CRIMINAL JUSTICE • PROFESSIONAL PRACTICE • CONCEPTUAL ARTICLE

The New Architecture of Defense Investigation

The Changing Role of Private and Defense Investigators in the Modern Criminal Justice System

James Allister Odd, PhD
j.a.odd@ntrklnk.net
Affiliation: NTRLNK, Oregon, USA
ORCID: 0009-0008-2976-6313

DOCUMENT TYPE: Research Paper
PUBLICATION DATE: April, 2026
VERSION: 1.0

NTRLNK RELATIONSHIP
This paper was authored by or in association with NTRLNK. The author is responsible for the research methods, analysis, findings, and conclusions presented.

Abstract

The private or defense investigator has traditionally been pictured as a field operative who locates witnesses, verifies alibis, photographs scenes, and uncovers facts overlooked by police. Those functions remain essential, but they no longer capture the role's full significance. Contemporary criminal cases are built from interdependent evidence systems: police reports, body-worn video, mobile-device extractions, cloud records, automated alerts, social-media content, forensic laboratory outputs, location analytics, and large electronic discovery productions. At the same time, negotiated dispositions dominate criminal case processing, public defense systems face resource and workload constraints, and artificial intelligence is entering legal and investigative workflows. This article argues that the modern defense investigator is evolving from an adjunct fact finder into an evidence-system integrator and adversarial reliability officer. The investigator increasingly helps the defense team reconstruct provenance, test the government's account, identify missing data, triage discovery, translate technology, preserve open-source material, develop mitigation, and document uncertainty. The article distinguishes private investigators from defense investigators, explains the constitutional and professional framework within which investigators operate, proposes a Defense Investigation Assurance Cycle, and analyzes ethical limits involving confidentiality, supervision, witness contact, deception, privacy, unauthorized computer access, and AI. It also examines structural inequality between retained and publicly funded defense, proposes a competency architecture and institutional reforms, and sets out a research agenda for measuring investigative quality. The thesis is not that technology replaces fieldwork. It is that effective fieldwork now occurs inside a broader system of digital, forensic, social, and procedural verification. A modern criminal justice system should therefore treat defense investigation as a core component of reliable adjudication rather than an optional service purchased only in exceptional cases.

Keywords: defense investigation; private investigators; criminal justice; digital evidence; discovery; mitigation; open-source intelligence; artificial intelligence; public defense; forensic science

1. Introduction

The familiar image of the private investigator belongs to an earlier evidentiary economy: a notebook, a camera, a vehicle, courthouse records, and a succession of in-person interviews. That image was always incomplete, but it now obscures more than it reveals. A single modern criminal case may include thousands of text messages, several body-worn-camera streams, a mobile-device extraction, cloud-service returns, vehicle telemetry, social-media posts, automated license-plate detections, surveillance video, laboratory reports, and spreadsheets built by police analysts. Each source has its own retention period, time standard, access controls, error modes, and chain of transformation.

Defense investigation has consequently become both more important and more difficult. The investigator still finds people and places, develops trust, notices inconsistencies, and tests whether an asserted event could have happened. Yet the investigator must increasingly understand how evidence was created, what was not collected, how a tool transformed it, what assumptions link a digital identifier to a human being, and whether several exhibits are independent or merely different renderings of one source. In a plea-centered system, this work often must occur before trial is realistic and sometimes before the defense has received complete or usable discovery.

The legal system already recognizes investigation as part of competent defense practice. The Sixth Amendment right to counsel, applied to state felony prosecutions through *Gideon v. Wainwright*, is not satisfied by the physical presence of an attorney who lacks the factual basis to advise and advocate [1,2]. *Strickland v. Washington* treats reasonable investigation—or a reasonable decision that particular investigation is unnecessary—as part of counsel's professional obligation [3]. The American Bar Association's Defense Function Standards state that counsel has a duty to investigate in all cases, should begin promptly, should independently evaluate prosecution evidence, and should consider engaging fact investigators, forensic experts, accountants, sentencing specialists, and social workers [4]. Federal law likewise authorizes investigative, expert, and other services necessary for adequate representation of financially eligible defendants [5,6].

Despite that foundation, the investigator is often operationally treated as supplemental. Some retained clients cannot afford sustained investigation after paying counsel. Some assigned-counsel systems require advance judicial authorization. Some public defender offices lack enough investigators for their caseloads. Bureau of Justice Statistics data for 2013 showed that six state-administered systems reported fewer than ten full-time-equivalent investigators in public defender offices, an older finding that illustrates the long-running resource problem rather than current staffing in every state [7]. The revised ABA Ten Principles identify funding, workload control, training, supervision, and essential defense-team components as system concerns [8]. The 2023 National Public Defense Workload Study further challenges inherited caseload assumptions and emphasizes the time needed for quality representation [9].

This article makes three claims. First, the changing evidence environment expands the investigator's function from isolated fact gathering to lifecycle-wide evidence assurance. Second, the expansion requires clearer governance: role definitions, attorney supervision, technical competence, source provenance, security, and explicit rules for AI-assisted work. Third, access to capable investigation is a system-quality issue. When only well-resourced defendants can independently test digital and forensic evidence, formally equal procedural rights operate on unequal factual foundations.

The discussion is principally about the United States. State licensing, privacy, recording, discovery, victim-rights, and professional-conduct rules vary substantially. The article therefore offers a conceptual and operational framework, not legal advice for a particular jurisdiction or case.

2. Terminology and Institutional Position

2.1 Private investigator and defense investigator are overlapping, not identical, categories

A private investigator is generally defined by occupation and state regulatory status. Private detectives and investigators gather, analyze, and report information for clients in legal, financial, corporate, or personal matters. The Bureau of Labor Statistics reports that most states require licensure and projects employment growth from 2024 to 2034 [10]. Licensing requirements, exemptions, permitted activities, continuing education, insurance, and reciprocity differ by state.

A defense investigator is defined primarily by function: the investigator works for or with the defense team in a criminal, juvenile, regulatory, military, or post-conviction matter. The person may be a salaried public defender employee, a federal defender investigator, a court-authorized contractor, a licensed private investigator retained by counsel, a mitigation specialist, a digital-forensic consultant, or a member of an innocence organization. Some jurisdictions exempt certain employees from private-investigator licensing; others do not. A license establishes regulatory permission to perform specified work. It does not, by itself, establish competence in criminal defense, digital evidence, mitigation, or the ethical duties flowing through counsel.

This distinction matters. A successful insurance-fraud or corporate investigator may not understand defense confidentiality, exculpatory-evidence strategy, client-centered practice, discovery restrictions, or the risk that an interview will create a discoverable statement. Conversely, an experienced public defender investigator may possess deep defense expertise but be limited by law when accepting independent private work. Engagement letters and case plans should identify the investigator's role, supervisor, authority, deliverables, confidentiality expectations, and limits.

2.2 The investigator is not a substitute lawyer, police officer, or forensic expert

The defense investigator works within a legal representation but ordinarily does not give legal advice, decide litigation strategy, or speak for the client. Counsel retains responsibility for legal judgments and supervision. ABA Model Rule 5.3 requires lawyers to make reasonable efforts to ensure that retained or employed nonlawyer assistance is compatible with the lawyer's professional obligations [11]. The specific rule adopted in the governing jurisdiction controls.

The investigator is also not a police officer. Private status generally confers no general power to compel answers, enter property, obtain nonpublic account content, execute process, or use restricted government databases. Interview subjects may decline. Consent must be real. Credentials and purpose must not be misrepresented in a manner prohibited by law or professional rules. Evidence must not be altered, concealed, or unlawfully possessed.

Finally, investigation and expert analysis should not be casually merged. An investigator may identify why a cell-site conclusion needs review, locate source records, document a scene, or coordinate an expert. A qualified expert may be required to conduct a forensic acquisition, interpret probabilistic DNA evidence, validate software, or offer an opinion. The investigator's emerging value lies partly in recognizing when a question exceeds personal competence and building the bridge to the right specialist.

2.3 Confidentiality, privilege, and work product require structure

Communications involving an investigator may receive protection when the investigator is engaged by counsel to assist the provision of legal services, but the result depends on jurisdiction, purpose, content, and handling. Labels do not create privilege. An investigator's presence in an interview, disclosure to a third party, a business-purpose engagement, or careless distribution can complicate protection. Written retention through counsel, defined legal purpose, need-to-know access, secure systems, and disciplined reporting reduce avoidable risk. Teams should never promise a witness or client that every investigator record is categorically privileged or immune from disclosure.

3. Forces Transforming Defense Investigation

3.1 Digital saturation of ordinary life

Digital evidence is no longer a specialty confined to cybercrime. NIST observes that digital information from computers, mobile devices, audio, video, and images can be relevant to most crimes [12]. Mobile devices may contain communications, location-related information, photographs, application data, account tokens, and links to cloud services. NIST guidance treats mobile forensics as an evolving specialty requiring preservation, acquisition, examination, analysis, and reporting under forensically sound conditions [13].

For defense investigators, digital saturation changes the first interview. Questions about “where were you?” now require questions about devices, accounts, shared credentials, vehicle systems, app settings, automatic backups, location permissions, workplace networks, and who else had access. A client may believe a deleted message is gone when it remains in a recipient's device or cloud return. A timestamp may reflect upload, conversion, or server processing rather than creation. A social-media screenshot may omit the account identifier, URL, surrounding thread, or time zone needed to evaluate authenticity.

The investigator therefore becomes an early-warning sensor. Counsel needs prompt notice that relevant data are volatile, held by a third party, subject to short retention, or at risk of remote alteration. The investigator should not seize or search devices without authority and competence; instead, the role is to recognize preservation needs, prevent well-intentioned contamination, and coordinate lawful collection.

3.2 Discovery has become an information-management problem

The ABA's 2020 Discovery Standards define the defense to include counsel, legal or investigative staff, and the defendant [14]. Federal criminal practice is governed in part by Rule 16, constitutional disclosure obligations, statutes, local rules, protective orders, and case-specific directions [15]. Federal Rule of Criminal Procedure 16.1 requires an early conference about the timetable and procedures for pretrial disclosure, a rule especially important in complex or voluminous discovery [15]. A joint federal ESI protocol developed by the Department of Justice and federal defender community encourages communication about format, timing, security, and discovery coordination [16]. State systems vary widely.

Receiving data is not the same as receiving usable information. Productions may be duplicated, unindexed, encrypted, stripped of metadata, associated with proprietary viewers, divided across supplements, or organized according to law-enforcement rather than defense questions. Investigators increasingly perform discovery assurance: inventorying what arrived, verifying readability, linking files to reports and warrants, identifying gaps, and escalating anomalies to counsel. This is not clerical work. A missing native file, absent audit log, unexplained date range, or unproduced attachment can change what can be investigated and challenged.

3.3 Evidence is generated by systems, not merely found at scenes

Modern exhibits often originate in systems that mediate observation. A face-recognition lead may begin with a vendor algorithm and candidate list. A gunshot alert may depend on networked sensors and classification logic. A phone-location visualization may rest on provider records, mapping software, analyst assumptions, and time conversion. A digital-forensic report may summarize selected artifacts while omitting extraction warnings or unsupported app versions.

This creates a new defense task: reconstruct the evidence pipeline. Who or what generated the original data? What was the business or technical purpose? Which version of hardware and software was

involved? What transformations occurred? What did the operator select? What uncertainty or failure information was discarded? NIST's scientific foundation review emphasizes that digital investigation methods have a strong scientific basis while also identifying the importance of tool testing, documentation, examiner competence, and interpretation [17]. The defense investigator need not reject technology. The role is to prevent technological authority from replacing verification.

3.4 Early case resolution compresses the investigation window

Investigation is often imagined as preparation for trial. In practice, factual investigation affects release, charging, diversion, plea advice, suppression, sentencing, and collateral consequences. Delay can make a witness unreachable, overwrite video, close an account, or erase a business system's logs. A rapid plea may foreclose investigation into attribution, search legality, alternative suspects, forensic limitations, or mitigation.

The modern investigator must therefore operate in parallel with legal triage. A short initial assignment should identify high-consequence uncertainties and perishable sources, not merely execute a generic checklist. Counsel needs concise interim findings that can inform an immediate decision while the fuller investigation continues.

3.5 The defense function is increasingly multidisciplinary

The ABA Defense Function Standards contemplate fact investigators, forensic and accounting experts, sentencing specialists, and social workers [4]. Capital defense standards expressly describe a team that includes a fact investigator and mitigation specialist and place overall responsibility on lead counsel [18]. The underlying insight extends beyond capital cases: legal outcome depends on facts about the charged event, the client, institutions, trauma, disability, treatment, family, employment, immigration, housing, and community support.

The investigator is often the team member who can connect these domains. A fact discovered during a family interview may affect competency screening, suppression, mitigation, or a release plan. A school record may explain behavior that police described as evasive. An employment record may establish both an alibi and a stable reentry plan. Modern investigation is not only about contradiction; it is also about context.

3.6 AI changes both the evidence and the work

AI affects defense investigation in two ways. First, AI-generated or AI-mediated content may itself enter a case: synthetic media, automated risk scores, face matches, content-moderation reports, transcription, translation, predictive policing outputs, or summaries created inside discovery platforms. Second, defense teams may use AI to search, cluster, translate, summarize, transcribe, or draft.

ABA Formal Opinion 512 explains that lawyers using generative AI must consider competence, confidentiality, communication, candor, supervision, and reasonable fees; outputs require review, and managerial lawyers must establish policies and training for lawyers and nonlawyers [19]. NIST's AI Risk Management Framework and Generative AI Profile emphasize governance, documentation, human oversight, measurement, provenance, and risks such as confabulation and information integrity [20,21]. For investigators, the consequence is straightforward: AI may generate leads, but it cannot relieve the defense team of source verification or responsibility.

4. The Emerging Role: Eight Interlocking Functions

4.1 Independent fact developer

The investigator's foundational role remains independent fact development. Police investigation is organized around public authority and prosecutorial decision-making. Defense investigation asks different questions: What weakens attribution? What supports a justification or excuse? What affects admissibility, credibility, punishment, or disposition? What was not asked because it did not fit the initial theory?

Independence does not mean predetermined opposition to every government fact. It means the defense does not outsource its factual understanding to the party carrying the burden of proof. The investigator should test the client's account as well as the government's account, document adverse findings, and avoid coaching facts. Loyalty to the defense function is compatible with methodological neutrality about what a source will show.

4.2 Discovery assurance analyst

The discovery assurance function verifies that the defense can account for, access, and understand what has been produced. Core tasks include:

1. maintaining a production register with dates, sources, media, file counts, hash values where supplied, and protective-order restrictions;
2. testing whether files open, whether proprietary viewers are available, and whether native structure or metadata has been preserved;
3. linking reports to underlying recordings, photographs, laboratory files, extraction reports, warrants, returns, and audit trails;
4. identifying unexplained gaps, duplicates, truncated exports, missing attachments, inconsistent Bates ranges, or changed files;
5. distinguishing absence from nonproduction, noncollection, deletion, retention limits, technical failure, or privilege withholding; and
6. giving counsel a prioritized exception report rather than a false assurance that “discovery was reviewed.”

This role requires coordination with litigation-support staff and counsel. The investigator should not make unilateral discovery demands or legal representations unless authorized. But investigators are well placed to notice when the materials do not support the narrative built around them.

4.3 Digital-evidence translator and preservation coordinator

Defense teams need someone who can translate between human events and technical artifacts. The investigator may explain that an IP address identifies a connection, not automatically a person; that a device extraction is a snapshot subject to acquisition limits; or that a map pin may reflect an estimated location. Translation should identify both the artifact's probative potential and its limits.

The investigator also coordinates preservation. This can include identifying businesses with video, documenting public web content, asking counsel whether preservation letters or subpoenas are required, and maintaining provenance for defense-collected material. NIST guidance on digital evidence preservation stresses that digital material presents problems beyond traditional evidence and requires attention to storage, integrity, and associated metadata [22]. Preservation should be minimally invasive, authorized, repeatable where feasible, and documented.

4.4 Forensic adversarial auditor

The defense investigator increasingly audits the path from raw material to forensic conclusion. This means asking:

7. Was the submitted item the same item described in the report?
8. Was the method validated for the device, sample, population, or software version at issue?
9. Were limitations, inconclusive results, contamination risks, or alternative interpretations reported?
10. Did an analyst receive context that could bias interpretation?
11. Does the report distinguish observation from inference?
12. Can the conclusion be reproduced from the disclosed materials?
13. Is a second method genuinely independent or derived from the same source?

The investigator may not have the expertise to answer every question. The value lies in building an evidence map, identifying the hinge assumptions, and preparing a focused expert referral. A broad request to “review the forensics” is expensive and vague; a structured referral can ask whether a specific result supports a particular proposition and what records are needed to evaluate it.

4.5 Witness and interview specialist

Human interviewing remains irreplaceable. Modern pressures make it more delicate. Witnesses may have reviewed online commentary, police video, news coverage, or other witnesses' posts before the defense arrives. Memory can be contaminated by repeated exposure. People may fear online harassment or

believe a defense contact is an attempt to undermine a victim. Investigators need trauma-informed, culturally competent, accessible, and noncoercive approaches.

The interview plan should identify the investigator, clarify that participation is voluntary, avoid legal advice, use open-ended questions before detail prompts, separate personal observation from later information, and document the conditions of the interview. Whether and how to record requires counsel's direction and compliance with jurisdiction-specific consent law. Recording may preserve accuracy but can alter rapport, create security risks, and affect disclosure obligations. Notes should distinguish quotations, paraphrase, investigator observation, and unresolved follow-up.

4.6 Mitigation and life-history investigator

Mitigation is not a plea for sympathy detached from facts. It is a disciplined reconstruction of a person's development, functioning, environment, trauma, health, education, relationships, responsibilities, and capacity for change. Records and interviews may identify disability, brain injury, mental illness, coercion, exploitation, substance-use disorder, military service, caregiving, cultural displacement, or institutional failure. The same work can inform release conditions, diversion, treatment, competency, sentencing, and reentry.

The modern mitigation function is longitudinal and relational. Records rarely explain themselves. A school file may use outdated diagnostic language; a medical record may fragment care across providers; family accounts may conflict because of trauma or estrangement. Investigators and mitigation specialists need consent practices, sensitivity to secondary trauma, secure record handling, and the humility to avoid clinical conclusions outside their qualifications.

4.7 Open-source and social-media investigator

Open-source investigation can identify witnesses, verify places and times, preserve public statements, compare images, trace organizational relationships, and discover exculpatory context. The Berkeley Protocol offers a useful methodology for professional, legal, ethical, and secure collection of digital open-source information, although it was developed for international criminal and human-rights investigations rather than ordinary domestic defense practice [23]. Its emphasis on planning, preservation, verification, documentation, and investigator safety is transferable.

Public availability does not erase ethical or privacy concerns. A public post may expose a child, victim, juror, or uninvolved person. Platform terms, state anti-pretexting laws, professional rules, protective orders, and expectations surrounding represented persons may matter. Investigators should use the least intrusive method that answers the question, preserve context, document the account and URL, avoid interacting with content unless strategically and ethically approved, and never assume that a screenshot proves authorship or authenticity.

4.8 Case integrator and uncertainty reporter

The final emerging function is integration. The investigator connects witness accounts, digital artifacts, forensic reports, scene evidence, records, and mitigation into a coherent case map. Integration is not storytelling untethered from uncertainty. It requires identifying conflicts, dependencies, missing sources, and confidence limits.

A useful investigative report separates:

14. verified observations;
15. source statements attributed to the speaker;
16. technical transformations and their tools;
17. investigator inferences;
18. alternative explanations;
19. unverified leads; and
20. tasks that remain incomplete because of time, authority, access, or resources.

This structure helps counsel make decisions and prevents a confident narrative from concealing a fragile evidentiary base.

5. The Role Across the Case Lifecycle

The investigator's work should be matched to the decision point. The following matrix illustrates how the role changes across a case.

Stage	Priority questions	Illustrative investigator contribution	Principal risk if omitted
Precharge or initial contact	What is volatile? What contact or conduct could create exposure?	Preserve public sources; locate counsel-approved witnesses; identify devices, accounts, and surveillance	Loss of short-retention evidence; avoidable self-help or contamination
First appearance and release	What facts bear on identity, stability, safety, and conditions?	Verify residence, employment, caregiving, treatment, transportation, and community support	Unnecessary detention; unrealistic release plan
Early discovery and plea advice	What is the prosecution's factual theory, and what remains untested?	Inventory discovery; test core attribution; identify missing source material; develop mitigation	Decision based on incomplete or unusable evidence
Motions practice	How was evidence obtained, generated, selected, and preserved?	Reconstruct search and evidence pipeline; locate consent and access facts; coordinate technical review	Unchallenged search, identification, or technical assumption
Trial preparation	Which facts are admissible, provable, and understandable?	Reinterview witnesses; verify exhibits; prepare scene and timeline materials; support expert testing	Surprise, impeachment vulnerability, or overstatement
Sentencing and disposition	What individualized history and feasible alternatives matter?	Develop life history, records, treatment options, restitution context, and reentry resources	Flattened account of the person; poorly supported alternative plan

Stage	Priority questions	Illustrative investigator contribution	Principal risk if omitted
Post-conviction	What was missed, withheld, newly testable, or inaccurately interpreted?	Reconstruct old files; locate witnesses; seek retained evidence; apply modern forensic methods	Irretrievable evidence and uncorrected error

6. A Defense Investigation Assurance Cycle

To operationalize the expanded role, this article proposes a Defense Investigation Assurance Cycle (DIAC). The cycle is not a legal standard and does not replace office policy. It is a repeatable planning model designed to keep investigation connected to counsel's decisions.

6.1 Define the mandate

Counsel and investigator identify the legal question, factual propositions, decision deadline, authority, budget, jurisdiction, safety concerns, and prohibited actions. The assignment should state what decision the investigation will inform. “Interview everyone” is not a mandate; “determine whether any witness independently observed the driver enter the vehicle before 22:15” is.

6.2 Identify hypotheses and consequences

Record reasonable competing explanations and the consequences of each. The government theory, client account, mistaken attribution, third-party action, system error, and insufficient-information outcome may all need consideration. The purpose is to prevent investigative activity from becoming a search for confirmation.

6.3 Map evidence sources and dependencies

List people, places, devices, accounts, records, physical items, and system-generated data. Mark who controls each source, retention risk, legal process required, and whether it derives from another source. A police report summarizing body-camera video and an AI summary of that report are not three independent observations.

6.4 Preserve proportionately

Prioritize lawful preservation of volatile, unique, and potentially exculpatory material. Do not manipulate a client's device, log into another person's account, or direct a witness to delete or alter content. Escalate to counsel when consent, process, forensic acquisition, or emergency action is required.

6.5 Test the hinge facts

Identify facts that would materially change a legal or strategic decision. Test high-discrimination facts first. An independent access log may resolve an attribution issue more efficiently than reviewing hundreds of repetitive messages. Record negative and inconclusive results; they can narrow the theory or expose collection limits.

6.6 Verify methods and provenance

For each material item, record origin, collector, date and time, method, transformations, storage location, integrity information where appropriate, and limitations. For digital material, preserve native files and metadata when lawful and feasible. For web content, preserve context and document the collection process.

6.7 Communicate in decision-ready form

Interim reports should lead with the question, current answer, confidence, decisive support, contradictory facts, and next action. Counsel should not have to infer urgency from a chronological activity log. Full notes and provenance remain available behind the summary.

6.8 Reassess, stop, or redirect

Investigation should change when evidence changes. Stop when the decision is adequately supported, further work is disproportionate, authority ends, or available sources cannot resolve the uncertainty. Redirect when a pivotal assumption fails. Document the reason rather than silently abandoning the original task.

7. Ethical and Legal Boundaries

7.1 Attorney supervision and professional responsibility

Investigators retained by counsel operate within counsel's supervisory framework. Model Rule 5.3 is central, but other rules may affect confidentiality, communication with represented or unrepresented persons, respect for third-person rights, fairness to opposing parties, candor, and misconduct [11]. State versions and ethics opinions differ. The engagement should specify escalation points for questionable contact, unexpected evidence, threats, privileged material, media inquiry, or potential illegality.

The ABA Defense Function Standards prohibit illegal or unethical investigative means and direct counsel to know the jurisdiction's rules concerning victims, witnesses, deceit, and represented persons [4]. An investigator should not be asked to do indirectly what counsel could not ethically do directly.

7.2 Witness contact and identity

Witnesses belong to neither side, but their rights and applicable restrictions must be respected. Investigators should accurately identify themselves and their relationship to the defense unless jurisdiction-specific law and ethics clearly permit a different practice approved by counsel. They should not imply governmental authority, guarantee outcomes, pay for testimony, threaten exposure, or interfere with lawful process. Reasonable expenses and expert compensation require careful distinction from inducements.

Contact with a represented person can implicate professional-conduct rules through counsel. Victim-rights statutes, protective orders, no-contact orders, workplace rules, and safety plans may impose additional limits. The correct approach is not categorical avoidance; it is planned, respectful contact under governing law.

7.3 Collection, possession, and alteration of evidence

An investigator who encounters contraband, stolen property, a weapon, or incriminating digital content should stop and consult counsel. Moving, receiving, copying, or changing an item can create legal, ethical, safety, and chain-of-custody consequences. The ABA standards specifically caution counsel to examine jurisdictional law on obstruction, tampering, confidentiality, and self-incrimination when a client possesses potentially incriminating evidence [4].

Defense-created evidence also requires integrity. Original notes, recordings, photographs, downloads, and metadata should be preserved according to policy. Corrections should be transparent. A polished report must not replace or obscure the underlying record.

7.4 Privacy, data brokerage, and permissible purpose

Commercial databases can locate witnesses and connect addresses, phones, properties, relatives, and businesses. Their availability does not create unlimited authority. The Fair Credit Reporting Act restricts consumer reports to statutory permissible purposes and imposes accuracy and other obligations in covered contexts [24]. Other federal and state laws regulate motor-vehicle data, communications, health information, financial records, biometrics, data brokers, and stalking-related conduct.

Before using a database, the investigator should know what it contains, the lawful purpose certified, accuracy limitations, audit rules, reuse restrictions, and whether results require verification in an authoritative source. “Database hit” should never be reported as a confirmed identity without matching reliable identifiers.

7.5 Unauthorized access and pretexting

The boundary between open-source research and unauthorized access must be treated conservatively. Investigators should not use borrowed credentials, guess passwords, bypass technical controls, solicit another person's authentication code, or enter a restricted account without documented authority. The Computer Fraud and Abuse Act addresses access without authorization and exceeding authorized access; the Department of Justice's charging policy underscores the importance of actual authorization and knowledge while making clear that a charging policy is not a grant of investigative permission [25]. State computer-crime and privacy laws may be broader.

Creating a false persona, sending a connection request, or interacting with a private group can implicate platform rules, deception law, professional ethics, and represented-person restrictions. Such tactics require jurisdiction-specific legal review and should never be normalized as routine OSINT.

7.6 Recording, surveillance, and physical safety

Audio-recording consent laws differ. Surveillance can implicate trespass, harassment, stalking, privacy, labor, and camera laws. Drone use adds airspace and local restrictions. Investigators should use written operational plans for prolonged surveillance, sensitive locations, domestic-violence contexts, minors, or subjects with known risk. Safety planning should protect the investigator, client, witness, and public; obtaining evidence never justifies escalating danger.

8. Artificial Intelligence in Defense Investigation

8.1 Appropriate uses

With approved systems and data controls, AI may assist with low- and medium-risk tasks such as generating search terms, clustering similar documents, producing a first-pass transcript, translating for investigative orientation, extracting named entities, comparing timelines, or identifying topics for human review. These uses can expand capacity when discovery is large.

The tool's role must be described precisely. A transcript produced by automatic speech recognition is a draft until checked against the recording. A translation used to locate a passage is not necessarily fit for evidentiary use. A model-generated timeline reflects selected inputs and can omit contradictions. An image detector's score does not establish that content is synthetic or authentic.

8.2 Prohibited shortcuts

Investigators should not:

21. submit confidential case material to an unapproved public service;
22. treat generated text as a source;

23. rely on a model-supplied citation without retrieving and checking it;
24. permit an AI summary to replace review of decisive evidence;
25. characterize probabilistic output as a factual identification;
26. use synthetic media to mislead a witness or court; or
27. conceal material AI involvement from supervising counsel.

8.3 An AI lead-and-verification register

Every material AI-assisted output should be logged with the tool, version or service where available, date, task, inputs or source set, settings, output location, reviewer, verification method, and disposition. The register should distinguish lead generation from evidentiary analysis. If an AI output changed whom the defense contacted or what it collected, enough context should be retained to explain that decision.

Human review must be substantive, not ceremonial. The reviewer should compare the output with source evidence, test omissions, check names and dates, and record corrections. Formal Opinion 512's focus on competence, confidentiality, candor, and supervision makes clear that responsibility remains with the legal team [19]. NIST's framework similarly supports defined human roles, documented limitations, evaluation, and lifecycle governance [20,21].

8.4 AI as an object of investigation

When the state or a private complainant relied on AI, the investigator should seek the evidence pipeline: system purpose, developer and operator, version, inputs, thresholds, output, human review, validation, error information, retention, audit logs, and downstream uses. The legal question may concern search, disclosure, confrontation, expert testimony, discrimination, or reliability; counsel decides the litigation theory. The investigator's role is to reveal what happened between raw input and asserted conclusion.

9. Structural Inequality and the Two-Tier Investigation Problem

The transformation described in this article can widen inequality. A retained defense may hire separate investigators, digital-forensic examiners, mitigation specialists, and litigation-support vendors. A public defender investigator may carry numerous urgent matters, lack specialized software, and depend on court approval for outside expertise. Federal law provides a route to necessary investigative and expert services, including ex parte applications in appropriate cases, but authorization, rates, and administrative practices still shape access [5,6]. State systems use different structures and funding rules.

Technology does not automatically equalize capacity. Low-cost AI may help triage documents, but it can also transfer risk to offices least able to validate outputs, negotiate vendor terms, or protect confidential data. Proprietary discovery formats and forensic tools can impose licensing costs. Cloud evidence may

require rapid legal process. Rural defense teams may lack local specialists. Language access and disability accommodation add further needs.

The revised ABA Ten Principles frame independence, funding, workload control, data, early access, training, supervision, and essential components as system requirements [8]. Investigation should be included in workload measurement. Counting attorney cases without measuring investigator hours, discovery volume, travel, language needs, digital complexity, and mitigation demands understates the resources required for effective defense.

A modern funding model should provide baseline investigator staffing, rapid-access preservation capacity, protected expert funds, secure discovery infrastructure, and regional specialist pools. Courts should evaluate requests for services in light of the factual work needed for an informed defense, not whether the defense can already prove the service will change the outcome. Requiring that proof can create a circular barrier: investigation is denied because the uninvestigated case lacks evidence demonstrating the need for investigation.

10. Competency Architecture for the Modern Investigator

No single investigator will master every domain. The goal is a T-shaped profession: deep competence in investigation, interviewing, documentation, and ethics, with enough cross-domain literacy to recognize specialized issues and coordinate experts.

10.1 Foundational competencies

28. lawful and ethical fact investigation;
29. interviewing, rapport, memory-aware questioning, and statement documentation;
30. scene assessment, photography, measurement, canvassing, and records research;
31. clear report writing that separates fact, source account, inference, and limitation;
32. case planning, prioritization, time management, and testimony preparation;
33. cultural humility, disability access, language-access coordination, and trauma awareness; and
34. safety, conflict screening, confidentiality, and secure information handling.

10.2 Digital and forensic literacy

35. basic data provenance, metadata, hashing, time zones, and chain of transformation;
36. mobile, cloud, social-media, video, location, and account concepts;
37. discovery inventories, file formats, viewers, search, deduplication, and exception reporting;
38. scientific-method concepts, validation, uncertainty, error, cognitive bias, and independent verification;

39. preservation of public web material and recognition of when forensic acquisition is required; and
40. AI capabilities, failure modes, confidentiality risks, prompt and output logging, and human verification.

10.3 Defense-team competencies

41. understanding the stages of a criminal case and the decisions investigation informs;
42. working under counsel's supervision without crossing into legal advice;
43. identifying when facts affect release, suppression, plea advice, trial, mitigation, or post-conviction review;
44. coordinating experts and preparing targeted referral packages;
45. communicating urgent findings concisely while preserving complete notes; and
46. practicing client-centered investigation without becoming uncritical of any account.

Competence should be demonstrated through scenario-based assessment, supervised casework, continuing education, and review of actual work products. A generic license exam or years of law-enforcement experience should not be treated as a complete defense-investigation credential.

11. Organization, Workflow, and Quality Assurance

11.1 Team design

Every matter should have a named supervising attorney and investigative lead. Complex cases should identify a discovery coordinator, digital-evidence lead, mitigation lead, and expert coordinator, even if one person holds several roles. Responsibility matrices prevent the common failure in which everyone assumes someone else preserved a source or reviewed an extraction.

11.2 Case-management controls

Minimum controls should include a source register, discovery-production log, contact log, task and deadline tracker, evidence-location map, privilege and protective-order designations, and decision log. Systems should support role-based access, encryption, multifactor authentication, secure sharing, retention, legal hold, and documented destruction when authorized.

11.3 Review gates

Quality review should occur at decision points rather than only before trial. Useful gates include:

47. **Initial preservation review:** Have volatile sources and access risks been identified?
48. **Plea-readiness review:** Has the core government theory been independently tested enough for informed advice?

49. **Forensic challenge review:** Are source files, validation materials, limitations, and an expert referral available?
50. **Witness readiness review:** Are contact, statement history, recording status, vulnerabilities, and impeachment risks documented?
51. **Disposition review:** Is the mitigation and alternative plan verified and feasible?
52. **Closeout review:** Are originals retained, derivative products identified, unresolved issues recorded, and future deadlines calendared?

11.4 Reporting quality

Reports should be useful to counsel and resilient under scrutiny. They should identify the assignment, methods, dates, people contacted, materials reviewed, results, limitations, and next actions. The report should not state that a person “lied” when the evidence only shows inconsistency, or that digital data “proved” presence when it supports a more limited inference. Quotations require fidelity; summaries require attribution.

Quality assurance can sample files for source traceability, timely escalation, complete adverse findings, correct time normalization, database verification, AI logging, and compliance with restrictions. The aim is learning and reliability, not paperwork for its own sake.

12. Measuring Investigative Value

Defense investigation is difficult to evaluate because success is not limited to acquittal. Investigation may secure release, narrow charges, expose inadmissible evidence, produce a safer plea, support treatment, improve sentencing information, prevent surprise, or confirm that the government's evidence is stronger than the client believed. It may also establish that a proposed avenue lacks merit, saving scarce resources.

Performance measures should therefore combine process, quality, and outcome indicators.

12.1 Process measures

53. time from appointment to investigator engagement;
54. proportion of cases receiving documented investigative screening;
55. time to identify and preserve volatile sources;
56. discovery exceptions detected and resolved;
57. expert referrals made before decision deadlines; and
58. investigator workload adjusted for complexity, travel, language, digital volume, and mitigation.

12.2 Quality measures

59. source traceability of material findings;

60. distinction between observation, statement, inference, and AI-generated lead;
61. documentation of adverse and inconclusive findings;
62. supervisor review at defined gates;
63. compliance with confidentiality, protective orders, and data security; and
64. reproducibility of timelines, calculations, and digital transformations.

12.3 Outcome measures

65. evidence preserved that would otherwise have been lost;
66. changes to release, charging, suppression, disposition, sentencing, or post-conviction posture associated with verified findings;
67. reduction in late continuances caused by discovery or investigative failures;
68. client understanding and participation; and
69. corrective action after quality review.

Metrics must not reward investigators for producing favorable facts or discourage honest adverse findings. A quota based on witness statements, “hits,” dismissals, or billable hours will distort practice. The appropriate question is whether investigation improved the factual reliability and informedness of defense decisions.

13. Future Directions

13.1 The investigator as evidence-system integrator

The most likely future is not a complete split between field investigator and technologist. It is layered practice. General defense investigators will conduct interviews, scenes, records, preservation triage, and discovery assurance. Specialist investigators will handle complex digital acquisitions, financial tracing, advanced OSINT, analytics, or technical surveillance. The generalist will need enough literacy to identify the issue early and preserve the specialist's ability to act.

13.2 Defense forensic readiness

Forensic readiness is usually discussed as an organizational capacity to preserve evidence before an incident. Defense systems also need readiness: standing vendor agreements, secure transfer tools, rapid preservation protocols, validated utilities, regional experts, emergency funding, and model discovery requests. Building capability after a client is arrested is often too late.

13.3 Portable evidence provenance

Discovery platforms and forensic tools should export provenance in open, reviewable formats. A defense team should be able to determine source, collection event, hashes, transformations, tool versions,

annotations, and production history without relying entirely on a vendor interface. Courts and rulemakers should consider whether complex digital productions are meaningfully usable when essential provenance or review capability is withheld.

13.4 AI governance as ordinary case governance

AI policy should not be a separate binder that investigators never consult. It should be embedded in intake, vendor approval, data classification, task assignment, output labeling, supervisor review, expert referral, and reporting. High-consequence uses should require more verification than low-risk administrative assistance. Defense offices should preserve enough information to explain material AI-assisted decisions without retaining unnecessary sensitive data.

13.5 A stronger professional identity

Defense investigation would benefit from shared competency standards, ethical guidance tailored to investigators, supervised pathways into practice, digital-evidence training, and continuing education. Professionalization should not create barriers that exclude community knowledge, language skills, or lived experience. The best model combines technical and procedural standards with diverse recruitment and accessible training.

14. Recommendations

14.1 For defense counsel and firms

70. Engage an investigator early enough to preserve evidence and inform release and plea decisions.
71. Retain investigators through clear written terms identifying legal purpose, supervision, scope, security, and deliverables.
72. Use a documented investigative screening process in every case, even when full investigation is not initially authorized.
73. Treat discovery usability and completeness as a factual assurance task, not only a legal exchange.
74. Establish approved-tool and AI policies; prohibit confidential uploads to unapproved services.
75. Budget for specialist consultation when digital, scientific, financial, language, or mitigation issues exceed team competence.
76. Review adverse findings and unresolved uncertainty rather than rewarding confirmation of the preferred theory.

14.2 For public defense organizations

77. Include investigator time and evidence complexity in workload standards and staffing models.

78. Create rapid-response preservation capacity and regional pools for digital, forensic, financial, and mitigation expertise.
79. Provide secure discovery infrastructure, not only software licenses without training and support.
80. Build career ladders, supervision, peer review, and continuing education for investigators.
81. Collect quality and workload data that do not compromise client confidentiality or defense independence.
82. Use multidisciplinary teams at the earliest consequential stages, not only after a case is designated for trial.

14.3 For courts and funding authorities

83. Treat necessary investigative services as part of adequate representation, consistent with governing law [5,6].
84. Permit confidential, timely requests and avoid requiring defense disclosure of strategy beyond what is necessary.
85. Set compensation and administrative processes that allow qualified specialists to accept defense work.
86. Address unusable digital discovery through early conferences, production standards, and adequate review time.
87. Evaluate equality of investigative capacity as part of public-defense system oversight.

14.4 For investigators and professional associations

88. Define defense-specific competencies beyond general licensure.
89. Adopt standards for source verification, note preservation, digital provenance, AI logging, and uncertainty reporting.
90. Develop reciprocal training among investigators, lawyers, forensic scientists, mitigation specialists, and technologists.
91. Create confidential consultation and ethics resources for novel investigative methods.
92. Evaluate tools and methods through realistic exercises rather than vendor claims.

14.5 For technology vendors

93. Design for defense-scale organizations, including transparent pricing and low-bandwidth environments.
94. Support open export, provenance, audit logs, role-based access, and deletion controls.
95. Disclose material limitations, version changes, model use, and validation evidence.
96. Do not use confidential defense data for model training without explicit, informed, and legally valid authorization.

97. Preserve human-review pathways and allow teams to trace a summary or alert to its underlying source.

15. Research Agenda

The field lacks sufficient empirical evidence about which investigative structures most improve defense quality. A coordinated research programme should examine:

98. the relationship between investigator staffing, timing of engagement, and case outcomes;
99. how digital discovery volume changes investigator hours and required competencies;
100. whether structured discovery assurance finds material omissions or errors earlier;
101. the effect of investigator involvement on release, plea comprehension, sentencing alternatives, and client participation;
102. error rates in defense uses of automated transcription, translation, document review, and generative AI;
103. differences among staff-investigator, contract-investigator, regional-service, and specialist-pool models;
104. the experiences of witnesses and clients contacted by defense investigators; and
105. the minimum documentation needed for reproducible, ethical investigation without excessive burden.

Studies should avoid treating dismissal or acquittal as the only valid success. Randomized designs may be ethically or operationally difficult, but phased implementation, matched-case comparisons, interrupted time series, blinded file review, and simulation can provide useful evidence. Research must protect privileged strategy, confidential client information, personnel fairness, and defense independence.

16. Limitations

This article is a conceptual synthesis, not an empirical test of a new staffing model. It focuses on U.S. criminal defense and cannot capture the law of every state, tribal system, territory, military forum, or federal district. Several cited professional standards are influential but are not themselves binding law unless adopted or used by the relevant authority. Supreme Court doctrine defines constitutional floors, while professional standards may describe more demanding practice.

The term “investigator” encompasses people with different licensing, employment, education, authority, and expertise. Recommendations must be adapted to office size, case type, client needs, collective bargaining, security, and local law. Technology changes quickly; current tools and guidance will require updating. The article also does not resolve contested questions about privilege, discovery of defense-

created materials, deceptive online practices, or admissibility of emerging AI evidence. Those questions require jurisdiction-specific analysis.

17. Conclusion

The private or defense investigator is not disappearing into software. The role is becoming more human and more technical at the same time. Modern investigators must still earn trust at a kitchen table, notice what a police interview missed, walk a scene, and find the person nobody else located. They must also understand that a report may be a derivative product, that a timestamp may not mean what it appears to mean, that a discovery production may be complete in volume but incomplete in usability, and that an AI summary is a lead rather than a witness.

The emerging investigator is best understood as an evidence-system integrator and adversarial reliability officer. This professional develops independent facts, tests the prosecution's pipeline, coordinates preservation and expertise, reconstructs context, supports individualized mitigation, and reports uncertainty to counsel. The function is not partisan distortion. Properly performed, it is a disciplined contribution to the accuracy of an adversarial system.

The criminal justice system should respond by engaging investigators earlier, defining defense-specific competencies, funding multidisciplinary capacity, governing AI, improving digital discovery, and measuring investigative quality. A right to counsel that cannot independently test facts is thinner than it appears. Treating investigation as a core service is therefore not merely an occupational upgrade. It is an institutional commitment to decisions based on evidence that has been preserved, understood, challenged, and placed in context.

References

106. U.S. Constitution, amend. VI. Constitution Annotated, Library of Congress. https://constitution.congress.gov/constitution/amendment-6/

107. *Gideon v. Wainwright*, 372 U.S. 335 (1963). U.S. Government Publishing Office. https://www.govinfo.gov/app/details/USREPORTS-372/USREPORTS-372-335

108. *Strickland v. Washington*, 466 U.S. 668 (1984). United States Reports, Library of Congress. https://tile.loc.gov/storage-services/service/ll/usrep/usrep466/usrep466668/usrep466668.pdf

109. American Bar Association. (2017). *Criminal Justice Standards for the Defense Function* (4th ed.), especially Standards 4-4.1 to 4-4.3. https://www.americanbar.org/groups/criminal_justice/resources/standards/defense-function/

110. 18 U.S.C. § 3006A, including subsection (e), investigative, expert, and other services. Office of the Law Revision Counsel. https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title18-section3006A

111. Administrative Office of the U.S. Courts. *Guide to Judiciary Policy, Vol. 7A, Chapter 3: Authorization and Payment for Investigative, Expert, or Other Services*. https://www.uscourts.gov/administration-policies/judiciary-policies/guidelines-administering-cja-and-related-statutes/chapter-3-ss-310-general

112. Bureau of Justice Statistics. (2016). *State-Administered Indigent Defense Systems, 2013*. https://bjs.ojp.gov/library/publications/state-administered-indigent-defense-systems-2013

113. American Bar Association. (2023). *Ten Principles of a Public Defense Delivery System*. https://www.americanbar.org/groups/legal_aid_indigent_defense/indigent_defense_systems_improvement/standards-and-policies/ten-principles-pub-def/

114. Pace, N. M., Brink, M. N., Lee, C. G., & Hanlon, S. F. (2023). *National Public Defense Workload Study*. RAND Corporation. https://www.rand.org/pubs/research_reports/RRA2559-1.html

115. U.S. Bureau of Labor Statistics. (2025). *Private Detectives and Investigators: Occupational Outlook Handbook*. https://www.bls.gov/ooh/protective-service/private-detectives-and-investigators.htm

116. American Bar Association. *Model Rule of Professional Conduct 5.3: Responsibilities Regarding Nonlawyer Assistance*. https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_5_3_responsibilities_regarding_nonlawyer_assistant/

117. National Institute of Standards and Technology. *Digital and Multimedia Evidence*. https://www.nist.gov/forensic-science/digital-and-multimedia-evidence

118. Ayers, R., Brothers, S., & Jansen, W. (2014). *Guidelines on Mobile Device Forensics* (NIST SP 800-101 Rev. 1). https://doi.org/10.6028/NIST.SP.800-101r1

119. American Bar Association. (2020). *Criminal Justice Standards for Discovery* (4th ed.). https://www.americanbar.org/groups/criminal_justice/resources/standards/discovery/

120. Administrative Office of the U.S. Courts. *Federal Rules of Criminal Procedure*. https://www.uscourts.gov/forms-rules/current-rules-practice-procedure/federal-rules-criminal-procedure

121. Department of Justice & Administrative Office of the U.S. Courts Joint Working Group on Electronic Technology in the Criminal Justice System. (2012). *Recommendations for Electronically Stored Information Discovery Production in Federal Criminal Cases*. https://www.justice.gov/sites/default/files/usao/legacy/2012/09/24/usab6005.pdf

122. National Institute of Standards and Technology. (2022). *Digital Investigation Techniques: A NIST Scientific Foundation Review* (NISTIR 8354). https://www.nist.gov/spo/forensic-science-program/foundation-studies/digital-investigation-techniques-nist-scientific

123. American Bar Association. (2003). *Guidelines for the Appointment and Performance of Defense Counsel in Death Penalty Cases*, Guideline 10.4. https://www.americanbar.org/groups/committees/death_penalty_representation/resources/aba_guidelines/2003-guidelines/2003-guideline-10-4/

124. American Bar Association Standing Committee on Ethics and Professional Responsibility. (2024). *Formal Opinion 512: Generative Artificial Intelligence Tools*. https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/ethics-opinions/aba-formal-opinion-512.pdf

125. National Institute of Standards and Technology. (2023). *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*. https://doi.org/10.6028/NIST.AI.100-1

126. Autio, C., et al. (2024). *Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile* (NIST AI 600-1). https://doi.org/10.6028/NIST.AI.600-1

127. National Institute of Standards and Technology. (2022; updated 2026). *Digital Evidence Preservation: Considerations for Evidence Handlers*. https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt/digital-evidence

128. Office of the United Nations High Commissioner for Human Rights & Human Rights Center, University of California, Berkeley. (2022). *Berkeley Protocol on Digital Open Source Investigations*. https://www.ohchr.org/sites/default/files/2022-04/OHCHR_BerkeleyProtocol.pdf

129. Federal Trade Commission. (2026 revision). *Fair Credit Reporting Act*. https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act

130. U.S. Department of Justice. (2022; updated 2025). *Charging Policy for Computer Fraud and Abuse Act Cases*. https://www.justice.gov/jm/jm-9-48000-computer-fraud

131. Administrative Office of the U.S. Courts. *Federal Rules of Evidence*. https://www.uscourts.gov/forms-rules/current-rules-practice-procedure/federal-rules-evidence

132. *Brady v. Maryland*, 373 U.S. 83 (1963). U.S. Government Publishing Office. https://www.govinfo.gov/app/details/USREPORTS-373/USREPORTS-373-83

133. *Kyles v. Whitley*, 514 U.S. 419 (1995).

134. Bureau of Justice Statistics. (2024). *Survey of Public Defenders Pilot Report*. https://bjs.ojp.gov/library/publications/survey-public-defenders-spd-pilot-report

135. Scientific Working Group on Digital Evidence. (2025). *Best Practices for Computer Forensic Examinations* (SWGDE 18-F-001-2.0). https://www.swgde.org/documents/published-complete-listing/18-f-001-swgde-best-practices-for-computer-forensic-examination/

Declarations

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Conflicts of interest: The author declares no conflict of interest.

Data availability: No empirical data were generated for this conceptual article. Any future evaluation instruments should be released where ethically, legally, and operationally permissible.

Ethics statement: No human participants or personal data were used in preparing this conceptual article. Future human-participant research proposed in the research agenda would require appropriate institutional ethics review.

Legal scope statement: This article provides general academic analysis and is not legal advice. Licensing, discovery, privacy, recording, professional-conduct, privilege, and investigative rules vary by jurisdiction and case.

Use of generative AI: The author used generative artificial intelligence as an assistive writing tool to help address difficulties associated with dyslexia, including support with spelling, grammar, sentence structure, organization, and clarity. The author developed the article's arguments, reviewed and revised the generated text, checked the cited sources, and takes full responsibility for the accuracy, originality, analysis, and final content. Generative AI was not used to generate or analyze empirical data.