

**Litigation** E-Discovery Bulletin

January 2023

# ESI in Trade Secret and Restrictive Covenant Litigation Involving Former Employees

An organization facing pending or anticipated trade secret or restrictive covenant litigation against a former employee must properly manage various e-discovery issues, including where to locate and how to preserve relevant electronically stored information (ESI).

## Table of Contents

### Potential Claims and Relevant Evidence

---

### Preservation Obligations and Common Risks of Loss

---

### Inspecting Another Party's Devices and Use of Third-Party Intermediaries

---

### Remediation

---

### Cost Control

---

### Reducing the Risk of Trade Secret Misappropriation

## Contributor

---

**Joshua M. Hummel** ✓

Counsel at Redgrave LLP

An organization faces substantial and time-sensitive business risks when it discovers either that:

- A recently departed employee shared the organization's trade secrets or other sensitive materials with a competitor.
- A current employee is secretly taking steps to:

- create their own competing business; or
- misappropriate the organization's proprietary information for another purpose.

When investigating these activities or pursuing related litigation, an organization often needs to quickly identify, preserve, and, if necessary, collect important electronic evidence. If not addressed in a timely manner, e-discovery issues may:

- Impact the organization's ability to fully determine the extent of the employee's actions or prevent any further misappropriation of the organization's electronic assets.
- Unduly complicate the employer's assertion of claims against the former or current employee (and, when applicable, third parties).

This article examines the types and sources of ESI and other evidence that is often important in investigations or litigation involving former employees who misappropriated an organization's trade secrets or other sensitive information, the relevant considerations for preserving, searching, and remediating those sources of information, key practical issues related to navigating personal privacy objections from the former employee or other concerns raised by third parties, and how to establish effective data loss prevention practices to help safeguard trade secrets.

## Potential Claims and Relevant Evidence

Employees who leave their employer and take proprietary information to a competitor may subject themselves (and possibly their new employer) to potential claims for:

- Theft or misappropriation of trade secrets.
- Conversion.
- Breach of fiduciary duty.
- Breach of an employment agreement (including provisions regarding confidentiality and non-competition) (see, for example, *CaramelCrisp LLC v. Putnam*, 2022 WL 1228191, at \*1-2 (N.D. Ill. Apr. 26, 2022)).

If other employees leave with the former employee, the employer may also have viable claims for:

- Violation of a restrictive covenant for the non-solicitation of employees.
- Tortious interference with contract.
- Employee piracy.
- Corporate raiding.
- Unfair competition.

## Types of Potentially Relevant Evidence

In restrictive covenant or trade secret litigation involving a former employee, the employee's electronic devices are often a treasure trove of relevant information. In addition to showing what proprietary information the employee misappropriated, relevant ESI may also reveal how and to where the employee copied or transferred the information, communications about the employee's activities, or how the employee may have attempted to conceal the improper conduct. While it is impossible to provide an exhaustive list for every case, the types of relevant evidence to search for in these types of cases may include:

- Documents (for example, Microsoft Word or PDF documents, spreadsheets, presentations, or other office documents), which may exist in the exact form copied from the former employer or in an altered state. In many situations, metadata from these documents may also reveal the original author or date of creation or last modification.
- Email communications.
- Text messages (that is, short message service (SMS) or multimedia message service (MMS)).
- Instant messages from workplace collaboration tools or other messaging platforms or applications (for example, iMessage, Slack, and WhatsApp) (see *Red Wolf Energy Trading, LLC v. Bia Cap. Mgmt., LLC*, 2022 WL 4112081, at \*25-27 (D. Mass. Sept. 8, 2022) (awarding sanctions for failure to produce highly relevant Slack messages related to trade secret misappropriation and alteration of algorithm evidence)).

- Ephemeral messages (for example, Snapchat, Signal, and Telegram) (for more information, see *Ephemeral Messaging: Balancing the Benefits and Risks* and *Ephemeral Messaging: Best Practices for Complying with Discovery Obligations* on Practical Law).
- Call logs and voicemails.
- Electronic calendars, contacts, tasks, notes, and memos.
- Photographs and videos.
- Human resources or personnel files, employment applications or agreements, and company policies.
- Structured data from company databases (such as customer relationship management (CRM) systems or other systems housing company trade secrets), which may include the trade secrets themselves, a user's profile, or the user's activities (audit trail) within the system.
- Global positioning system locations and activity.
- Internet protocol (IP) addresses and login information, which can help identify devices the employee used.
- Evidence of recent activities on the device, such as:
  - copying, printing, accessing, or transferring certain documents or files;
  - logging in to a cloud-based email account or file-sharing system;
  - obtaining access to physical sites or document storage locations;
  - internet activity, such as browser logs or Google search histories, that may reveal what the user was viewing or searching; and
  - efforts to conceal the user's activities, such as deleting documents, clearing the internet browsing history or cache, performing a major system update, installing other software, or restoring or "wiping" a device (see *Int'l Fin. Co. v. Jabali-Jeter*, 2019 WL 2268961, at \*18-20 (E.D. Pa. May 28, 2019); *Sys. Spray-Cooled, Inc. v. FCH Tech, LLC*, 2017 WL 10154221, at \*6 (W.D. Ark. Feb. 22, 2017); *Organik Kimya, San. ve Tic. A.S. v. Int'l Trade Comm'n*, 848 F.3d 994, 997, 999, 1003-04 (Fed. Cir. 2017)).

## Common Sources of Potentially Relevant Evidence

An organization may store relevant evidence across many devices and other data sources, including:

- Email accounts.
- Computers (laptops or desktops).
- Servers.
- Cell phones and tablets, possibly including backups of cell phone data stored on iTunes or iCloud (see *Prudential Def. Sols., Inc. v. Graham*, 2021 WL 4810498, at \*7 (E.D. Mich. Oct. 15, 2021)).
- Removable media (such as hard drives, USB or flash drives, CDs, and DVDs).
- Collaboration or instant messaging platforms (such as Slack, Microsoft Teams, and Google Hangouts Chat).
- Ephemeral messaging platforms (such as Snapchat, Signal, and Telegram).
- Document management systems or cloud-based document storage accounts (such as Dropbox, Box, Google Drive, OneDrive, and SharePoint). In addition to the documents themselves, these systems may also include audit trails or account histories that track logins, views, printing, downloading, file transfers, or file sharing, which may also be relevant.
- Social media accounts. This may include:
  - public posts;
  - an individual's contacts and connections;
  - private messages;
  - the dates of any updates made to the profile or account;
  - photographs or videos;
  - devices or IP addresses used to access the account; and
  - other relevant account history.
- Printer spool logs on computers, which may show which documents were last printed and when.
- Paper documents or physical items.

- CRM systems or other databases used to store or export customer and client information or other trade secrets.

Some sources may be owned by (or in the possession, custody, or control of) the organization, while others may be owned or controlled personally by the former employee or a third party.

For each relevant individual in a case, counsel should seek to:

- Identify all devices and data sources used.
- Determine which individual (or what entity) owns or is in possession of each device or data source (for more information, see Possession, Custody, and Control of ESI in Federal Civil Litigation on Practical Law).

While certain kinds of evidence may not be readily accessible to or detectable by a layperson, forensic specialists can often find evidence of a user's activities by using forensic tools.

Specialized tools often work best when working with an original device or a complete forensic image, instead of a backup or copy of the user-created content (such as a My Documents folder).

## Preservation Obligations and Common Risks of Loss

Parties generally must take reasonable and proportional steps to preserve relevant information once they are aware of pending or reasonably anticipated litigation (see, for example, *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 217-18 (S.D.N.Y. 2003); The Sedona Conference, Commentary on Legal Holds, Second Edition: The Trigger & The Process, 20 Sedona Conf. J. 341, 351 (2019)).

The duty to preserve arises "when that party has notice that the evidence is relevant to litigation or should have known that the evidence may be relevant to future litigation" (*Prudential Def. Sols.*, 2021 WL 4810498, at \*5-6 (quoting *John B. v. Goetz*, 531 F.3d 448, 459 (6th Cir. 2008) and holding that a duty was triggered based on the defendants' emails contemplating legal action and noting that some text messages were saved "in case they needed to be used as evidence"); see also *Sonrai Sys., LLC v. Romano*, 2021 WL 1418405, at \*10 (N.D. Ill. Jan. 20, 2021) (stating that "a demand letter threatening litigation may trigger the

duty to preserve documents within its scope"); *Int'l Fin. Co.*, 2019 WL 2268961, at \*15 (holding that a duty arose when the defendant sent demand letters claiming that an information technology (IT) investigation was a pretext for pregnancy discrimination); *Steves & Sons, Inc. v. JELD-WEN, Inc.*, 327 F.R.D. 96, 106 (E.D. Va. 2018)).

(For more on the duty to preserve, including in the employment litigation context, see **Duty to Preserve Evidence (Federal)** and **E-Discovery in Employment Cases: Practical Considerations for Employers** on Practical Law; for a collection of resources to assist counsel in preserving ESI when anticipating litigation or an investigation, see **Preserving Documents and Electronically Stored Information Toolkit** on Practical Law.)

## Scope of Preservation

An organization need not preserve every piece of paper, email, or electronic document in its possession, nor must it preserve duplicative copies of the same ESI. Instead, an organization generally must only preserve key players' unique evidence that may be relevant to the pending or anticipated dispute. (*CAE Integrated, LLC v. Novak*, 2021 WL 3008296, at \*6 (W.D. Tex. June 7, 2021); *In re Ethicon, Inc. Pelvic Repair Sys. Prod. Liab. Litig.*, 299 F.R.D. 502, 517 (S.D.W.V. 2014) (citing *Zubulake*, 220 F.R.D. at 217); The Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production, 19 Sedona Conf. J. 1 (2018) (Sedona Principles), Principle 5, at 93-96.)

Regarding the electronic devices used by a former employee, it is sometimes difficult to determine which party must preserve certain ESI because it is unclear which party is actually in possession, custody, or control of the evidence.

Complicating this determination, various jurisdictions define possession, custody, and control differently. For example, courts may:

- Apply a legal right standard, which examines whether a party has a legal right to obtain the ESI.
- Apply a legal right plus notification standard, which examines whether a party has a legal right to obtain the ESI, and if it does not but is aware that the evidence is in the

hands of a third party, requires the party to notify the adversary.

- Consider whether there is a practical ability to obtain the evidence.

(See The Sedona Conference, Commentary on Rule 34 and Rule 45 “Possession, Custody, or Control,” 17 Sedona Conf. J. 467, 483 (2016); for more information, see **Possession, Custody, and Control of ESI in Federal Civil Litigation** on Practical Law.)

Therefore, the ability to preserve or collect the information may depend on:

- How and where the company stores the devices, documents, or ESI at issue.
- The terms of any contracts or company policies addressing the ownership of those assets.

This further illustrates the need to begin investigating quickly.

## Common Risks of Loss

An unreasonable delay in preserving ESI may result in the loss of relevant information in a matter, and the risk is heightened in matters involving trade secrets. In addition to potential spoliation concerns, because electronically stored trade secret information can be transferred with ease to other individuals, devices, email accounts, backup media, and cloud storage areas, it may be difficult (if not impossible) to track down and remediate all copies that may exist.

While it is not possible to list all the ways information can be lost, the following risks to ESI are common in these types of cases:

- When former employees are accused of wrongdoing, they may panic and begin deleting documents or even reformat or wipe their devices (see, for example, *Sonrai Sys.*, 2021 WL 1418405, at \*12-13). These actions, whether malicious or not, may permanently alter the documents and their metadata.
- Even when innocently compiling information, an individual may move or reorganize files, print documents, change file names, or slightly alter a document’s content. These actions or even simple attempts to copy or save over the original document, may alter the



document and its metadata or make the original versions unavailable. (See, for example, *Healthplan Servs., Inc. v. Dixit*, 2020 WL 12048884, at \*15 (M.D. Fla. July 29, 2020); *OmniGen Research v. Wang*, 321 F.R.D. 367, 375-76 (D. Or. 2017).)

- The act of turning a computer on and off (particularly many times over a period of weeks or months) can flush out the older history of a user's activities, such as data contained in temporary storage areas of a device. Depending on the condition of the computer, turning the computer on and off may also cause the hard drive to crash, making data recovery difficult or impossible.
- Many organizations have retention policies calling for the permanent deletion of emails, documents, or other information after a period of time. It can be important to determine whether those policies exist, if and how they can be suspended or modified, and whether a collection is necessary to ensure that no important information is lost while the investigation or litigation is pending.
- Devices can be lost, stolen, damaged, discarded, repurposed, or simply more difficult to identify or track down over time.

## Ways to Mitigate the Risk of ESI Loss

It is important to ensure that the devices used by the former employee and other relevant witnesses are handled carefully. When it is determined that the devices contain relevant information, reasonable and prompt actions to preserve that content may include:

- Talking with the organization's IT personnel to:
  - identify the devices and sources of relevant information to which the former employee had access; and
  - ensure that reasonable steps are taken to preserve relevant data located on the devices or sources.
- Identifying any other individuals who may become witnesses and investigating what devices and relevant ESI they have.

- After ensuring that disabling a user's access does not also delete their account or alter other relevant information, disabling the departing employee's access (and others' access as needed) to the organization's data to prevent them from logging in.
- If necessary and appropriate, requesting in writing that the former employee return any company-owned devices remaining in their possession (ideally, this would have occurred when the former employee left the company).
- Avoiding repeatedly powering any physical device on and off to prevent further access or modification of relevant information until the device is imaged.
- Sending litigation hold notices or preservation notices to individuals or entities in possession, custody, or control of relevant information, such as:
  - individuals within the organization (for a model litigation hold notice from an organization's in-house counsel to employees, with explanatory notes and drafting tips, see *Litigation Hold Notice on Practical Law*);
  - cloud service providers that maintain some or all of the organization's relevant ESI (for a model document preservation letter for a cloud service provider, with explanatory notes and drafting tips, see *Document Preservation Letter for a Cloud Service Provider on Practical Law*);
  - neutral third parties maintaining relevant information (for a model document preservation letter for a nonparty, with explanatory notes and drafting tips, see *Document Preservation Letter for a Nonparty on Practical Law*); and
  - other parties to the litigation, including the former employee (see *QueTel Corp. v. Abbas*, 2017 WL 11380134, at \*5 (E.D. Va. Oct. 27, 2017) (stating that a detailed, specific, and clear preservation letter established notice of potential litigation and the employee's duty to preserve); *Konica Minolta Bus. Sols., U.S.A. Inc. v. Lowery Corp.*, 2016 WL 4537847, at \*4 (E.D. Mich. Aug. 31, 2016) (same); for a model document preservation letter for an opposing party or a co-party, with explanatory notes and drafting tips, see *Document Preservation Letter for an Opposing or Co-Party on Practical Law*).

- Identifying and suspending (or modifying), as appropriate, any organizational policies or practices that may impact relevant devices or ESI, including:
  - retention policies calling for the automatic deletion of relevant emails or other documents after a period of time; and
  - policies that the organization's IT department may have in place, such as deleting a former employee's email account or wiping and repurposing their devices at a set time (such as within 30 to 90 days after their departure), or overwriting backups.
- Determining whether the organization has any policies in place concerning ownership of and access to any electronic devices used for work and the data on those devices.
- Obtaining and memorializing any user passwords, login credentials, and encryption keys necessary to open and decrypt the relevant devices.
- Assessing whether a forensic e-discovery vendor may be needed to:
  - image or otherwise preserve relevant information on the devices;
  - perform a forensic examination of the devices; or
  - conduct other searches for relevant information.
- When a device must be forensically analyzed, ensuring that untrained individuals do not analyze the device in a manner that alters relevant data (see *CaramelCrisp*, 2022 WL 1228191, at \*7-8).
- Creating and maintaining a chain of custody form related to any devices or data sources containing relevant information (for a model chain of custody template, with explanatory notes, see Data Collection: Chain of Custody for Digital Media on Practical Law). If preserving a physical device (in addition to or instead of copying files or imaging the device's contents):
  - ensure that the device is clearly labeled or otherwise identified as subject to a litigation hold; and
  - store the device in a safe location to prevent it from being lost, damaged, stolen, wiped, recycled, or repurposed.

- Preserving and collecting relevant ESI. This may include imaging the most critical devices, collecting the most critical ESI promptly, and applying the proportionality factors to determine an appropriate preservation strategy for the remaining sources of relevant ESI (see FRCP 26(b)(1); for more information, see Preserving Documents and Electronically Stored Information Toolkit and Collecting Documents and Electronically Stored Information in Federal Civil Litigation on Practical Law).
- Documenting efforts made to identify, preserve, and collect the relevant information, including:
  - questions asked and facts learned about the relevant information;
  - the availability and location of relevant information;
  - the representations made by the custodians and other individuals with knowledge of where and how relevant information resides; and
  - decisions made not to collect or preserve certain data sources and the reasons why those decisions are reasonable or proportional.

An organization often does not know or even suspect foul play until it begins analyzing the former employee's computer, email account, or other data sources, possibly under the organization's departure policy or standard IT operating procedures. Additionally, a duty to preserve the evidence does not arise (if at all) until there is a reasonable anticipation of litigation. Therefore, it may be unduly burdensome and expensive and not proportional to the needs of the matter to image all of the former employee's devices before the initial review of the data sources begins.

An organization may instead wish to start its initial investigation by reviewing data sources that are unlikely to be altered during the review, such as email accounts, network storage locations, or other systems that are fully backed up. If the cursory investigation reveals the potential for litigation involving the former employee, it may then be helpful for the organization to image or otherwise collect relevant information from devices that may present preservation risks (such as computers, flash drives, and cell phones) before further searching those devices.

Given that the scope of discovery may change throughout the litigation or new facts may be learned that may impact the relevance or availability of materials in the organization's possession, custody, or control, it can be prudent for parties to periodically:

- Revisit and adjust their preservation efforts (including the scope of the litigation hold) as appropriate.
- Follow up with custodians and others in possession or control of relevant information to remind them of their litigation hold obligations and ensure that they are continuing to preserve relevant information.

## **Inspecting Another Party's Devices and Use of Third-Party Intermediaries**

Disputes frequently arise when an employer demands direct access to devices and data sources that the former employee (or another third party) personally owns (for example, where the organization had a Bring Your Own Device (BYOD) program). In these situations, employees may:

- Store sensitive company trade secret information in one folder on a personally owned computer or flash drive and personal content such as photographs, financial information, private health information, or passwords in one or more other folders.
- Use a personal cell phone to text or send trade secret information to the new employer and also text with family or friends about unrelated personal matters.

In addition to irrelevant personal content, direct access to another party's computer systems or devices may reveal confidential attorney-client communications or work product or their new employer's trade secrets and confidential information. Gaining access to another party's devices or network may also unreasonably disrupt the former employee's ongoing work or business, endanger the stability and security of their new employer's systems, or expose private or confidential information belonging to other individuals or third parties.

As a result, courts are typically reluctant to provide a party with access to another's devices or network. However, courts sometimes make exceptions, such as on a showing of:

- Substantial need or a material failure of the responding party to meet their discovery obligations (see Sedona Principles, at Comment 6.d; see also *Henry Schein, Inc. v. Cook*, 191 F. Supp. 3d 1072, 1078-79 (N.D. Cal. 2016)).
- Good cause and the entry of a protective order to guard against any release of proprietary, confidential, or personally identifiable information (see Sedona Principles, at Comment 10.e).

Frequently, related court orders appoint a neutral forensic examiner and establish a protocol for the inspection of the devices and ESI (see *Intel Corp. v. Rivers*, 2019 WL 7212314, at \*2-4 (E.D. Cal. Feb. 19, 2019); *Genworth Fin. Wealth Mgmt., Inc. v. McMullan*, 267 F.R.D. 443, 449 (D. Conn. 2010)). Benefits of using a neutral forensic examiner to assist with collecting, imaging, and analyzing the devices at issue may include the ability to:

- Prevent spoliation or later transfers or use of the former employer's information by removing the relevant devices and data from the former employee's possession.
- Secure the examiner's analysis and report on the user's activity (or lack of activity) and assistance with searching for and locating relevant documents and information on the devices.
- Work with the examiner or their colleagues to load any disputed documents into a document review platform where the parties and their counsel can establish a protocol to search for and identify relevant documents and address any concerns regarding privilege, confidentiality, ownership rights, and potential steps for remediation related to any particular documents.
- Obtain the examiner's advice on or assistance with remediating the devices at the conclusion of the project.

## Remediation

When pursuing litigation against a former employee, the organization often seeks to remediate any devices that the employee used during their employment to store proprietary or

confidential information that belongs to the former employer.

Remediating a device is often complex and difficult. Merely deleting a file from a user's desktop or My Documents folder and emptying the recycling bin does not fully delete the file but instead simply removes the file from the more accessible areas of the hard drive. Specifically, this action may only mark the space the file occupied as available memory (that is, memory that is available to be used for storing other files). Until that available memory actually is used to store another file, the original file may still be recoverable.

To truly delete a file, forensic technicians often recommend wiping the entire device using US Department of Defense standards. This approach returns the device to its out-of-the-box condition, destroying all documents, software, and other content in the process. However, one or more parties may have important content on the devices they want to keep (such as the individual's personal information or the employer's proprietary documents) and, if litigation is ongoing, the parties may need to retain certain documents or information for litigation hold purposes.

It is important to factor in all of these competing issues and develop a plan before remediating any electronic devices. A remediation plan often requires:

- The initial imaging and preservation of relevant devices.
- A transparent process to review and identify both parties' information and resolve ownership issues.
- An agreement on the appropriate disposition of the devices and data at issue.
- The ultimate destruction of the forensic copies.

Until a remediation plan is in place, the party in possession of the devices or data should be advised not to:

- Make copies of documents.
- Move documents to another location (even on the same computer or device).
- Rename or change any of the files.

Any of these activities can alter the documents' metadata and make it difficult to locate or match up those files later.

## Cost Control

E-discovery costs can easily reach into the tens or hundreds of thousands of dollars, especially when using one or more vendors to assist with the forensic examination and search for relevant information, provide document hosting and production services, and perform remediation. An organization is often best able to obtain good results and control costs if it is the first party to select and engage the vendor. An organization may also address cost shifting in a third-party forensic examination protocol (see *Genworth*, 267 F.R.D. at 448).

To save costs, an organization can:

- Confirm that the e-discovery vendor is qualified and properly equipped to handle all phases of the project for which they are engaged.
- Act early and perform a diligent investigation into the relevant devices and data sources, while factoring in the proportionality considerations to exclude devices and data sources not reasonably likely to contain unique, relevant information (FRCP 26(b)(1); for more on proportionality in employment litigation, see *E-Discovery in Employment Cases: Practical Considerations for Employers on Practical Law*).
- Ask the vendor for a cost estimate or budget for each phase of e-discovery work. If the vendor's scope of work changes during the matter, they should be able to provide an amended or supplemental budget that reflects the revised scope.
- Inquire about whether the vendor offers a departing employee package that provides discounts or specific cost-saving protocols for cases involving investigations or claims against a former employee.
- Where possible, be transparent and reasonable with the other party in developing a protocol and exploring the use of an intermediary vendor that may help both parties reach their discovery goals. The parties may potentially spend enormous amounts of



money on e-discovery, so selecting a single vendor and entering into a cost-sharing agreement may be a way for both sides to save costs.

## Reducing the Risk of Trade Secret Misappropriation

Organizations can proactively establish policies and data loss prevention practices to reduce the risk of employee misappropriation of trade secrets and other proprietary information.

Specifically, organizations can:

- Identify and classify the organization's most sensitive and valuable trade secrets and, where possible, limit access to only those who require access.
- Establish employment agreements and policies that contain clear and reasonable terms regarding confidentiality and nondisclosure of the organization's trade secrets and confidential information.
- Tailor IT security for specific trade secret assets to include audit trails, ownership, and documents.
- Establish an acceptable use policy providing:
  - the organization with a clear right of ownership and possession of all work-related devices and the information they contain; and
  - employees with notice that they should have no expectation of privacy related to company-owned devices and that the employer has the right to monitor the use of those devices.
- Establish a litigation hold policy requiring employees to turn over any devices, documents, and ESI the organization must preserve for pending or anticipated litigation.
- Adopt a mobile device policy that balances the organization's risks and needs and includes terms to satisfy its litigation hold obligations and data security interests. For example, an organization may adopt a BYOD policy allowing employees to select, pay for, and own their devices (sometimes with the employer paying for some of the related expense in a stipend or by paying for monthly cell phone service) (for a model BYOD policy, with explanatory notes and drafting tips, see *Bring Your Own Device to Work*

Policy on Practical Law). While BYOD policies may present initial cost savings, they can also create risks of confusion and complication regarding access to the devices for company information, and add costs and delays in an e-discovery and litigation hold setting.

- Use Mobile Device Management software that:
  - containerizes company-owned email accounts, document stores, and information in other applications or databases and ensures that the organization's data stays on its servers instead of on the device itself;
  - prevents users from copying information from a secured area of the network onto personal or unmonitored areas of a device; and
  - if a device is lost or stolen (or the employee leaves the organization), allows the organization to remotely wipe the device and discontinue access to the organization's network and data.
- If allowing employees to access the organization's network remotely from a home computer or other personal device, establish secure connections, encryption, passwords, authentication, and access points to containerize company data and prevent it from being exfiltrated to a non-company-owned device or other external storage areas.
- Train employees to keep their personal and work information separate, because the intermingling of personal and work data is one of the reasons why e-discovery expenses often spiral out of control (and in some instances, may be what causes litigation in the first place). For example, employers may advise employees that if a device is to be wiped and personal data cannot be easily parsed from work data without great time or expense, the employee may lose personal information that the employee prefers to keep.
- Consider adopting IT policies preventing users from copying or saving organizational information on flash drives or other removable media. If an organization allows the use of removable media, at a minimum, it should consider requiring it to be encrypted. Organizations may also take steps to only allow specific individuals to copy to or from removable media and train these individuals to document and flag potential risks.

- Adopt IT security protocols allowing the organization to monitor computers, cell phones, email accounts, and other points of access to the network to detect exfiltration of information from either external or internal sources (such as large transfers of documents and information). Some organizations use analytics and artificial intelligence to detect patterns in emails and communications that may signal when an employee is disgruntled or exhibiting other red flag behavior.
- Create a policy calling for the organization's IT department to collect departing employees' devices and inspect them for suspected violations of the organization's policies governing its trade secrets. When establishing a timeline to recycle or repurpose former employees' devices, organizations should also consider their need to preserve evidence if there is a potential claim.
- Audit all security measures and network access regularly.
- Provide regular policy training and reminders.

Technology continues to evolve in both business and personal settings. Organizations should continually reassess their policies and practices, along with the tips outlined above, as they face new, practical issues related to preserving relevant evidence in litigation and safeguarding their sensitive trade secret information.

*The author would like to thank M. Lynne Hewitt, a former senior advisor with Redgrave LLP, for her contributions to this article.*

## Related Content on Practical Law

### Trade Secrets Litigation

Access on Practical Law →

---

### Trade Secrets and Confidential Information at End of Employment Checklist

Access on Practical Law →

---

### Social Media and Restrictive Covenant Litigation

[Access on Practical Law →](#)

---

## **E-Discovery in Employment Cases: Practical Considerations for Employers**

[Access on Practical Law →](#)

---

## **Restrictive Covenants Toolkit**

[Access on Practical Law →](#)

---

## **Possession, Custody, and Control of ESI in Federal Civil Litigation**

[Access on Practical Law →](#)