledgments

We would like to thank our colleagues, Antonio Rega and David Kennedy, for their insights and expertise that greatly assisted this research.

Antonio Rega is a Managing Director who leads the emerging technology and data governance service areas under Digital Investigations & Discovery, within J.S. Held's Global Investigations practice. He has more than 20 years of experience providing consulting, advisory, and subject matter expertise in the areas of digital forensics, incident response, data privacy, governance, and discovery on behalf of global corporations and law firms. Based in New York, Antonio regularly assists clients with advice and strategy through all phases of a given client need, including regulatory compliance, responses to government subpoenas, and expert testimony, when required.

Antonio can be reached at antonio.rega@jsheld.com or + 1 551 345 8502.

David Kennedy is a Senior Managing Director and Certified Public Accountant in Ocean Tomo, a part of J.S. Held. David is an expert in intellectual property valuation and negotiating the economics of patent sales and licensing agreements. Acknowledged as one of the World's Leading IP Strategists by Intellectual Asset Management (IAM) for more than a decade, he has bought and sold patent portfolios, negotiated license agreements in commercial transactions, and helped clients establish royalty rates for individual patents and large portfolios of implementation and standard essential patents. He also has testified as a patent licensing and reasonable royalty expert in ICC International Arbitration proceedings and federal courts.

David can be reached at David.kennedy@jsheld.com or +1 430 207 7051.