HEURISTICA
DISCOVERY COUNSEL LLP

Solving the Hard Questions of Criminal Disclosure

At the Forefront of Electronic Evidence

Solving the Hard Questions of Criminal Disclosure

Digital evidence is revolutionizing criminal investigations, demanding that police, Crown and defence embrace new technological competencies. This urgent shift is equally crucial in quasi-criminal and regulatory arenas. To accelerate this adaptation, this paper suggests that valuable insights can be drawn from longstanding eDiscovery practices in civil procedure.

Every participant in the criminal justice system knows that collecting, reviewing, disclosing, and receiving large volumes of digital evidence are daunting tasks that directly impact investigations, timelines, and *Charter* rights. Adding to the challenges of evidence management and disclosure are issues of authentication and integrity - in which failure can lead to diminished evidentiary weight, or worse, inadmissibility.

There is a confluence of issues at play. While several reports and policies making sensible recommendations for reform have been released over the years,[1] it was during a time when large volumes of paper documents represented the vexing disclosure challenge. As the use of digital evidence in investigations has increased, solutions to the challenges arising from collecting, analyzing, and disclosing this evidence have been pursued independently by different police services and regions, without the benefit of centralized coordination. Finally, police, prosecutors, defence counsel and judges are still struggling and resources are limited on all sides.

We are not lacking in technology available in the market, and solutions which can decrease overall costs to the criminal justice system. But like all tools, data collection and evidence review platforms are most effective in the hands of trained experts using proven methodologies. Therein may lie a solution to the hard questions of criminal disclosure.

There are critical areas in the disclosure of electronic evidence that overlap with experiences and lessons learned in civil and regulatory proceedings. These include:

(a) the benefit of respected national guidelines and standards which could help guide the police, Crown, defence counsel and the court;
(b) the use of a variety of broadly accepted legal technologies, to help decrease timelines for meaningful disclosure, and, importantly, legal process innovation and flexible

[1] For example, the Steering Committee on Justice Efficiencies and Access to the Justice System – Report on Disclosure in Criminal Cases, June 2011. https://www.justice.gc.ca/eng/rp-pr/csj-sjc/esc-cde/rod-crc/toc-tdm.html.; Crown Prosecution Manual https://www.ontario.ca/document/crown-prosecution-manual.

legal resourcing. This will enable all participants to reduce time and costs while achieving improved access to justice incorporating proven methodologies used in regulatory, quasi-criminal and civil matters.

The Evolution of the Technology for Collecting Digital Evidence

Timely disclosure of large volumes of printed documents has arguably been a concern for many years and since 1991, disclosure obligations have been simply referenced as *Stinchcombe*[2] disclosure. But it is clear that the introduction and widespread use of email, social media, mobile devices, and data from the internet of things has completely changed the landscape. Purpose-built tools for legally defensible collection were not developed until the late 1990s,[3] and the expertise required to run them properly was in short supply.

Although an early product such as EnCase incorporated text search functionality, it was designed to find individual characters or strings which could lead investigators to relevant content, including potentially recoverable data that had been deleted by the user. It was not (nor intended to be) a full-fledged content search tool, let alone advanced analysis and disclosure. In the late 1980s and early 1990s pioneers in the industry introduced full-text and fielded search software designed specifically for the review of disclosures (and productions on the civil side), including SUPERText, Concordance and Summation.

Today the legal technology industry has mostly moved to the cloud and grown in size and sophistication to meet the rapidly growing volumes and diverse nature of the data needed for legal proceedings, regulatory requirements, and investigations. The skill levels needed to navigate modern tools have also increased significantly. We have moved on from “learn as you go” in the 1980s and 90s, using rudimentary tools, to the requirement for understanding complex functionality, professional certifications, and best practices.

Respected National Guidelines

The first decade of the new millennium brought with it several important electronic discovery developments - not just in software tools, but more importantly in process and the developments of best practices. The *Sedona Principles*, first published in the US for comment in 2002,[4] aimed to provide guidelines and best practices for managing eDiscovery in legal proceedings. It addressed the challenges posed by the increasing volume and complexity of electronically stored information

[2] *R.* v. *Stinchcombe*, 1991 CanLII 45 (SCC)
[3] Released in 1998, EnCase was the first serious tool for digital evidence investigation (it is now a product of OpenText, and has several competitors.)
[4] https://thesedonaconference.org/.

and sought to balance the need for relevant information in litigation with the burden and cost of its production. The principles significantly impacted the legal field by promoting a framework for cooperation between parties, emphasizing the importance of proportionality, and helping to shape subsequent rules and standards.

The Sedona Principles were followed in 2005 by the Electronic Discovery Reference Model (https://edrm.net/) - at first a simple diagram illustrating a proposed workflow for the eDiscovery process. Simple - but widely adopted in the industry. The EDRM has continued to develop valuable resources in eDiscovery and other areas of information governance.

In 2008 The *Sedona Canada Principles* were first published, building on its US predecessor, but incorporating Canadian civil procedure standards and norms. The third edition of the *Sedona Canada Principles*, released in 2023, updates and refines guidelines for the management of eDiscovery in Canadian legal proceedings. It addresses evolving technological advancements and substantial case law developments, emphasizing the principles of proportionality, reasonableness, and cooperation. The *Sedona Canada Principles* are now referenced in almost every civil jurisdiction in Canada by providing practical guidance, fostering consistency in electronic evidence practices across the country.

In criminal law, the standard of meaningful disclosure today is based on precedent, most notably *R. v. Dunn*, 2009 CanLII 75397 (ON SC), where the defendants argued that the data on a hard drive was not reasonably accessible because it was not properly searchable. Justice Boswell found that the database of almost 23 million images was not reasonably accessible by the defendants because the various datasets were not searchable together; parent documents were not linked with their attachments, and some datasets were not searchable at all. After this decision, further disclosure applications are often referred to as “Dunn motions,” as was the case in the notable decision, *R. v. Cuffie*, 2020 ONSC 4488.

In *Cuffie*, the Ontario Superior Court of Justice evaluated the Crown's disclosure practices in criminal proceedings, specifically addressing the issue of non-searchable PDFs. Justice Corrick stressed that for disclosure to be considered "meaningful," it must be accessible, identifiable, and sufficiently detailed to enable proper trial preparation. In this case, the disclosure encompassed approximately 7,000 documents and over 9,000 multimedia files. The non-searchability of many documents severely limited their utility, ultimately leading Justice Corrick to deem the disclosure as failing to meet the established criteria for meaningful disclosure.

In *Quebec Revenue Agency c. Morris*, 2020 QCCQ 4200, the Court of Quebec suggests that an accused must be provided with the means to review voluminous criminal case disclosure. This suggestion

likely supports the presumption that the accused may have to be provided with access to document review software to enable a complete review of voluminous criminal case disclosure.

These cases, alongside broader discussions on eDiscovery and disclosure, underscore the need for evidence disclosure standards within the Canadian criminal justice system. As digital evidence becomes ever more central to criminal proceedings, the development of comprehensive protocols and enhanced support for all stakeholders in managing disclosure is essential to maintaining the fairness of the judicial process.

Legal Process Innovation

The presumptive timeline ceilings established by *R. v. Jordan*, 2016 SCC 27 (CanLII) (of 18 months in the Ontario Court of Justice and 30 months in the Superior Court of Justice) often leave police and prosecutors limited time to deal with complex evidence and ever-increasing volumes in a meaningful manner. Innovation in disclosure and criminal procedures will be required to meet this growing tension of volumes and complexity vs. time. Effective management of the increasing volumes of electronic evidence will continue to challenge the Crown and police to meet the timelines established by *Jordan.*

Another consideration for the collection and disclosure of criminal investigation materials is the use and disclosure in other forums and collateral proceedings, such as regulatory and civil proceedings. Standardized processes and disclosure models would also provide efficiencies and mitigate risks associated with the collateral use. This includes decreasing the time required by the Crown and police on subsequent review of the investigation materials for further use.

The increasing volume of electronic evidence, types of data and communication methods, complexity of financial crimes, and the sheer proliferation of data will require advanced tools and techniques. The *Sedona Canada Principles* and the stages of the EDRM can be adapted to provide guidance and best practices for electronic evidence in criminal and quasi-criminal proceedings to help meet the timeliness requirements established in *R. v. Jordan*.

Differences and Similarities Between Criminal and Civil Law Practice

There are fundamental differences in objectives, processes, standards of proof, and outcomes between civil litigation and criminal law practice in Canada. But there are also critical overlaps in the challenges around collecting, reviewing and exchanging large volumes of electronic information. These similarities underscore the technical and procedural commonalities in handling electronic information, despite the different legal contexts and objectives of both. For example:

1. **Identification**: Both processes require the identification of relevant electronic information. This includes determining what data is pertinent to the case, whether it be emails, text messages, documents, or other forms of digital evidence. In the civil context, we conduct custodian interviews to determine the location and type of data that will need to be preserved and collected. In the criminal context, the police need to determine the same information, albeit using various legal means to obtain the information.
2. **Collection**: Both civil and criminal cases can involve the forensic collection of electronic data from computers, servers, mobile devices, cloud storage and the Internet of Things. In the civil context, the parties will often discuss and agree upon the techniques which will be used to collect and the scope of the collection, and in some Anton Piller order matters, the court will issue an order for the seizure of the evidence. In the criminal context, standardization of language for warrants and subpoenas tailored to the particular evidence and data source would be beneficial for all participants.
3. **Processing**: The collected electronic data needs to be processed to be usable in legal proceedings. This includes converting data into a reviewable format, de-duplicating, and indexing the information to allow searching. In civil proceedings, the parties often agree on the processing parameters, and these have become standardized for common document types. The criminal justice sector would benefit from standardized processing practices for electronic evidence.
4. **Review**: Both processes require an analysis of the collected data to determine what information is relevant, privileged, or otherwise subject to exclusion. The ever-increasing volume of information necessitate the use of advanced technologies to defensibly analyze the collected and seized data. Advanced technologies for the review and analysis of documents are available in the Canadian market, but in the criminal context are separate and apart from the advanced tools being developed for forensic collection and processing. Data analysis in forensics uses different tools than analysis of the content of documents.
5. **Exchange**: There is an obligation to exchange relevant information with the opposing party. In civil cases, this is part of the eDiscovery process, while in criminal cases, this is fulfilled by the Crown and police through disclosure obligations. *Dunn* and *Morris* have placed obligations on the Crown and police to provide meaningful disclosure using technology. The advantage is now that the technology has become so advanced that that this can be accomplished with little extra cost to the Crown/police with appropriate evidence review technology.

6. **Technology Use**: Both civil and criminal law practices increasingly rely on technology and specialized software for managing large volumes of electronic data, including eDiscovery platforms and digital forensic tools. There are tools currently being used by some Crowns and police that promote disclosure using RelativityOne, a market leading eDiscovery platform. Secure access by Crowns and defence counsel to the same underlying data was possible with permissions and customization created by Heuristica. This enabled the Crown to provide disclosure quickly, securely, and with the best tools available at minimal cost.

7. **Expert Involvement**: Both processes may involve experts such as forensic analysts, data management consultants, or other IT specialists to ensure the accurate identification, collection, and analysis of digital evidence. Innovation in legal process and legal process outsourcing has enabled counsel and parties in civil and regulatory proceedings to benefit from specialized legal and technical expertise. Just as a market developed to provide flexible legal service needs in the civil and regulatory context, these legal services can also be developed in the criminal sphere. Language used in search warrants can be adopted from common civil discovery exchange agreements and be tailored to the nature of the digital evidence being seized. It is important to understand the impacts of provisions dealing with time and data types, and how to protect privacy where needed.

8. **Confidentiality, Privacy and Privilege**: Both processes must consider the confidentiality and privacy of the individuals involved, ensuring that sensitive and privileged information is segregated or otherwise protected according to applicable rules. In the criminal context this is primarily protection of the accused's privilege and Charter rights, and the privacy of victims and witnesses.

9. **Proportionality**: Proportionality is principle 2 of the Sedona Canada Principles[5], which states:

> In any proceeding, the parties should ensure that steps taken in the discovery process are proportionate, taking into account (i) the nature and scope of the litigation, including the importance and complexity of the issues, interest and amounts at stake; (ii) the relevance of the available electronically stored information; (iii) its importance to the court's adjudication in a given case; and (iv) the costs, burden and delay that may be imposed on the parties to deal with electronically stored information.

Proportionality is not primarily concerned with cost or the dollar value in dispute, albeit these are important considerations. The key considerations in a proportionality analysis are the probative value of the evidence and its importance to the issues before the court. The

[5] https://thesedonaconference.org/

proportionality analysis is applicable to the criminal context, even if less weight is given to the consideration of cost to the Crown.

Authentication, Privacy and Privilege

To date in Canada, there has been little civil case law regarding the need to authenticate electronic evidence. However, in *Wang v. Liu*, 2023 BCSC 972, one of the parties relied upon screenshots of text messages. While the evidence was admitted, the Court ultimately placed no reliance on it because it could not be authenticated. The Judge made a point of saying that they were not making a finding that the evidence was fabricated, but that it could not be authenticated. This case draws attention to the increasing importance of authenticating electronic evidence and using best practices to ensure that metadata associated with electronic evidence is preserved. The ease of creating fake evidence creation and the use of generative AI will only increase the importance of authentication. While civil matters have a lower burden of proof, it is arguable that in criminal law with higher standards of proof, that it is even more important for evidence to be properly authenticated.

Social media and text messaging raise issues of privacy and potential privilege when seizing or collecting mobile devices. In the case of an Anton Piller seizure and similar circumstances, an independent counsel is appointed by the court to analyze the information seized to protect privilege and potential privacy interests. Similar processes could be developed using specialized legal resources to protect privilege and privacy rights relating to information seized in a criminal context. An approach like this will enable fulsome collection to protect metadata and the integrity of data, while at the same time putting in place the protections needed when collecting broadly.

Conclusion

Ultimately, we believe there are three critical areas in which criminal law disclosure could learn from its civil law counterpart. First, with the introduction of respected national guidelines and standards, the disclosure process from beginning to end would benefit from a high level of standardization. Second, access to not only the best available tools, but to a variety of tools, would provide all parties with benefits in terms of time and cost saved. Third, legal process innovation and the use of outsourced expert legal resources is needed to assist with legal process planning and flexible resource requirements.

Agreed-upon standards and guidelines consistent with legal and ethical obligations could streamline all processes in disclosure and likely reduce the number of legal challenges launched against prosecutors. Unlike in the civil arena, where rules of court may differ in each province and territory, criminal law (and criminal evidence law) applies in all jurisdictions. Thus, national standards would have an even greater impact than those in the civil sphere.

The sources of data that must be addressed in current matters are very broad, from decades old computers to a brand-new social media service, and now generative AI platforms. These various sources are themselves under constant change with improvements to their security and configuration. A tool that worked for months effectively may stop working if the source changes. Another tool may address the change in the source and therefore it becomes the most effective tool, for a time. The assumption that one product does it all, even with the assurances of its developer, is a recipe for underwhelming or even disastrous outcomes.

Legal process innovation and the use of outsourced legal teams has provided substantial benefits in many areas of the law. External legal resources are already being used by Governments in all areas of law, and Heuristica has encouraged and supported innovative disclosure methods. The criminal law sphere could benefit from adopting some of the flexible and innovative processes to improve meaningful disclosure.