LOS ANGELES & SAN FRANCISCO

Daily Journal

www.dailyjournal.com

THURSDAY, DECEMBER 28, 2023

PERSPECTIVE

Understanding the distinct roles of E-discovery and digital forensics

By Daniel B. Garrie, Esq. and Hon. Gail A. Andler (Ret.)

Shutterstock

E-discovery and digital forensics are two distinct and nuanced concepts that are often conflated in the world of legal technology. While both fields converge in their utilization of digital data and may overlap once litigation is instituted, their applications, methodologies, and implications in legal proceedings significantly differ.

E-Discovery is by its nature employed once litigation (or arbitration, under some rules) has commenced; digital forensics implicates the pre-litigation obligation of preservation, as discussed below, and perhaps other aspects of the discipline which may come into play for pre-litigation mediation or other forms of alternative dispute resolution.

Take, for example, the hypothetical situation of a key employee ("Former Employee") leaving Business A to start a competing business, Business B. As soon as competing business enterprise Business B or Former Employee are put on notice that Business A may dispute some aspect of Former Employee's actions in leaving Business A or engaging at Business B, Digital Forensics must come into play to identify, preserve and maintain certain electronically stored information of all concerned. Early mediation efforts may take place pre-mediation with the sides, separately or together, utilizing a digital forensics expert to review hard drives or phones to determine whether information has been accessed, downloaded or deleted. In our hypothetical, it is not until either litigation or arbitration permitting discovery commences that eDiscovery may come into play, potentially overlapping with Digital Forensics activities. Following below is a more expansive discussion of each. Understanding the roles and characteristics of these two critical facets of legal practice can aid legal professionals in managing the technical aspects of legal proceedings more efficiently and avoid costly pitfalls. This article provides an overview of the defining features of e-discovery and digital forensics and how they are used in distinct ways in the legal field.

E-discovery: The process of identifying, collecting, and producing electronically stored information to comply with disclosure obligations

E-discovery, which stands for electronic discovery, is a process as ingrained in modern legal practices as discovery itself. It encompasses identifying, collecting, and producing electronically stored information (ESI) as part of a party's disclosure obligations in response to litigation, government investigations, or criminal proceedings. ESI includes digital files (such as Word docs or Excel spreadsheets), cloud-based documents (such as Google docs), emails, instant messages, social media profiles, website content, digital images, audio files, videos, and any other form of digital information.

With the increasing prevalence of ESI in the daily lives of individuals and operations of companies and organizations, it's difficult to think of a legal proceeding that does not involve e-discovery at some level. Traditional hard copy discovery might not even play a role in some cases anymore. In this way, it may make more sense in the modern

era to think of e-discovery as just discovery, assigning the othering prefix to its physical counterpart (p-discovery perhaps?).

The e-discovery process shares many characteristics with traditional p-discovery in terms of general structure. As one might expect, however, the execution of e-discovery processes differs significantly. At a high level, e-discovery encompasses the following key stages:

1. Information governance: Establishing policies and procedures for managing a company's electronic information to ensure compliance and readiness for potential litigation. For example, a corporation may implement specific guidelines on how employees store and manage emails and documents.

2. Identification: Locating potential sources of relevant ESI. This could involve identifying specific computers, servers, or mobile devices that contain data pertinent to a legal case.

3. Preservation: Safeguarding identified data to prevent alteration or loss. An instance of this would be applying a legal hold to employee email accounts to preserve all communications during the period under investigation.

4. Collection: Gathering ESI for further analysis. This might include extracting data from various sources such as laptops, servers, cloud storage, and mobile devices.

5. Processing: Converting collected data into a reviewable format. An example is processing raw data from a company server to filter out irrelevant information and organize the remaining data.

6. Reviewing: Examining the processed data for relevance and privilege. For instance, legal teams might use specialized software to review thousands of emails to identify those pertinent to the case.

7. Production: Delivering relevant ESI in an appropriate format to opposing counsel or the court. This can include creating a set of documents that are redacted for sensitive or privileged information.

As set out above, the focus of e-discovery is identifying, collecting, and producing relevant information as part of a party's disclosure obligations in a legal proceeding. Throughout these stages, maintaining the integrity and authenticity of digital evidence is paramount, often achieved through placing data under legal hold. This ensures the evidence is preserved in its original form without unauthorized alterations, deletions, or destruction.

Digital forensics: Investigation of digital sources to establish facts and uncover evidence

Digital forensics is a specialized branch of forensic science used to establish facts and uncover evidence. Digital forensics extends beyond mere data collection. It involves a comprehensive investigation of ESI, metadata, and digital artifacts to identify digital evidence that might not be apparent or accessible to the layperson. Much as a physical forensic investigator might use special tools to lift fingerprints or identify gunpowder residue, a digital forensic investigator might use special tools to identify deleted files or trace file activity to specific users. With the right tools, digital forensics can be applied to virtually any digital source, ranging from standard fare such as mobile phones and computers to things like electronic door locks, vehicle navigation systems, and smart refrigerators.

A recent and notable case demonstrating the impact digital forensics can have is *United States v. Lichtenstein*, No. 22-CR-00136 (D.D.C. filed Feb. 8, 2022), in which digital forensic experts played a crucial role in tracing and seizing over $3.6 billion worth of stolen Bitcoin. A New York City couple employed sophisticated laundering techniques to steal approximately $4.5 billion in cryptocurrency following a 2016 cyberattack on the Bitfinex exchange. Digital forensics and cryptocurrency experts meticulously tracked the laundered Bitcoin, leading to the arrest of the perpetrators.

As another example, in *United States v. Zhang*, No. 5:19-CR-00758 (N.D. Cal. 2022), an Apple engineer was found guilty of stealing trade secrets related to autonomous vehicle technology. Digital forensics tools were used to analyze the engineer's network activity and data from his Apple devices. The investigation uncovered the unauthorized download of sensitive files, strengthening the case against the engineer.

The above cases underscore the critical role of digital forensics in uncovering evidence. From recovering stolen assets and identifying cybercriminals to protecting corporate trade secrets and unearthing fraudulent schemes, digital forensics offers a powerful tool for law enforcement and legal professionals. As digital technology continues to evolve, the significance of digital forensics in legal proceedings will only increase, highlighting the need for continued advancement and expertise in this dynamic field.

Common ground and differences

E-discovery and digital forensics, while intertwined in their focus on digital data, diverge in application and scope. Both disciplines involve data gathering, processing, preservation, and analysis, as well as utilizing automated tools for efficiency. Yet, their usage in legal contexts differs. E-discovery focuses on producing digital evidence for litigation to comply with disclosure obligations. It deals with unaltered data collection for legal review. Digital forensics involves in-depth technical analysis to uncover evidence. It includes retrieving hidden or deleted information, crucial in cybercrime or intellectual property theft cases. Where e-discovery is concerned with collecting and producing evidence known to exist, digital forensics is concerned with establishing previously unknown facts.

In our digital epoch, the indispensability of e-discovery and digital forensics in the legal domain cannot be overstated. As fundamental as discovery is to our legal system and forensics is to crime scene investigation, so too are their digital counterparts. Their distinctive methodologies, standards, and technological tools are a testament to the multifaceted nature of contemporary legal challenges. Proficiency in these areas transcends mere competency – it is a fundamental necessity for navigating the intricate interplay of law and technology.

Daniel B. Garrie, Esq. *is the founder of Law & Forensics and* **Hon. Gail A. Andler (Ret.)** *is a retired Orange County Superior Court judge and Southern California-based neutral who specializes in business, employment, class actions, and mass torts.*