



AI, Metadata and the Future of Evidence

**Women of Class 2026
Quebec City
January 2026**

At the Forefront of **Discovery**

Class actions present unique discovery challenges in modern litigation. Frequently, plaintiffs' counsel must manage voluminous productions from defendants, who typically have greater resources and technological capacity. At the same time, new threats from AI-generated evidence cast doubt on a long-standing evidence principle that digital records can be trusted.

Last year, we focused on resisting discovery gamesmanship and taking control of the discovery process. This year, we turn to the next frontier, the integrity and reliability of digital evidence. As manipulated and synthetic data proliferate, the trustworthiness of evidence is increasingly at risk. This paper provides class action counsel with practical guidance to respond effectively.

We begin by considering the UK's Horizon scandal as a cautionary example of what can go wrong when reliability is simply assumed. We then examine the legal framework set out in the *Canada Evidence Act* and the Canadian General Standards Board (CGSB)'s "Electronic Records as Documentary Evidence" standard to understand how Canadian courts are guided to approach electronic records.¹ We will then look at AI-generated evidence and expert evidence that relies on AI for analysis. Finally, we will examine issues arising from hyperlinked attachments. Throughout, we offer strategies to help counsel secure better outcomes.

Lessons from the UK Horizon Scandal

The United Kingdom's Post Office Horizon scandal illustrates what can happen when digital evidence is presumed to be reliable. For more than 15 years, the Horizon accounting software generated discrepancies that were treated as proof of theft and fraud. Hundreds of sub-postmasters were wrongfully prosecuted and convicted. Many were financially ruined; some were imprisoned; and at least four died by suicide. It was subsequently determined that the software produced errors calling into question all the convictions.

The leading appellate decision, *Hamilton & Others v Post Office Ltd*², quashed dozens of convictions, finding that the prosecutions were an abuse of process because the reliability of the Horizon system had never been properly investigated. Courts presumed the computer was always right, and there was no scrutiny of the system's flaws.

¹ The Canadian General Standards Board (CGSB) is a federal standards-writing body accredited by the Standards Council of Canada which develops consensus-based national standards across technical and professional fields. Its standards are authoritative because they reflect multi-stakeholder expertise and are widely recognized by courts and regulators as benchmarks for best practices, including in records management and electronic evidence.

² [2021] EWCA Crim 577

The Horizon scandal underscores the unfairness of placing the burden onto parties without access to the relevant systems. Once the presumption of reliability applied, the burden fell on individuals to prove the computer system was faulty, which is an impossible task without access to technical expertise or system-level information. The UK is now considering reforms that would flip the analysis, requiring courts to scrutinize reliability when challenged and mandating disclosure of audit trails, system controls, and provenance.

In Canada, the *Canada Evidence Act* [CEA]³ framework creates the very same risk that led to the Horizon wrongful convictions.

The Canada Evidence Act and the Presumption of Reliability

Sections 31.1 to 31.8 of the CEA establish a statutory shortcut for electronic evidence. Section 31.2(1) provides that a record generated or stored by an electronic system that “operated properly” at the relevant time is presumed to be authentic and accurate. Once invoked, this presumption shifts the burden to the other side to prove the record is unreliable.

This mechanism promotes efficiency, particularly in cases involving massive volumes of electronic records. It avoids turning every digital document into a mini trial on authenticity. But it also has significant consequences in the class action context: defendants who control the systems that generate evidence enjoy a strong evidentiary advantage, while plaintiffs are left to challenge reliability without necessarily having the access or technical expertise to do so.

In the face of this presumption of authenticity, class counsel should argue that proportionality includes procedural fairness. Specifically, parties who rely on digital evidence must disclose enough metadata, audit logs, and system documentation to allow meaningful testing of reliability. This is especially important in cases where digital records form the backbone of liability or damages.

The CGSB Standard, Auditability and Metadata

The CGSB’s “Electronic Records as Documentary Evidence” standard⁴ provides a national framework for ensuring that electronic records are reliable, accurate, authentic, and therefore capable of being admissible as legal evidence. It emphasizes proving system integrity and record integrity to satisfy rules of authenticity, best evidence, and the business records exception in the CEA. While not legally binding, it is highly persuasive. Courts may consider compliance with the standard as evidence of proper records management.⁵

³ RSC 1985, c C-5

⁴ Originally titled CGSB-72.34-2017, the standard was updated in 2024 and is now CAN/CGSB-72.34-2024.

⁵ See CEA, s. 31.5

Key features of the standard include:

- a. **Auditability:** every record should be supported by metadata and audit trails that demonstrate its origin, integrity, and chain of custody.⁶
- b. **System Controls:** organizations should have policies and safeguards in place to prevent unauthorized alteration.⁷
- c. **Retention and Preservation:** records must remain accessible and trustworthy over time, including during litigation holds.⁸

For class action counsel, CGSB-72.34 is a valuable advocacy tool. Digital evidence depends on its metadata and audit trails, but in Canada these are often disclosed only if counsel specifically asks for them. For class actions, where the imbalance of power and resources is most acute, plaintiffs' counsel should make metadata central to discovery requests. Auditability, the ability to demonstrate how, when, and by whom a record was created, stored, or altered, should be treated as essential, not optional.

Demanding production of metadata and audit trails in line with the standard transforms abstract reliability into something verifiable. It gives courts a benchmark against which to measure whether records are trustworthy, rather than relying solely on the statutory presumption in the CEA.

There might be occasions when the opponent's entire system needs to be challenged for lack of integrity, and other times it may only be one record that is suspect. Attached as Appendix A are two charts laying out some helpful arguments to challenge an entire IT system (system integrity) or to challenge individual records (records integrity).

We are frequently confronted with occasions to use such arguments. This often happens when evidence comes from Crown or regulatory investigations and is obtained through "Wagg motions"⁹. In our experience, data seized or received by the Crown or a regulator is often not properly preserved, even if the collection was done appropriately. In one case we have, the Crown failed to preserve family relationships between documents, they complicated the search process by stripping metadata which is no longer available, and they further impeded access to the evidence by changing document titles. This mishandling of evidence is now part of an abuse of process application to get serious criminal charges dismissed as against our client.

⁶ CGSB-72.34-2024, Policy 6

⁷ *ibid.*, Policy 4

⁸ *ibid.*, Policy 9

⁹ Wagg motions are a specific type of court motion that seeks the production of documents, such as police or Crown files, from a non-party to a civil lawsuit.

Evidentiary Risks and the Explainability of AI Systems

AI systems have created a whole new set of problems related to reliability. If left untested, AI tools could disproportionately disadvantage plaintiffs in class actions, undermining both fairness and access to justice.

If the inner workings of an AI system are explainable, then it is easier to get people to trust the results and find the system to be reliable. However, AI systems often, and increasingly, generate outputs through opaque processes that are not easily explained, even by experts. This is known as the “black box” problem.

Canadian criminal justice research reinforces the problematic nature of the AI black box. The Law Commission of Ontario¹⁰ has warned that black box algorithms raise risks to fundamental Charter rights, including s. 7 (life, liberty, and security of the person) and s. 11(d) (fair trial guarantees), if accused persons cannot meaningfully challenge AI-generated evidence. But meaningful challenge does not always require technical explainability.

Full explainability is often impossible, prohibitively costly, and not very helpful to judges or juries. Instead, courts should assess AI evidence the way they treat other accepted black boxes, such as pharmaceuticals whose mechanisms of action are unknown or forensic expertise based on experience. The focus should be on inputs and outputs, not on inner workings. Was the methodology peer-reviewed? What is the error rate? Has the output been independently verified? In law, what matters is not explanation but justification, that is, whether the result can be grounded in legal norms and tested under the rules of evidence. For that reason, admissibility should require transparency about inputs and outputs, disclosure of system limitations, and evidence of testing and error rates. These are the safeguards that allow counsel to probe reliability in practice.

While there is not yet a Canadian case on point, a recent American appellate case recognized the limits of explainability. In *State v Carr*¹¹, the Court of Appeals in the Ninth Judicial District found that the AI-generated evidence the state tried to proffer was not admissible because it failed to meet evidentiary standards. The decision recognized the challenge of AI’s black box but did not focus on it. Instead, the court found that while full technical explainability may be unrealistic, due process requires that AI evidence be capable of meaningful challenge through disclosure of methodology, inputs, and limitations. Without such safeguards, admitting AI evidence risks violating the accused’s rights.

In civil discovery, similar risks apply. Plaintiffs must insist on disclosure of metadata, audit logs, and system documentation so that AI-generated or system-based evidence can be tested. Procedural fairness does not require prying open the black box; it requires ensuring that the outcomes of these systems can be scrutinized against legal standards.

¹⁰ Law Commission of Ontario, “AI at Trial and on Appeal”, AI in Criminal Justice Project, Paper 4, April 2025 [See <https://www.lco-cdo.org/en/our-current-projects/crimai/>]

¹¹ 2024-Ohio-4471

In the class action context, we see challenges with AI-generated evidence incorporated into expert reports. Increasingly, experts rely on AI tools to prepare portions of their analyses. The reliability of an expert opinion depends on the foundation of admissible evidence. If AI is used, courts must be assured that the expert's conclusions are rooted in actual evidence rather than unverifiable algorithmic outputs. The maxim "garbage in, garbage out" is apt here. If the AI system is trained on or fed flawed, incomplete, or inadmissible data, then the resulting analysis will be equally compromised. Ensuring that expert reports remain anchored in admissible, verifiable evidence is therefore critical to maintaining their probative value.

Take one of our current cases as an example. Opposing party's expert report quotes excerpts from alleged productions, but the entire documents which from the excerpts allegedly came are not specified. First, we are faced with the question of whether the excerpts actually come from documents in the production set. Further, even if they do come from the productions, we query whether the AI tool used by the expert had the proper inputs: Did the expert merely feed the algorithm selected quotes from the documents instead of the entirety of each admissible document? If the inputs can be challenged as being too selective, we might be in the position to successfully challenge the output.

Attached as Appendix B is a table which sets out some of the issues that you might want to consider when AI-generated evidence is proffered.

Hyperlinked Attachments

Hyperlinked attachments, sometimes called "modern attachments", are files stored in the cloud (such as OneDrive, Google Drive, or SharePoint) that are shared by inserting a link into an email or chat message, rather than attaching a static copy of the file. Where you have a traditional attachment, that attachment is preserved as part of the email itself, creating a fixed snapshot of the document the moment it was sent. Conversely, a hyperlinked attachment points to a live document that can be changed, moved, or deleted at any time. What appears to be a minor change in technology can create major evidentiary problems if the data is not collected properly and promptly.

Unlike traditional attachments which are embedded and are automatically captured and indexed along with the parent email, hyperlinked documents require a specific approach to be collected. This means that relevant content may be overlooked if collection workflows do not properly identify and collect linked files. As a result, critical evidence may never be considered, despite being within the control of the producing party. This is compounded by collecting using keywords which would not search linked attachments.

Even where the linked attachments are collected, problems can arise. A link points to a live file that may have been altered, moved, or deleted after the message was sent. This means the version collected later may differ from the one originally shared. This makes it far more difficult to prove what the

recipient saw and when, and it also breaks the usual family relationship between a message and its attachments that is critical for preserving context.

Recently, we have begun to see solutions. For example, Microsoft now allows for the ability to collect the hyperlinked document as it was initially shared or all prior versions of the linked document, but only if the client has a premier license. There are other options to properly collect hyperlinked documents. The key point is that it is crucial that the issue be explicitly addressed in the discovery plan.

While there is no Canadian case law regarding hyperlinked attachments yet, there are some instructive decisions from the US. In an early decision from 2021, *Nichols et al v. Noom Inc. et al*¹², the court held that hyperlinks in emails were not automatically attachments under the agreed protocol, prioritizing proportionality over completeness. By contrast, more recently, in *In re Uber Techs., Inc. Passenger Sexual Assault Litig.* [Uber]¹³, the court interpreted “attachments” broadly to include modern attachments, though it acknowledged technological limits on producing contemporaneous versions. Similarly, in the *StubHub Refund Litigation*¹⁴, the court first required hyperlinked documents to be treated as attachments under the protocol, only to later relax that requirement when defendants showed the burden of compliance.¹⁵ These inconsistent rulings in the US illustrate both the unsettled legal landscape in different jurisdictions and the risks of selective disclosure.

Among these US decisions, we expect the Uber decision to be in line with upcoming Canadian court decisions in the area. US decisions often turn on what was agreed to in a protocol or what was specifically requested by opposing counsel. In contrast, in Canadian jurisdictions aside from Quebec, litigants have positive obligations to produce relevant (and, in some jurisdictions, material) documents. Our courts are unlikely to overlook the failure to capture hyperlinked documents if those are expected to be relevant to the issues in dispute, especially now that technologies are emerging to properly collect them.

Further, proper collection of hyperlinked documents goes directly to the requirements of system integrity under the CEA, s. 31.5, which contemplates proof of the procedures and practices by which records are created and maintained. Likewise, the CGSB-72.34-2024 standard emphasizes that metadata, family relationships, and audit trails are essential to establishing record integrity. If hyperlinked files are ignored or their contemporaneous versions cannot be shown, the evidentiary foundation required for admissibility is undermined.

¹² 2021 WL 948646 (S.D.N.Y. 2021)

¹³ 2024 WL 1772832 (N.D. Cal. 2024)

¹⁴ 2024 WL 2305604 (N.D. Cal. 2024)

¹⁵ StubHub showed that, despite considerable effort (hundreds of hours plus hiring an outside e-discovery vendor), it was unable to locate many of the linked/hyperlinked documents. Most of the hyperlinks were broken or no longer worked.

Conclusion

Deepfakes and AI outputs capture public attention, but the Horizon scandal reminds us that even conventional systems can cause devastating injustice when reliability is taken for granted. The central lesson is that all technology, whether basic accounting software or advanced AI, must be treated as fallible and therefore open to testing.

For class counsel, this means insisting that digital evidence be transparent, auditable, and subject to meaningful challenge. The CEA may still presume authenticity, but plaintiffs' lawyers can and should demand the metadata, audit trails, and system documentation necessary to test that presumption. Only by pressing for this level of disclosure can we protect fairness, preserve access to justice, and ensure that technology serves the truth rather than obscuring it.

Appendix A

Arguments to challenge system integrity and record integrity

A. System integrity

System Integrity Arguments (IT system as a whole)
Intermittent compliance: Standard requires continuous compliance with policies and procedures; partial or reactive compliance undermines system integrity.
Authentication failures: No reliable process to prove that the system consistently produces authentic records (e.g., no records management (RM) manual or IT system documentation).
Weak records management program: Lack of a formal RM policy/manual, unclear Records Officer authority, or inconsistent classification and retention procedures.
Inadequate audit trails: Missing, alterable, or incomplete logs make it impossible to reconstruct events, showing poor control over the system.
Security/control failures: Weak access controls, encryption lapses, or poor backup validation allow unauthorized access or tampering.
Unreliable conversion/migration: Poorly documented or unverifiable digital conversions/migrations create uncertainty that system processes preserve record accuracy.
Emerging tech risks: Use of AI, social media, or mobile devices without risk assessments creates uncertainty about trustworthiness.
Legal hold failures: Inability to suspend destruction/disposition when litigation is anticipated undermines confidence in overall system preservation.

B. Record integrity

Record Integrity Arguments (individual records)
Altered content: Evidence that the record has been modified, corrupted, or otherwise changed from its original state defeats record integrity.
Missing or inconsistent metadata: If creation dates, authorship, or version history are incomplete or contradictory, authenticity and identity are undermined.
Multiple versions without version control: Absence of documented versioning procedures raises doubt about which copy is authoritative.
Breaks in chain of custody: Inability to show how the record was captured, stored, transferred, or preserved creates doubt about whether it is complete and unaltered.
Inconsistent business use: If an organization does not actually rely on the record in its ordinary course of business, its reliability as evidence is questionable.
Lack of contemporaneity: Records not created, received, or stored within a reasonable time after events may lack reliability.
Data entry errors: Records entered outside normal business processes, or without documented procedures, may be inaccurate.
Incomplete preservation: If a record or its supporting metadata was deleted or destroyed prematurely, its integrity cannot be demonstrated.

Appendix B

Challenges to AI generated evidence

Category	Issues for Challenge	Key Considerations
Threshold Admissibility	• Relevance • Authentication	– Does the AI output address a material issue? – Who sponsors and authenticates it?
Reliability of the AI System	• Explainability / transparency • Validation and testing • Bias and training data • Updates / versioning • Auditability	– Can the process be explained or is it a 'black box'? – Has the system been validated and error-rates measured? – Was the training data biased or incomplete? – Was the same version used consistently? – Is there a reproducible audit trail?
System & Records Integrity	• Metadata preservation • Tampering risks	– Is metadata intact to show creation and alterations? – Could the output have been manipulated or “deepfaked”?
Collection & Discovery Concerns	• Reproducibility • Completeness • Methodology	– Can the result be replicated with the same inputs? – Were all relevant inputs disclosed? – Were collection and preprocessing transparent and defensible?
Fairness & Prejudice	• Right to challenge • Undue prejudice • Access to comparable tools	– Can the opposing party meaningfully cross-examine the AI? – Will the novelty/objectivity of AI overawe the trier of fact?¹⁶ – Does one party have exclusive access to proprietary systems?
Legal & Ethical Standards	• Compliance with statutory frameworks	– Does the evidence align with Canada Evidence Act s.31.5 and provincial rules? – How have courts treated AI/digital

¹⁶ AI systems often present results in a highly technical, statistical, or authoritative form. Because of this, there is a danger that judges or juries may treat the output as inherently more reliable than it actually is. This is sometimes referred to as “automation bias”.

Category	Issues for Challenge	Key Considerations
	• Case law precedent • Professional responsibility	evidence to date? – Has counsel met duties of competence and candour?