ALFA International
THE GLOBAL LEGAL NETWORK

2026 International Client Seminar

March 5-7, 2026

It's A (not so) Small World of Evidence

Digital Forensics in the Connected Workplace: Role of Counsel

Sarah H. Lamar
Moderator
HUNTERMACLEAN
Savannah, Georgia
slamar@huntermaclean.com

It's A (not so) Small World of Evidence

The Interconnected Workplace

Why does it seem as though the collection and preservation of evidence with respect to legal claims continues to become increasingly complicated? Because it is! Each of us creates many digital footprints every day and the workplace is no longer just at the office. Employees work remotely from home, on the road, and in shared workspaces. Hours of work are fluid and the equipment, software, and platforms used to accomplish our jobs are constantly changing. Moreover, many workers use their own devices for business purposes, further complicating the landscape when it comes to preserving evidence.

The Universe of Possible Evidence

When a business receives notice of a legal claim, potential evidence can be found in many places:

- Social media (Facebook, Instagram, Snapchat, etc.)
- Collaboration platforms (Teams or Slack)
- Mobile devices (voicemail, texts, iMessage, WhatsApp)
- Corporate phone systems (voicemail)
- Corporate and personal computers (laptops and desktops)
- Corporate computer accounts (software systems, email, calendars)
- Personal computer accounts (email, calendars, photographs)
- Cloud services
- Security cameras
- Access systems (building entry codes, monitoring software)

Common Legal Scenarios

There are a vast number of litigation scenarios that trigger a duty to preserve evidence. Easy examples arise from the employment law context, as most business have employees, which inevitably, at some point, leads to claims. These may relate to trade secret misappropriation, violation of restrictive covenant agreements, wage and hour practices with respect to classification of workers or overtime pay, and claims of discrimination, harassment, or retaliation.

All these potential claims prompt a multitude of preservation questions. For example, in connection with a trade secret case, does the trade secret exist in electronic format? If so, on which computers, platforms, or software systems does it reside? Which employees were authorized to access the data? Did employees download any data on a thumb drive? Did employees sign a confidentiality agreement – and can it be found?

Another example might involve a claim of misclassification. In this scenario, how does the employer prove the hours worked by the employee whom the employer classified as exempt? Is there a secured entry system where the employee swipes a key fob or card? Do security cameras show the employee's entry/exit from the premises? Does the employee work remotely and does the employer monitor laptop use?

Security footage always seems to have the shortest retention period, some as brief as thirty (30) days or even seven (7) days, which makes preservation, review, and production extremely difficult. How else does the

electronic record prove when the employee worked and did not work? Emails or texts are a more challenging method of reconfiguring an employee's work history and require more detective work but can nevertheless be critical in defending a wage and hour claim. Switching third-party payroll providers can also add complexity. After a period of time, some payroll services delete certain data and only skeletal information can be obtained by the employer. (In this regard, a business should ensure continued access after the vendor relationship ends through negotiating favorable contract terms).

Finally, EEO claims present some of the knottiest electronic preservation issues, as texts, chats, and social media often play a central role in these cases. Even where the employer has a strong Bring Your Own Device ("BYOD") policy, problematic behavior often is revealed in private in texts and social media posts that were made outside of work and on the employees' own devices. This makes preservation much more challenging because the employer has little to no control over the electronically stored information ("ESI").

Role of Defense Counsel in Digital Data Collection

The defense attorney should set expectations early with their client as to the need to preserve relevant or potentially relevant information. Key elements of this process include identifying the data custodians and the categories of evidence, the document chain of custody, and sources of data, understanding the document retention policies or practices of the client, and preparing the litigation hold notice.

A key role of counsel is to advise clients *not* to delete data. To do this, counsel may need to speak with the client's IT professionals, whether in-house or outside. Depending on the size and sophistication of the client, outside counsel may need to convince the client of the importance of document preservation and when it is recommended to use an outside vendor to collect, preserve, and manage the data during the litigation process.

Some pitfalls encountered by defense counsel include:

- Letting employees self-collect from personal devices
- Relying solely on corporate backups that exclude personal devices or BYOD
- Ignoring messaging apps like Signal, Snapchat, or iMessage
- Delay in forensic imaging, which creates the risk of overwriting relevant metadata
- Failure to advise regarding the Fed. R. Civ. P. 26 requirements (sometimes supplemented by local rule additions or anomalies), especially when anticipating litigation
- Failure to follow up with reminders and when there is a change in the scope of the litigation

Role of In-House Counsel in Digital Data Collection

In-house counsel should take the lead or coordinate creation and implementation of applicable policies and procedures with other company leaders, to include document retention policies, BYOD policies, social media policies, and proper use of work/personal equipment, devices, and accounts policies.

In addition, when anticipating litigation or after notice of a claim, in-house counsel should discuss the practicalities of digital creation, collection, and management with IT and other stakeholders. Depending on the size and resources of the company and the in-house legal department, the in-house counsel may also take the lead in creating and managing the litigation hold process:

- Identify the potential custodians

  - Include former employees?
  - Include independent contractors/vendors?
- Standardize the preservation notice template
  - Identify the scope
  - Identify sources of data, such as not only company issued equipment and accounts, but also personal devices and accounts
- Work with outside counsel to weigh accessing difficult data (social media, voicemail, texts, google chats, etc.)
- Actively monitor and manage the process
  - Do you engage an outside vendor?
  - Assessment of ongoing and potential additional costs
- When the litigation ends, work with IT to release the hold and return to the standard retention policies.

Final Procedural Reminders for Counsel

Under Fed. R. Civ. P. 26 and 37, a business has a duty to preserve data when litigation is reasonably anticipated. The scope of retention may include personal devices. Implement litigation hold processes early and distribute the notice promptly.

Remember Fed. R. Civ. P 26(b)(1) and its proportionality standard. Courts increasingly require data collection to be proportional to the needs of the case, which generally is good news for defendants. Businesses must evaluate the burden versus the benefit before, for example, agreeing to broad or costly forensic imaging. In this regard, at the Fed. R. Civ. P. 26(f) conference, carefully review the ESI protocols to be implemented for both sides, including without limitation the format of production, access to metadata, and privilege issues. Consider whether clawback agreements make sense for privileged data. Remember that the failure to preserve ESI can trigger sanctions under Fed. R. Civ. P. 37. Finally, it is critical to assess additional requirements or anomalies caused by federal court local rules, which may vary jurisdictionally.

*Additional Resources**

- The Sedona Conference, *Commentary on Legal Holds, Second Edition: The Trigger & The Process,* 20 Sedona Conf. J. 341 (2019).
- *The Sedona Principles, Third Edition: Best Practices, Recommendations and Principles for Addressing Electronic Document Production,* 19 Sedona Conf. J. 1 (2018).
- Conrad Jacoby, Jim Vint and Michael Simon, *Databases Lie! Successfully Managing Structured Data, the Oft-Overlooked ESI,* 19 Richmond J. of Law and Technology, Issue 3/Article 2 (2013).
- Lindsey Blair, *Contextualizing Bring Your Own Device Policies,* 44 J. of Corporation Law 1, 151 (2018).

****

**Additional Resources suggested by Brett Creasy, President and Director of Digital Forensics, bit-x-bit (bit-x-bit.com).*