HEURISTICA
DISCOVERY COUNSEL LLP

Reconsidering the Presumption of Reliability for Digital Evidence in Canadian Law - A Cautionary Reflection on the UK Horizon Scandal

At the Forefront of Discovery

Executive Summary

The Canadian legal framework for the admissibility of electronic evidence is grounded in a presumption that digital records generated or stored by a functioning electronic system are reliable. Codified in sections 31.1 to 31.8 of the *Canada Evidence Act* (CEA), this presumption was introduced in 2000 to accommodate the growing volume of digital records and to promote efficiency in legal proceedings.[1]

However, recent developments in the United Kingdom - most notably the *Post Office Horizon* scandal - have exposed the dangers of over-reliance on such presumptions. In that case, faulty computerized accounting data led to the wrongful prosecution of over 900 sub-postmasters. The court cases, criminal convictions, imprisonments, loss of livelihoods and homes, debts, and bankruptcies led to significant personal suffering - stress, illness, family breakdowns - and, most tragically, at least four suicides linked to the scandal.[2] The UK is now proposing legislative amendments to remove the automatic assumption of system reliability and to require courts to assess the integrity of computer-generated evidence more rigorously.

This paper invites Canadian lawmakers, judges, and legal practitioners to critically evaluate the continued appropriateness of the CEA's presumption in light of contemporary technological and evidentiary realities. It advocates for a measured reconsideration of whether this presumption still serves its intended purpose or whether it may now expose the justice system to unintended risks of error and unfairness.

While this mechanism facilitates judicial efficiency and access to justice - particularly in cases involving voluminous digital records - it has also led to a degree of evidentiary complacency.

---

[1] Presumption of integrity
31.3 For the purposes of subsection 31.2(1), in the absence of evidence to the contrary, the integrity of an electronic documents system by or in which an electronic document is recorded or stored is proven
(a) by evidence capable of supporting a finding that at all material times the computer system or other similar device used by the electronic documents system was operating properly or, if it was not, the fact of its not operating properly did not affect the integrity of the electronic document and there are no other reasonable grounds to doubt the integrity of the electronic documents system;
(b) if it is established that the electronic document was recorded or stored by a party who is adverse in interest to the party seeking to introduce it; or
(c) if it is established that the electronic document was recorded or stored in the usual and ordinary course of business by a person who is not a party and who did not record or store it under the control of the party seeking to introduce it.

[2] For official details, see https://www.gov.uk/government/publications/post-office-horizon-system-offences-bill-supporting-documents/horizon-scandal-factsheet-post-office-horizon-system-offences-bill?utm_source=chatgpt.com.

1. Introduction: The Statutory Shortcut for Digital Evidence

In its current form, the CEA provides that a document in electronic form is presumed to be authentic and accurate if it is produced or maintained within an electronic document system that "operated properly" at the relevant time. The burden to disprove this presumption falls to the opposing party. While this mechanism facilitates judicial efficiency and access to justice - particularly in cases involving voluminous digital records - it has also led to a degree of evidentiary complacency.

When introduced, this presumption responded to the operational needs of an increasingly digitalized legal environment. Courts needed a practical means of admitting electronic records without turning each document into a contested mini-trial. The assumption that electronic systems generally function correctly was widely accepted as a reasonable compromise.

However, that assumption no longer appears as reliable as once seemed.

2. Lessons from the UK: The Horizon Scandal

The United Kingdom is now reckoning with the consequences of its own evidentiary shortcut. The *Post Office Horizon* scandal involved a computerized accounting system (Horizon) used to manage branch transactions. Between 1999 and 2015, discrepancies generated by the system - often the result of bugs, user interface issues, or system errors - were treated as proof of fraud or theft.

Relying on the presumption that Horizon was working correctly, the Post Office prosecuted hundreds of sub-postmasters. Many were convicted. Some were imprisoned. Decades later, the system's flaws were exposed, leading to widespread calls for redress, apologies, and legislative reform.

Critically, although the presumption of system reliability was not always formally cited during trials, its underlying logic was deeply embedded in the decision-making process. Courts assumed that if the computer said something occurred, it probably did - placing an unrealistic burden on accused individuals to disprove a presumption they had neither the expertise nor resources to contest.[3]

[3] "The evidential rules relating to computer-generated evidence do not take proper account of the reality that software is inherently "buggy". As Bates vs Post Office Ltd (No. 6: Horizon Issues) [2019] EWHC 3408 (QB) shows, this can lead to the courts accepting computer-based evidence without assessing to any significant extent whether the software includes errors that could have an impact on the evidentiary quality of the computer-generated evidence that is being presented. Roger Bickerstaff, Computer-Generated Evidence – Time for a New Approach. 2024. https://www.twobirds.com/en/insights/2024/uk/computer-generated-evidence-time-for-a-new-approach.

3. The UK's Legislative Response

In response, the UK House of Lords is now considering amendments to the *Data (Use and Access) Bill*[4] that would upend the traditional presumption. Among the proposed clauses championed by Lord Arbuthnot and others are the following stipulations:

- Electronic evidence is only admissible if its reliability is not challenged, if the court finds it cannot reasonably be challenged, or if the court is satisfied the system is reliable. Parties must have a clear procedural opportunity to challenge such evidence.
- Reliability determinations may include factors such as audit trails, software security, regulatory oversight, and operational controls.

This proposed reform seeks to restore a basic evidentiary principle: that parties who introduce potentially determinative electronic evidence should bear the burden of establishing its reliability when questioned.[5]

4. The Canadian Context: Are We Vulnerable to Similar Risks?

Canada has not experienced a public scandal on the scale of Horizon, but the underlying conditions are present:

- **Presumption of integrity**: Under section 31.2(1) of the CEA, the system's proper operation creates a presumption of record reliability.
- **Shifting burden**: Once the presumption is established, the burden shifts to the opposing party to disprove integrity - often without access to the system or expertise required to do so.
- **Judicial deference to technology**: As digital systems become more complex and opaque, courts and counsel may lack the technical literacy to identify and challenge potential flaws.
- **Absence of systemic safeguards**: There is no formal requirement for courts to examine metadata, audit logs, access controls, or digital chain of custody unless an issue is raised.

These factors, taken together, suggest that the Canadian system might be insufficiently prepared to detect or prevent injustice in cases where digital records are flawed, manipulated, or misunderstood.

---

[4] https://bills.parliament.uk/bills/3825.

[5] See Nick Wallis, Proposed amendment to legal presumption about the reliability of computers. 2024. https://www.postofficescandal.uk/post/proposed-amendment-to-legal-assumption-about-the-reliability-of-computers/.

These factors, taken together, suggest that the Canadian system might be insufficiently prepared to detect or prevent injustice in cases where digital records are flawed, manipulated, or misunderstood.

5. A Call for Reflection

This paper does not argue for the immediate repeal of the CEA's presumption. Nor does it suggest that digital evidence is inherently untrustworthy. Rather, it urges a national conversation about whether our current evidentiary rules strike the right balance between efficiency and fairness.

Possible areas for examination include:

- **Clarifying the scope of the presumption**: Should it apply to all electronic evidence, or only to routine business records?
- **Introducing rebuttable thresholds**: Could a system be required to meet baseline reliability criteria before the presumption applies?
- **Formalizing disclosure and challenge rights**: Should rules require disclosure of system architecture, audit logs, or data provenance where evidence is challenged?
- **Improving digital literacy within the legal system**: Should more training or expert support be available to judges and counsel to interrogate digital evidence more effectively?

6. Conclusion: Avoiding the Next Horizon

The UK's experience should serve as a cautionary reminder: legal presumptions that once appeared benign can become dangerous when left unexamined in the face of technological change.

Canada has the opportunity to learn from these events and proactively strengthen its evidentiary framework. By doing so, we can reduce the risk of systemic injustice, restore balance to the burden of proof, and uphold public confidence in the administration of justice in the digital age.

A conversation is overdue.

About Heuristica Discovery Counsel

Heuristica Discovery Counsel LLP ("Heuristica") is Canada's only national law firm that is focused exclusively on electronic evidence. Heuristica has significant experience and expertise in the areas of electronic evidence, policy and procedure in civil, criminal and regulatory proceedings and was recently awarded a Chambers & Partners ranking. Heuristica has assisted defence counsel, regulators, investigators, police, and prosecutors in managing evidence and developing leading disclosure practices in complex criminal and regulatory proceedings.

Crystal O'Donnell

Crystal is CEO and the founding partner of Heuristica Discovery Counsel LLP. She has extensive experience as litigation and eDiscovery counsel having practiced with a leading Canadian law firm and the Ontario Ministry of the Attorney General, Crown Law Office. Crystal's practice areas included malicious prosecution and claims against police and Crowns regarding the criminal process. In addition, she was a leading policy counsel for the disclosure of criminal investigation materials in collateral legal proceedings.

Crystal is past Chair of the Board of Directors of CanLII, a sitting member of the Ontario Rules of Civil Procedure Committee, Subcommittee on Artificial Intelligence, and the Ontario Bar Association committee on Artificial Intelligence. Crystal is recognized as a leading eDiscovery counsel in Who's Who Legal, Canada and Global, and was the recipient of the Ontario Bar Association President's Award in 2020 for contributions to the advancement of justice in her roles involving legal technology.