

CANADA / JUDGMENT

R. v. Vermeer

2023 BCCA 206

COURT

British Columbia Court of Appeal

DECIDED

18 May 2023

Source: bccourts.ca · Research copy typeset by Esheria. Not court-issued or certified.

2023 BCCA 206 R. v. Vermeer

COURT OF APPEAL FOR BRITISH COLUMBIA

Citation:

R. v. Vermeer,

2023 BCCA 206

Date: 20230518

Docket: CA47820

Between:

Rex

Respondent

And

Johannes Vermeer

Appellant

Before:

The Honourable Madam Justice Newbury

The Honourable Madam Justice Fenlon

The Honourable Mr. Justice Voith

On appeal from: An order of the Provincial Court of British Columbia, dated
April 30, 2021 (conviction) (R. v. Vermeer, Chilliwack Docket 67677).

Counsel for the Appellant:

R. Mansoori-Dara

T.C. Paisana

M. Iyengar

Counsel for the Respondent:

L.A. Vizsolyi

Place and Date of Hearing:

Vancouver, British Columbia

April 3, 2023

Place and Date of Judgment:

Vancouver, British Columbia

May 18, 2023

Written Reasons by:

The Honourable Madam Justice Newbury

Concurred in by:

The Honourable Madam Justice Fenlon

The Honourable Mr. Justice Voith

Summary:

Appeal from convictions for possessing and accessing child pornography via Internet. Case was almost entirely circumstantial. Appellant alleged trial judge had failed to comply with the 'best evidence' rule as modified by s. 31 of the Canada Evidence Act (CEA); relied on hearsay in the form of file titles suggestive of child pornography to infer that the files actually contained child pornography; and in the form of a menu or 'interface' to a 'cleaner' program to find it had been deployed by appellant to delete files when he became aware of investigation into his computer use. Misapprehensions of evidence by trial judge were also asserted.

Held: Appeal dismissed. Although judge had not held voir dire(s) to decide on admissibility of "electronic documents" as defined in s. 31, she had paid attention to the reliability of the system on which documents were stored and most of the trial had been taken up with evidence as to the functionality of the appellant's computers. Three experts had been called by the Crown and there had been no suggestion the computers were not functioning properly; nor was there any suggestion that any evidence "better" than what was adduced had been available but not adduced. If file titles constituted "statements" by "persons", the principled exception to the hearsay rule would apply. File titles were also circumstantial evidence of appellant's seeking out pornographic material involving children. In any event, one of the experts had been able to view some files

directly, and trial judge viewed that material in an in camera session in order to be satisfied they contained child pornography. Defence counsel had also told court it was not necessary to see more -- the material was child pornography and the real issue at trial was the identity of the perpetrator. As for the 'cleaner' program, there was expert evidence that one of its functions was to delete files. Alleged misapprehensions asserted by appellant were not shown.

Reasons for Judgment of the Honourable Madam Justice Newbury:

- [1] The appellant Mr. Vermeer was convicted in Provincial Court of possessing and accessing child pornography between May 1 and June 11, 2012 and between March 17 and April 21, 2015, contrary to ss. 163.1(4) and (4.1), respectively, of the Criminal Code, R.S.C. 1985, c. C-46.
- [2] There is no doubt, and Mr. Vermeer agreed at trial, that the desktop computer on which the pornographic material was found was his "primary-use" computer. He had also purchased a laptop in August 2011 and used it until January 9, 2012 when he turned it over to a work colleague for his use. Both computers were password-protected and the trial judge disbelieved the appellant's evidence that his password was readily accessible by others. (See para. 128 of the judge's reasons.) Mr. Vermeer also agreed (see para. 8) that files "consistent with child pornography" were located on both computers and that the material in question met the definition of "child pornography" in s. 163.1(1) of the Code. Thus, as his defence counsel told the court below, the "real question" at trial was one of identity -- whether the Crown had proven beyond a reasonable doubt that it was Mr. Vermeer who had possessed and viewed the offending material.
- [3] The reasons of the trial judge, Judge Ormiston, are lengthy, fact-intensive and highly technical in nature for obvious reasons. Because of this and because of the particular arguments raised on appeal, I do not propose to rehearse the factual aspects of those reasons except as necessary to address the specific grounds of appeal raised in this court. I will assume the reader has read the reasons and has some familiarity with the workings of computers, applications and programs that are now ubiquitous in our daily lives.
- [4] The trial judge did make adverse credibility findings against the appellant, describing his testimony as "marked by repeated inconsistencies on issues of real significance in the trial." (At para. 18.) These inconsistencies included his response to questions about the workings of Reg.Clinic, a program the appellant deployed on his office computer on April 20, 2015 -- the day on which his computer use first came under scrutiny. Contrary to his insistence that the Reg.Clinic program did not delete "normal" files or data, the judge found the program was "meant to locate and delete computer data." (At para. 21.) She also found several external inconsistencies in the appellant's testimony, described at paras. 35-43, and concluded that "at best", the consistencies that did exist in his evidence were acknowledgements of irrefutable fact. Taken together, she said, the nature of the contradictions had detracted significantly from the strength of his evidence. The judge acknowledged, however, that in accordance with *R. v. W.D.* [1991] 1 S.C.R. 742, she was

required to consider whether she was left with a reasonable doubt. To do this, she carried out a detailed review of the evidence, beginning at para. 44 and continuing to para. 143 of her reasons.

- [5] In terms of legal analysis, the judge found, correctly, that the case against Mr. Vermeer was circumstantial. She referred at para. 145 to *R. v. Villaroman* 2016 SCC 33, from which she drew the following principles:

The Court re-affirms in *R. v. Villaroman* that the test in a circumstantial case is whether the only reasonable inference that can be drawn from the evidence is guilt. Various inferences that are inconsistent with guilt have been raised by the defence in the present case. My assessment of the evidence is informed by the principles articulated in *R. v. Villaroman*, which include:

- If the evidence, or lack of evidence, logically supports reasonable inferences that are inconsistent with guilt, then the Crown's evidence does not meet the standard of proof beyond a reasonable doubt (*Villaroman* at para. 35);
- A theory that is inconsistent with guilt is not speculative just because it arises from an absence of evidence. A gap in the evidence may result in inferences other than guilt. "But, those inferences must be reasonable given the evidence and the absence of evidence, assessed logically, and in light of human experience and common sense": *Villaroman* at para. 36;
- While the trier of fact should consider other plausible theories and "other reasonable possibilities," the Crown need not "negative every possible conjecture, no matter how irrational or fanciful, which might be consistent with the innocence of the accused." *R. v. Bagshaw*, [1972] SCR. 2 at pg. 8. "Other plausible theories" or "other reasonable possibilities" must be based on logic and experience applied to the evidence or the absence of evidence, not on speculation (*Villaroman*, para. 37).

- [6] The judge analyzed the theories inconsistent with guilt advanced by the defence (see paras. 146-191), the appellant's "post-fact conduct" (at paras. 192-211), and whether there were any reasonable inferences, other than the appellant's guilt, that could be drawn from the evidence or absence thereof. She concluded at para. 223 that the Crown's evidence established beyond a reasonable doubt that Mr. Vermeer had "searched for, downloaded and sometimes opened the child pornography files revealed in [the Crown's] investigation", and that this was the only reasonable inference that could be drawn from the evidence. On the possession charges, she found that although (much of) the evidence had been gleaned from files that were no longer accessible, the appellant had knowingly "downloaded child pornography in order to store it in a specific place for his use or benefit" (at para. 227); and that the majority of the material had been saved over a period of years to a specific removable drive. The appellant had controlled this "PCC Offsite" drive, which could have been accessed remotely. Given the totality of the evidence, the judge was satisfied the Crown had proven the appellant had possessed child pornography from as early as May 1, 2010. (At para. 229.)

- [7] As for accessing the material, the judge found that the only conclusion that could reasonably be drawn from the whole of the evidence was that the appellant had viewed the child pornography in his possession and done so knowingly. (See para. 232.) In summary, she said:

The overall constellation of evidence in this case leaves me with no other reasonable inference other than Mr. Vermeer viewing child pornography dating back to the earliest dates of access in the LNK files in 2010. This is a common sense conclusion based on the way the evidence shows Mr. Vermeer sought out and procured this amount of pornographic material. It would be unreasonable to suggest in these circumstances that he did nothing more than possess the file data in these circumstances. [At para. 235.]

Computer-Based Evidence

- [8] The prospect of a person's being convicted on the basis of evidence that is not only primarily circumstantial but also almost exclusively computer-generated must surely give any judge pause. We are all aware that computers operate by means of programs designed by people and that people make mistakes. In some circumstances, they may manipulate computer programs. Computers may also malfunction and are subject to 'hacking' and malware. At the same time, computers are used and relied upon every day by billions of people. Courts must adapt, and are adapting, to technologies that are now part of everyday life. At least in the civil context, trial judges have become accustomed to proceedings in which emails, pages from Facebook or other social media, and electronically-stored information, including photos and videos, are routinely admitted into evidence without formal inquiry into how computers or particular programs or applications were created or are intended to operate. In this regard, the comments of the Alberta Court of Appeal in *Kon Construction Ltd. v. Terranova Developments Ltd.* 2015 ABCA 249 are apt:

Mechanically generated evidence is accepted by the courts because of various indicia of reliability. First of all, the equipment and software are designed by experts in accordance with scientific and engineering knowledge; at a theoretical level, they should produce accurate results. Secondly, the prototype equipment is tested against known samples to ensure that it does provide accurate results. Thirdly, the field equipment is mass-produced in accordance with the precise design and specifications of the prototype, and each piece is usually tested before it leaves the factory. Fourthly, those who use the equipment follow established standards for maintenance, calibration and operation. Fifthly, the equipment and the data are then used on a day-to-day basis, and are shown by experience to be reliable. Once this threshold of reliability is met, the party tendering the evidence does not have to re-prove the underlying technology in every case: *R. v A.K.*, 2004 ABQB 875 at paras. 4, 10-12, 44 Alta LR (4th) 308, 373 AR 141.

New technology is always a bit mysterious, particularly where it lacks transparency. The rules of evidence have always been designed to screen out unreliable information, and the courts look skeptically on untested forms of information, particularly in criminal cases. The technical rules of evidence should not, however, be used to screen out information that is inherently reliable.

Information gathered by electronic equipment is routinely relied on by the average citizen and the courts because of the indices of reliability just noted. The information may not be perfect, infallible, or accurate to a certainty, but it is sufficiently reliable to be used in court. The admissibility of evidence does not depend on proof to a certainty of exact accuracy; flawed evidence is routinely admitted, and its weight is assessed by the trier of fact. [At paras. 17-18; emphasis added.]

[9] In criminal proceedings, however, s. 31 of the Canada Evidence Act, R.S.C. 1985, c. C-5 ("CEA") governs the admissibility of "electronic documents", a term broadly defined at s. 31.8. The relevant portions of s. 31 provide:

31.1 Any person seeking to admit an electronic document as evidence has the burden of proving its authenticity by evidence capable of supporting a finding that the electronic document is that which it is purported to be.

31.2 (1) The best evidence rule in respect of an electronic document is satisfied

- (a) on proof of the integrity of the electronic documents system by or in which the electronic document was recorded or stored; or
 - (b) if an evidentiary presumption established under section 31.4 applies.
- (2) Despite subsection (1), in the absence of evidence to the contrary, an electronic document in the form of a printout satisfies the best evidence rule if the printout has been manifestly or consistently acted on, relied on or used as a record of the information recorded or stored in the printout.

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.

...

31.5 For the purpose of determining under any rule of law whether an electronic document is admissible, evidence may be presented in respect of any standard, procedure, usage or practice concerning the manner in which electronic documents are to be recorded or stored, having regard to the type of business, enterprise or endeavour that used, recorded or stored the electronic document and the nature and purpose of the electronic document.

31.6 (1) The matters referred to in subsection 31.2(2) and sections 31.3 and 31.5 and in regulations made under section 31.4 may be established by affidavit.

- (2) A party may cross-examine a deponent of an affidavit referred to in subsection (1) that has been introduced in evidence
 - (a) as of right, if the deponent is an adverse party or is under the control of an adverse party; and
 - (b) with leave of the court, in the case of any other deponent.

31.7 Sections 31.1 to 31.4 do not affect any rule of law relating to the admissibility of evidence, except the rules relating to authentication and best evidence.

31.8 The definitions in this section apply in sections 31.1 to 31.6.

computer system means a device that, or a group of interconnected or related devices one or more of which,

- (a) contains computer programs or other data; and
- (b) pursuant to computer programs, performs logic and control, and may perform any other function.

data means representations of information or of concepts, in any form.

electronic document means data that is recorded or stored on any medium in or by a computer system or other similar device and that can be read or perceived by a person or a computer system or other similar device. It includes a display, printout or other output of that data.

electronic documents system includes a computer system or other similar device by or in which data is recorded or stored and any procedures related to the recording or storage of electronic documents.

secure electronic signature means a secure electronic signature as defined in subsection 31(1) of the Personal Information Protection and Electronic Documents Act. [Emphasis added.]

[10] In keeping with these provisions, Canadian courts have been appropriately cautious concerning the use of computer-generated evidence in the criminal context: see for example this court's decision in *R. v. Ball* 2019 BCCA 32, to which I shall return below; *R. v. Lamb* 2010 BCSC 1911; *R. v. Martin* 2021 NLCA 1 and *R. v. Coban* 2021 BCSC 2428.

- [11] The case at bar was considerably more complex than cases turning on the authenticity of a message or photograph on social media. Although an expert witness provided direct evidence of actually viewing material that constituted child pornography from files stored on the appellant's office computer (and parts of that evidence were shown at trial in an in camera session), there were records of voluminous materials to which only references or 'traces' of pornographic material could be found. In these circumstances, expert evidence was clearly in order.
- [12] The Crown adduced the evidence of three experts, two of whom were employed by a company called Empyrion Technologies Inc. ("Empyrion"). They were found to be qualified to give expert evidence concerning "computer systems and related technology". Empyrion had been retained in 2012 to provide technical support for the computer network of Mr. Vermeer's church, where he worked. The church had a total of 27 computers in use, including a desktop (referred to by the trial judge as the "office computer") used by Mr. Vermeer until it was seized by police in April 2015, and the laptop he had used for some months ending in early 2012.
- [13] One of the two Empyrion experts, Mr. Maguire, was working when the AVG CloudCare program used by Empyrion to monitor the church's network for viruses alerted the company to a possible virus in the early hours of April 20, 2015. When Empyrion personnel accessed the church network remotely, they found that a virus had attached to files that appeared to be child pornography. The trial judge recounted the events that followed:

By accessing the church network remotely, the technicians could see that child pornography appeared to have been downloading throughout the weekend on the E drive of Mr. Vermeer's office computer. This led Empyrion to contact the head pastor of the Main St. Church, Shawn Vandop. As Empyrion technicians carried on their remote investigation of the child pornography issue, they came to realize that, at 9:01 a.m., the E drive containing the child pornography was no longer there. Without the E drive connected to the computer, both the impugned material and the drive it was on became inaccessible to Empyrion. This E drive has never been located or recovered.

Mr. Vermeer agrees that he probably arrived at work the morning of April 20, just before 9 a.m. Mr. Vandop immediately told him of the concerns about child pornography located on his computer, prompting Mr. Vermeer to go check on his office computer. Later that same morning, Empyrion called back and this time spoke to Mr. Vandop and Mr. Vermeer together. Empyrion technicians advised that the E drive had disappeared and they recommended contacting the police. Following that conversation, Mr. Vermeer called the police. As a result of Mr. Vermeer's complaint, police did not immediately investigate. However, Empyrion followed up with their efforts to determine the source of the illegal material, which included scans of other church computers.

Empyrion found further evidence indicative of child pornography on Mr. Vermeer's office computer, as well as on a church laptop ("the laptop"). On April 21, 2015, police were again contacted and the Chilliwack RCMP started their investigation. On that day, Mr. Vermeer's office computer and the laptop were seized and were later forensically analyzed. ... [At paras. 4-6; emphasis added.]

One of the key issues at trial was who was responsible for the apparent disappearance of the missing drive and whether it had been physical (such as a USB or Blackberry) or only virtual.

- [14] The other Empyrion employee qualified to give expert evidence was Mr. Kullman, who attended at the church around noon on April 20. He found the appellant running "Reg.Clinic" (a name the trial judge found at para. 19 is used interchangeably with "Reg.Cleaner") on his desktop computer. Mr. Vermeer complained the program was "stuck" on something and was repeatedly rebooting. Mr. Kullman checked for malware or spyware but found none. He looked inside the computer and found no external drives but did find a hardware identifier associated with an E drive. Mr. Kullman testified that when he later accessed "Event Viewer" in the registry of Mr. Vermeer's desktop he found that an eMule (or "aMule," which he said is the same thing) program had been running until it had "crashed" at about 9:00 or 9:01 am. He testified that the removal of the missing E drive without the computer being properly shut down could have caused the crash.
- [15] Empyrion ultimately examined approximately 20 of the 27 computers belonging to the church network but was unable to locate any trace of pornographic material on any computer other than Mr. Vermeer's desktop and his former laptop. (The remaining seven computers were firewall-protected or otherwise unavailable for examination.)
- [16] The third expert called by the Crown was an RCMP forensic examiner, Sgt. Rostie, whom the trial judge found was qualified to give evidence on the following subjects:
1. the preservation and analysis of stored computer data using a variety of forensic software tools;
 2. a date and time analysis of computer forensic artefacts;
 3. forensic evidence relating to human-directed internet downloading through both browsing and file-sharing software;
 4. forensic evidence retained in computer storage indicating actions of a human user as opposed to automatic functions of the computer itself;
 5. the forensic evidence relating to the storage locations of various electronic files as a result of the actions of a human user;
 6. forensic evidence of the use of various software and electronic documents the content and use of which supports an inference of possession by a particular individual;

7. the functioning of computer networks including the internet and the forensic artefacts left by accessing these networks; and
 8. the nature and functionality of computer viruses and malware and their effects on the integrity of data storage.
- [17] Sgt. Rostie produced a report that became Exhibit 10 at trial. Although it referred several times to evidence of file names "consistent with child pornography", she did, as I have mentioned, find and view actual child pornography in a "thumbcache" file. Some of this material was viewed by the trial judge sitting in camera. In addition, Sgt. Rostie reported that the known.net file accessed through aMule (a "peer-to-peer" program) contained 28 entries with typical child pornography names. The "hash values" of those entries had been compared with a database held in the Integrated Child Exploitation Unit ("ICE") of the RCMP; eight of them, she said, "were confirmed to meet the definition of child pornography under the Criminal Code."
- [18] The appellant did not challenge the qualification of any of the Crown's experts, and did not seek to adduce any experts on his own behalf. Mr. Vermeer himself was very experienced in computer systems, having obtained various certificates in that field and having been an instructor in "networking and operating systems" at a local college. Some years later he became a full-time consultant to what was then known as the Promontory Heights Church in Chilliwack. He was referred to as the "executive pastor" of the church, although it appears his duties were purely secular. He testified that with one possible exception, he was the person most experienced in technology among the church's staff, and indeed that he could 'build a computer'. He was the "administrator" of the network and in the trial judge's words, had "significant control" over it. (At para. 183.)

Grounds of Appeal

- [19] The appellant advances three errors in judgment on the part of the court below, namely that:

First, the trial judge failed to consider whether the Crown had satisfied its onus to show that the electronic evidence in this case complied with the best evidence rule.

Second, she admitted and relied upon hearsay evidence in finding Mr. Vermeer guilty.

Third, the trial judge made a number of overlapping and mutually reinforcing errors in rejecting Mr. Vermeer's evidence.

It seems to be common ground that these are errors of law and thus subject to the standard of correctness.

Best Evidence

[20] The best evidence rule was not raised at trial. The appellant submits that s. 31.2 of the CEA required a voir dire to be held as a condition of admissibility so that the trial judge could be satisfied that the evidence -- presumably, all the many pages of screenshots, log files, and other data detected in the two computers -- was the best evidence that could be provided of the presence of child pornography. Counsel referred in particular to *Ball*, where the electronic documents in question were photographs of Facebook messages the authenticity of which was contested. Indeed, the only witness who testified to the authenticity of the texts and photos in question was the alleged "tamperer" and there was no expert evidence on the point. Madam Justice Dickson for this court observed with respect to the best evidence rule that the concept of an "original" is "poorly-suited to electronic documents." However, she observed, the rule may be met in the manner provided by s. 31.3:

... As Justice Paciocco explains in "Proof and Progress", it is not immediately obvious whether the original is "the actual hard drive containing the code, the translation of the code that is displayed by the electronic device, a copy of the file, or the first print out". Consequently, the statute adopts an inclusive approach; for framework purposes, an original is any translation of the computer code in observable form: "Proof and Progress" at 193, 199-200; Hirsch at paras. 22-23.

Like the common law best evidence rule, the statutory rule is intended to help ensure that an electronic document accurately reflects the original information input into a computing device by its author. The framework provides alternative methods of satisfying the rule, some of which rely on statutory presumptions available in the absence of evidence to the contrary. Section 31.2 provides for proof, direct or circumstantial, of the integrity of an electronic documents system, proof via secure electronic signature and proof via printout; s. 31.3, for presumptions of integrity with respect to electronic documents systems; s. 31.4, for presumptions regarding secure electronic signatures; and s. 31.5, for consideration of relevant standards, procedures, usages and practices. The standard of proof for the prerequisites to admissibility is the balance of probabilities: *R. v. Oakes*, [1986] 1 S.C.R. 103; "Proof and Progress" at 202. [At paras. 72-3; emphasis added.]

[21] The Court in *Ball* also referred to *R. v. Donaldson* 2016 CarswellOnt 21760, where Mr. Justice Paciocco declined to admit evidence of Facebook messages in the absence of any investigation to determine the account from which they had come. (See *Donaldson* at para. 22, quoted at para. 78 of *Ball*.) After considering these and other cases, the Court ruled in *Ball* that the admissibility of the photographs had not been properly scrutinized and that the appellant had been "deprived of an important procedural protection, which compromised trial fairness and contributed to what was, overall, a miscarriage of justice." Dickson J.A. continued:

... In these circumstances, in the absence of a clear concession from counsel, the judge should have made these determinations in the first instance, on a voir dire, in the absence of the jury. However, he did not, apparently because all concerned overlooked the need for him to do so. [At para. 87; emphasis added.]

- [22] The appellant submits that the same happened in this case, even though defence counsel at trial was clearly content to proceed on the basis that the appellant's two computers had been operating properly -- i.e., that the electronic documents "system" had integrity. In support of Mr. Vermeer's argument on appeal, counsel noted various "oddities" and "inconsistencies" in the evidence, which he says should have been resolved by rulings in a voir dire. Instead, the evidence was admitted by the trial judge essentially without debate, and the inconsistencies and oddities were explored in the trial proper.
- [23] Respectfully, I am unable to accede to the argument that the best evidence rule was not complied with in this case. First, it seems to me that we are not really concerned here with the "best evidence rule" per se -- a rule that as Justice Paciocco notes simply requires that "if an original document is available in one's hands, one must produce it". ("Proof and Progress: Coping with the Law of Evidence in a Technological Age", (2013) 11 C.J.L.T. 181 at 199.) Mr. Vermeer did not bring to the trial judge's attention, and has not brought to our attention, any evidence of the presence or absence of pornographic material, whether in existence at the time of trial or not, that was "better" than that adduced at trial. Three experts testified as to the operation of the appellant's computers and with one exception, none suggested there was information crucial (or even relevant) to the case that had not been brought forward (or, as regards to the missing E drive, searched for.) The one exception relates to the disclosure in the course of Sgt. Rostie's testimony of certain file logs that the defence had evidently not received prior to trial. The trial was adjourned for a lengthy period to allow these to be examined by the defence, and Exhibits 16-18 were ultimately introduced by defence counsel when the trial resumed.
- [24] In these circumstances, it is difficult to accept the notion that the appellant may have been deprived of some important procedural protection or that one or more voir dires would have led the trial judge to exclude any particular evidence that was admitted.
- [25] Justice Paciocco suggests that given the broad statutory concept of "original document" in s. 31.1, the "primary role" played by the best evidence provisions of the CEA is now "merely as an adjunct to authenticity". (My emphasis.) The provisions exist, he contends (*supra* at 200), "not so much to assure that the best evidence is presented, but to provide some further assurance that the document adduced at trial is the same as the one that was input into the computer." (In this case, the assurance would be that the electronic documents, traces of which were adduced at trial, correctly indicated those that had been downloaded by the perpetrator.) The fact that s. 31.2(1)(a) provides that the best evidence rule can be met in respect of an electronic document by proving the "integrity" of the electronic documents system that recorded or stored the document confirms this point. Effectively, the requirement that no "better" evidence exists than the evidence adduced at trial has been

superseded by a requirement that the system by which information tendered at trial was stored or downloaded is, or was, operating properly at the relevant time(s). As one commentator has put it, "Proof of the proper functioning of the computer system is ... a proxy for the integrity of the electronic document at issue." (Nader R. Hasan, "No Progress Without Proof: Authenticating Electronic Evidence in the Digital Age", (2020) 40:3 For the Defence: The Criminal Lawyers' Ass'n Weekly 55, at 59.)

[26] The CEA does not require, at least expressly, that a voir dire be held for this purpose. Although a voir dire might have been appropriate in respect of discrete parts of the Crown's evidence in this instance, I believe it would have been unworkable to address in one or more voir dires the admissibility of all the evidence (including expert evidence) that was adduced in this trial concerning the workings of the appellant's computers and their drives, programs and applications. In my respectful view, provided the Court was alive to the importance of the integrity of the electronic system by which the "documents" were recorded or stored and downloaded, such documents could be properly admitted at trial without the formal step of one or more voir dires.

[27] The trial judge's reasons clearly demonstrate her concern to determine whether the computer-based evidence adduced by the Crown was reliable (which I equate with the "integrity" of the computer system for purposes of s. 31.2(1)(a)). She stated at para. 137, for example, that:

When I review the evidence as a whole, I have considered whether any of the above noted inconsistencies detract from the reliability of the computer data generally or Sgt. Rostie specifically as an expert witness. I have concluded the dates of access in the LNK files should be approached with caution to ensure that they are consistent with other evidence. The overwhelming majority of the evidence Sgt. Rostie presented has an internal consistency that accords with the opinions she formed about where and when both legal and illegal material was accessed. I reviewed with particular attention her evidence about the apparent inconsistencies in the C drives and her opinion around the dates of access on the laptop.

and at para. 140 that:

I must consider whether the data itself is reliable and whether it supports the inferences the Crown invites the Court to draw. There are limitations on the evidence available to this court since it was almost entirely retrieved from unallocated space. As all of the computer experts noted, many things on a computer can be manipulated by an advanced user. Inferences do need to be drawn with caution, and with an awareness that some of the computer evidence is consistent with more than one interpretation. The more complicated and determinative issue in this case is what inferences can be supported by the body of evidence that I do accept.

(Emphasis added; see also paras. 83-5; 220-1.)

[28] While it may be unfortunate that s. 31.1 of the CEA was not brought to the trial judge's attention and that she did not refer to the relevant provisions herself, the entire trial was effectively an inquiry into the "integrity" of the computer system and the electronic documents on which the Crown relied. Further, while a "clear concession from counsel" for the appellant was not made with respect to the requirements of the CEA, trial counsel was content not to challenge the admissibility of the documents (which of course is subject to a "low" threshold), but to address their weight in connection with the elements of the charged offences, including in particular the central issue of who was responsible for the child pornography having been downloaded and accessed on the appellant's computers.

[29] A somewhat similar situation arose in *R. v. Hirsch* 2017 SKCA 14, another case involving Facebook messages and their authenticity. The trial judge was found to have been "alive to the issues of authentication and authorship, although perhaps not to the requirements of s. 31.1 of the Canada Evidence Act, which had not been raised at trial." Nevertheless, Caldwell J.A. for the Court of Appeal reasoned:

... I am satisfied the evidence adduced in this respect was capable of authenticating the screen captures as a record of Mr. Hirsch's Facebook page. While it might have been preferable to have the complainant's friend testify as to authenticity, there was sufficient evidence of authentication before the trial judge for him to reach the conclusion that he did and, because of that, I find no compelling reason to interfere with his conclusion that the screen captures were admissible. [At para. 21.]

The Court also referred specifically to the utility of a screenshot as capturing the best evidence available to the Crown to adduce Mr. Hirsch's Facebook page itself into evidence. Caldwell J.A. continued:

... the more compelling conclusion is that the screen captures are the best evidence available to the Crown to adduce Mr. Hirsch's Facebook page itself into evidence. Indeed, given the fluidity and impermanence of postings on a Facebook page, a screen capture may be one of the few ways of establishing what was actually posted on a Facebook page at any point in time. On this basis, I am satisfied the presumption of integrity under s. 31.3(b) of the Canada Evidence Act applied in these circumstances and was not rebutted [At para. 24; emphasis added.]

The appeal was dismissed.

[30] I also note the decision of the Ontario Court of Appeal in *R. v. B.(C.)* 2019 ONCA 380, where the authenticity of certain cellphone messages and photos "extracted" from a phone by a private investigator was challenged. Watt J.A. for the Court noted that s. 31.1 of the CEA places on the proponent the onus of adducing evidence capable of supporting a finding that the electronic document is what it purports to be -- again, a "low" threshold. In his words:

... Section 31.1 does not limit how or by what means the threshold may be met. Its only requirement is that the evidence be capable of supporting a finding that the electronic document "is that which it is purported to be". That circumstantial evidence may be relied upon is well

established: Hirsch, at para. 18; [other authorities omitted]. This accords with general principles about proof of facts in criminal proceedings, whether the facts sought to be established are preliminary facts on an admissibility inquiry or ultimate facts necessary to prove guilt. [At para. 68; emphasis added.]

The trial judge in B.(C.) was found to have erred in finding that the text messages in question lacked probative value because they had not been properly authenticated by direct evidence. (See para. 73.)

[31] In the case at bar, there was no suggestion that the subject computers lacked integrity in the sense that they were not operating properly or as expected. The possibility of hacking was rejected, as was malware, both by Mr. Maguire and by Sgt. Rostie, whose evidence on this point was accepted by the trial judge at paras. 126 and 176; see also paras. 148-191 regarding the possibility of an unknown person's accessing the appellant's office computer. The trial judge's rejection of these possibilities did not mean, however, that there were no anomalies or inconsistencies as suggested by the defence. As noted in *Kon Construction*, "The admissibility of evidence does not depend upon proof to a certainty of exact accuracy." (At para. 18.) The anomalies were explored by the trial judge and she accepted or rejected them as part of the process of weighing the evidence in its entirety under the "Conclusions" heading.

[32] In all the circumstances, including in particular the fact that most of the lengthy trial consisted of expert evidence concerning the workings of the two computers, I would not accede to the first ground of appeal.

Hearsay Evidence?

[33] The appellant's second ground of appeal is that the trial judge improperly admitted and relied on hearsay evidence for the truth of its contents. This is said to have occurred in connection with two categories of evidence. First, since Sgt. Rostie had not actually been in a position to view the contents of the hundreds of files whose titles were ultimately in evidence, the appellant submits the file titles were hearsay and therefore presumptively inadmissible as proof that the files in fact contained child pornography. Second, it is said the trial judge drew inferences concerning the functionality of the Reg.Clinic program based on screen shots of its "interface", or "menu", which indicated a deleting function. Again the defence contends this amounted to hearsay and led the judge to make the important inference that the appellant had deleted his Internet history upon becoming aware of the investigation on April 20, 2015.

File Names

[34] Both arguments require us to define clearly what hearsay is and the purposes for which the file names and Reg.Clinic interface were used at trial. Sidney N. Lederman, Michelle K. Fuerst and Hamish J. Stewart, authors of *The Law of Evidence in Canada* (6th ed., 2022) posit the following working definition of the hearsay rule:

Written or oral statements, or communicative conduct made by persons otherwise than in testimony at the proceeding in which it is offered, are inadmissible, if such statements or conduct are tendered either as proof of their truth or as proof of assertions implicit therein. (At 263.)

The authors note that at the root of the rule is the abhorrence of the common law to "proof which is unsworn and has not been subjected to the trial by fire of cross-examination. Testimony under oath, and cross-examination, have been considered to be the best assurances of the truth of the statements of facts presented." (At 265, quoting *R. v. Abbey* [1982] 2 S.C.R. 24 at 41, per Dickson J. as he then was.)

[35] In this case, of course, it may be debated whether a file title constitutes a "statement" or "communicative conduct" of a "person" for purposes of the rule. I suspect it would be impossible to determine the "author" of one or more titles attached at some point to files in the marketing and distribution of child pornography on the Internet, much less to call any such 'author' to testify. On this point, I note the reasoning of Mr. Justice Ehrcke in *Lamb*:

evidence that the hash value of a file on a given computer matches what is in a database of purported child pornography is hearsay. It is evidence that some unidentified person, who is not before the court as a witness, made a decision to include a particular file in the database. Since the person who made that decision is not before the court, is not under oath, and cannot be cross-examined, there is no way to know why he or she made the decision, and therefore no way to test the correctness or reliability of that decision. [At para. 45.]

In *Lamb*, police had remotely carried out a search of a shared folder of the accused's computer containing names suggestive of child pornography, but the contents of the folder had not been actually downloaded. The Crown was seeking to prove they contained child pornography only on the basis of the hash values of the files. Only one video file contained material that the Court found depicted explicit sexual activity on the part of a person under age 18.

[36] If one assumes in the case at bar that the file titles did constitute statements or communicative conduct of a person for purposes of the rule, the question then is whether the titles were adduced into evidence as proof of the truth thereof -- i.e., as proof they contained what the titles suggested they contained. The Crown submits that the file names were not adduced for this purpose, but rather as circumstantial evidence that the person who downloaded and/or viewed them was seeking out child pornography. In the Crown's words, "the sheer volume of entries pointing to file names indicative of child pornography was strong circumstantial evidence of the knowledge component of possession in relation to files which could be verified to meet the definition of child pornography". (My emphasis.)

- [37] Although I see no error in the trial judge's using the file names as circumstantial evidence, it is possible a reasonable doubt might still exist as to whether the offending material did in fact constitute child pornography within the meaning of s. 163.1(1) of the Criminal Code. As Ehrcke J. stated in *Lamb*, "What the child pornography sections of the Criminal Code are concerned with is the content of the files, not their names. An otherwise innocuous file does not become illegal simply because someone attaches a suspicious name to it." (At para. 41; my emphasis.)
- [38] Both Mr. Maguire and Mr. Kullman were unable to testify as to the contents of the files in question, since they had not wished to risk seeing child pornography and knew it was illegal to view such material. (Evidently they were unaware they would have been protected by s. 163.1(4.1.) of the Code.) However, Sgt. Rostie did give direct evidence on the point. In the course of her testimony, she was taken to page 9 of her report, which stated:

Evidence of Possession (LNK Files)

LNK files are also referred to as shortcut files, The operating system creates these automatically for easier access to recently accessed files,

Evidence that images and videos (with filenames indicative of child pornography) were possessed by a user of this computer was located in LNK files for user account jvermeer.OFFICE.

The LNK files were recovered from unallocated space, meaning that they had been deleted. Over 100 LNK files with child pornography file names were recovered with dates ranging from January 14, 2012 to May 23, 2014.

An example of the LNK files recovered include:

- F:\New folder\amule\Incoming\((Lolitaguy)) Ls-Magazine Lsm-07-09-01 Bonus, Killer, Three 11-13Yo Girls

- o Date January 14, 2012

- o 11-13Yo in the title indicates that the subjects in the video are 11 to 13 years old

- J:\New folder\downloads\2010 PTHC 9Yo Lizka mast on webcam_mpeg4.avi

- o Date: February 24, 2012

- o PTHC is short for pre-teen hard core

- o 9yo indicates that the subject is 9 years old

- J:\New folder\downloads\Teenfans - (Mytola Info) - Lolitas Mexican Preteen 7 - 9 yo - Girlss With Male.avi

- o Date: March 2, 2012 at 12:14 am

- J:\dwnlds\New folder\Three 14Yo White Boys And One 15Yo Black Boy Have Some GaySex.mpg

o Date: May 19, 2012 at 9:22 pm

The full list can be reviewed by clicking the following LNK:

xxxx

She began to testify concerning the meaning of some of the words used in the titles, but defence counsel told the Court it was not necessary that she be questioned on the remaining titles. In his words, "There's no issue that they're on the face of it indicative of child pornography".

[39] As mentioned earlier, Sgt. Rostie did view the contents of a few of the titles herself, and the contents of them were shown in camera at trial. At page 382 of the transcript, Crown counsel proposed the in camera procedure to the Court and the following colloquy took place:

[Crown Counsel]: Then once that part of the evidence is over I propose make it exhibit then open the courtroom and then I'll qualify her as an expert so that the public can see her qualifications and so on.

THE COURT: All right. Anything on that, Mr. Klein? You don't think we need to watch the entirety of the evidence being submitted?

[Defence Counsel]: No. In fact, I think whatever skills -- I mean, it becomes very self-evident.

THE COURT: Right.

[Defence Counsel]: I can advise I've spoken to my friend, I take real no -- no issue with any of the descriptions. I'm not calling anybody a liar about those. And I'm not arguing on artistic merit or anything of that nature. So --

THE COURT: I see.

[Defence Counsel]: -- this is really about whether or not Mr. Vermeer was in control of anything that was illicit. So I encourage it to be as brief as possible and whatever efficiencies can be brought into that process, I encourage.

The trial judge told Crown counsel:

Well I echo [defence counsel's] sentiment ... that however brief you can be in -- in playing what you think is necessary to establish that it's child pornography is agreeable. And I will make an order that the courtroom is closed to the public only for the portion of this officer's evidence where she's playing the impugned material.

[Emphasis added.]

Shortly thereafter, defence counsel told the Court that "with regard to the exhibit that was just filed, once again we take no issue that it meets the definition of child pornography". The images viewed by the Court from a "thumb cache" file were placed on a disc that became Exhibit 9.

- [40] The position taken by counsel for the appellant may not have amounted to a "formal" admission, but it was an admission nevertheless, and was relied on by the Crown and the Court. It was consistent with the defence strategy of focusing on the question of identity, which defence counsel had identified, correctly in my view, as the most difficult element to be proven by the Crown in this case.
- [41] Even if this concession had not been made, I believe the trial judge would have been justified in invoking the principled exception to the hearsay rule to admit the titles as proof that the files contained what the titles suggested. The criterion of necessity would in my view be met given the unavailability of most of the files for viewing following their deletion by means of the removal of the PCC Offsite drive and the deployment of Reg.Clinic in April 2015. The trial judge found that it was the appellant who had carried out the deletions. It would be ironical if Mr. Vermeer was permitted to take advantage of those deletions to argue against the necessity of relying on the titles as proof of the presence of child pornography. As far as reliability is concerned, file titles are designed to indicate to users the contents of the material they contain. It would be non-sensical for titles suggestive of child pornography to be used if users were to be consistently disappointed to find something else. In any event, we may infer that the showing in court of some of the material Sgt. Rostie was able to access left no doubt that it constituted child pornography. Even if the witness had had access to all the contents of all the folders, it would not have been necessary for her or the judge to view every single file (of which there were hundreds) for this element of the offence to be proven.
- [42] For these reasons, I would not accede to the second ground of appeal insofar as the file names are concerned.
- [43] For the sake of completeness, I confirm that I have also considered whether what otherwise might be hearsay could have been admissible under the 'business records' exception to the hearsay rule, as modified by s. 30 of the CEA. However, given the illegal nature of the 'business' of distributing child pornography, that possibility seems unlikely (Cf., however, *R. v. Lukacko* (2002) 1 C.R. (6th) 309 (Ont. C.A.)). In any event, the application of the business records exception would have to be justified under the principled approach discussed above: see *R. v. Starr* 2000 SCC 40 at paras. 210-217 and *The Law of Evidence in Canada* at 288-9.

The Reg.Clinic Program

- [44] Finally under the hearsay rubric, the appellant objects that the trial judge's treatment of evidence as to Mr. Vermeer's deployment of the "Reg.Clinic" program in the morning and evening of April 20, 2015 to delete data was founded on hearsay. It seems clear that the judge's findings on this point were material to the conviction of the appellant.

[45] The trial judge first considered the appellant's evidence concerning Reg.Clinic at paras. 19-29 of her reasons in connection with the credibility of Mr. Vermeer. Her reasoning included the following:

part of Mr. Vermeer's description of the program in direct examination included the fact that the software does not alter files or data. In cross, he further claimed the program could not remove files or data. These characterizations of the program are false and self-serving. Not only is this evidence contradicted by the external evidence about the Reg. Cleaner functions presented by Sgt. Rostie, it is contradicted by Mr. Vermeer himself after persistent questioning in cross-examination when he eventually conceded that the program can delete registry data.

Second, Mr. Vermeer was inconsistent about how he used Reg.Cleaner. In direct examination, Mr. Vermeer said the Reg.Cleaner program was already running when he first opened his computer on April 20th. In fact, he says that the computer appeared frozen on the Reg.Cleaner program. Mr. Vermeer attributed this to some system malfunction due to what he believed was a breach of the network, and he compared it to "the blue screen of death." Mr. Vermeer's initial description of how he used Reg.Cleaner suggests that he did not intentionally launch the software on the morning of April 20, rather the software was already activated when he found out about the child pornography. [At paras. 24-5; emphasis added.]

(Again, I note that the trial judge stated at para. 19 that the names "Reg.Clinic" and "Reg.Cleaner" were interchangeable.)

[46] Under the heading "Post-Fact Conduct", the judge found that the appellant had deleted information regarding recent use of his computer and had done so knowing there was an impending police investigation into his computer. She acknowledged the care required in using such conduct as evidence of guilt:

The disappearance of these search history logs is perfectly consistent with the function of the Reg. Cleaner program, used by Mr. Vermeer. Reg. Cleaner specifically allows a user to delete internet history. Given the access Mr. Vermeer had to his office computer, including exclusive access the evening of April 20, 2015, I am satisfied that Mr. Vermeer deleted the information regarding recent use of his computer and I am satisfied that he did so knowing that there was an impending police investigation into his computer.

Post-fact conduct must be approached with considerable caution by triers of fact. I must not leap from the fact that Mr. Vermeer deleted data from his computer to the conclusion that he downloaded and accessed child pornography on his computers. Unlike the other circumstantial evidence in this case, when it comes to post-fact conduct, I must be satisfied that the post-fact conduct evidence is consistent only with the ultimate conclusion of guilt. I am satisfied that it is. I cannot fathom, nor is there anything in the evidence that would explain, why Mr. Vermeer would have deleted data from his computer in this way after being told that there is child pornography being downloaded through that very computer. I am mindful that innocent people can do strange, or even dishonest, things when they are under investigation. This general rule has particular applicability to a pastor like Mr. Vermeer, who would presumably face internal or even

public shaming as a result of having child pornography found on his church computer -- regardless of whether or not he was the one who put it there.

I have considered whether Mr. Vermeer could have deleted information by accident through a legitimate use of the Reg. Cleaner program to delete malware, but I am satisfied given Mr. Vermeer's high level of computer expertise and his previous use of this program that he did not accidentally remove data. I have considered whether Mr. Vermeer deleted activity of recent use on his computer before he learned of the child pornography investigation in his stated efforts to improve the efficiency of his computer. However, this cannot be reconciled with his evidence that he continued to work on his computer throughout the day and evening of April 20, 2015. There was no evidence of such recent use in the active operating system according to Sgt. Rostie, which suggests that data was deleted close in time to when the computer was seized. [At paras. 198-200; emphasis added.]

[47] The appellant takes the position that there was "no evidence of what Reg.Clinic actually did" because Sgt. Rostie ran the program on a "virtual" machine that had never been used before and therefore had no data to delete. As well the appellant submits that the program could not delete data by means of the program because the data was "unregistered". On this point, he referred us to the following colloquy during defence counsel's cross-examination of Sgt. Rostie concerning the various checked boxes under "Privacy Scan Settings" at page 2 of the interface at Exhibit 15:

Q So is it your understanding that when you opened this particular program up, the Reg Clinic program, all of these are -- all of the checked-off boxes are done so -- you used the word -- term "by default," so it's done automatically by the program?

A From what I can tell, running it on the virtual machine, yes.

Q All right. And then-- but these other ones, the person has to include them or check them off, is that correct?

A Correct.

Q And similarly, internet browsing history, but Internet Explorer, Netscape, Opera, Firefox, but AOL's not checked off, so you'd have to check that off as well?

A Right.

Q Okay. Just moving on to page 3 --

A Yes.

Q -- and again, this is what pops up on the screen. For example, all of the things under "MS office history" are checked off?

A Yes.

Q And so that's how you saw it when the program came up and running?

A Correct.

Q And you don't have any prior familiarity with this program in terms of how it operates?

A That's correct.

Q So I guess we're operating under the assumption that this is how it does in fact operate --

A Yes.

Q -- is that fair?

A Yes. [Emphasis added.]

After it was agreed there was some "redundancy" between files selected in the "Windows cache and history" section of the program and "Document History", the following colloquy occurred:

Q And then the 'flush recycle bin', you said this would delete files and they would end up in unallocated space?

A Correct.

At p. 483 she was asked what her understanding of the word "cleaning" was in this context:

Q Okay. And your understanding of -- cleaning, you say, means deleted, is that correct?

A Correct.

Q And I take it you're ascribing that to your experience of what the vernacular for computers is, is cleaning rather than deleting files --

A Yes.

Q -- that that --

A Yes.

Q Those are one and the same --

A Yes. [Emphasis added.]

[48] She agreed at p. 484 of the transcript with the suggestion that she had no experience with "this particular software -- or computer cleaner" and did not know its level of effectiveness. She stated that she was not suggesting that "these type of cleaners have no effectiveness", and continued:

They'll -- they will often claim that they will clear all your traces of activity, but they usually miss something, because computers change so rapidly and -- and operating systems and software changes, the locations where they save things.

- [49] After further cross-examination, the witness was stood down and defence counsel asked to address the Court in her absence. He told the trial judge that it had become clear from Sgt. Rostie's testimony that the defence did not have all of the information that was available from the computers and that, for example, the list of "LNK" files that had been disclosed might not be complete. With no objection from the Crown, the cross-examination of Sgt. Rostie was adjourned from March 4 to March 10, 2020. By the time the trial resumed, defence counsel had received (presumably from the Crown) about 170 pages of "pathways similar to what we have". At the request of defence counsel, the trial was again adjourned to September 15, 2020.
- [50] On that date, defence counsel adduced into evidence a 46-page document headed "00C1LINK Files" as Exhibit 16, a 111-page document entitled "00C2LINK Files" as Exhibit 17, and a 19-page document entitled "Jump List" (associated with the laptop) as Exhibit 18. Under the heading "00C1 Link Files," Exhibit 16 recorded many diverse titles relating to church business, Mr. Vermeer's personal businesses, titles of recorded music, and some titles indicative of child pornography. At p. 250, four references consistent with child pornography stated "PCC Offsite" under the heading "Volume Name". Several more titles suggestive of child pornography were also listed: see pages 255, 260, 261, 262, 264, and 265 of the Appeal Books, most of which were also associated with the "PCC Offsite" heading. At AB 267, one of the entries stated "C:\Program Files (x86)\RegClean Pro\unins000.exe" and referred to a date in February 2013. Further references to "aMule" also appeared in conjunction with "PCC Offsite" at AB 269. Defence counsel's cross-examination of Sgt. Rostie from this point on focused on what he argued were anomalies in the dates shown under the headings "target file created" and "target file last accessed" in the exhibits.
- [51] As far as the hearsay question regarding Reg.Clinic was concerned, however, Mr. Maguire's evidence given earlier in the trial reflected a greater familiarity with Reg.Cleaner and Reg.Clinic than Sgt. Rostie's evidence. At p. 74 of the transcript, Mr. Maguire testified as follows:

Q This Reg Clinic program that we talked about earlier, does it operate within that registry file?

A Are you talking about the --

Q The Window registry?

A -- the Reg Cleaner Pro?

Q Yeah.

A So Reg Cleaner, the -- that tool in particular is most likely designed to go in and remove orphan registry files. So if it had found that Shareaza, for instance, was not installed on that computer anymore, it would look for potential registry keys to remove any of those entries. By doing that, it essentially keeps the computer a little bit cleaner, which in some respects helps it to run and operate faster.

Q So the -- it sort of removes unnecessary traces, things it had done to help a new program run? It is related to --

A Yeah. Like --

Q -- stuff that's been --

A -- once a program --

Q -- uninstalled, for example? You don't need bits and pieces anymore, so Registry Cleaner cleans those out?

A Correct. If -- if you don't need the program anymore, it -- it removes -- it removes all those little traces that are sometimes not removed through the --

Q Okay.

A -- removal process.

Q And that's the registry that we've just been talking about?

A A reg cleaner program would typically do that. There are other programs as well. [Emphasis added.]

[52] In light of the foregoing, I do not agree that the trial judge's findings that one of the functions of the Reg.Clinic program was to "delete" files, was based only on hearsay or an "assumption" made by Sgt. Rostie. The fact that Mr. Vermeer insisted in his testimony -- at least at first -- that Reg.Clinic deleted only "registry files" was not pursued or explained and in my opinion, must be read together with his evidence in cross that he was not familiar with the program; he had "just bought it". It did not preclude the judge from reaching her own conclusions based on all the evidence. I would not accede to this 'hearsay' ground of appeal.

Misapprehension of Evidence

[53] Mr. Vermeer's final ground of appeal is that in assessing his credibility and making other findings of fact, the trial judge misapprehended evidence and made "multiple reversible errors". (The defence also alleges under this rubric that the trial judge relied on hearsay evidence, but I have already dealt with that matter.) Counsel notes the Court's statement in *R. v. Morrissey* (1995) O.J. No. 639 (C.A.), (1995) 97 C.C.C. (3d) 193, that a conviction that rests on a misapprehension of the substance of the evidence adduced at trial means the accused has not received a fair trial and is therefore the victim of a miscarriage of justice. (At para. 93; see also *B.(C.)* at paras. 94-8.) The defence also notes that it is an error of law to make a finding of fact on the basis of no evidence, citing *R. v. J.M.H.* 2011 SCC 45 at para. 25.

[54] In his factum, the appellant cites a few particular ways in which the trial judge is said to have erred. First, the appellant argues the trial judge "misunderstood" the evidence about Reg.Clinic and made "speculative" findings of fact concerning it. The trial judge had stated at

para. 19 that Mr. Vermeer testified that he had purchased the Reg.Cleaner software a few days before April 20, 2015 and had used it to increase his computer's speed and efficiency. As we have already seen, the Crown adduced expert evidence (and the program interface) indicating that Reg.Cleaner could also be used to delete data from a computer. The trial judge found that Mr. Vermeer had used it for that purpose once he became aware of Empyryon's investigation. As well, the trial judge noted at para. 22 that although Mr. Vermeer claimed to have purchased the software only days before he used it in April 2015, the logs reviewed by Sgt. Rostie indicated that Reg.Cleaner had been deployed in 2013 and 2014 on Mr. Vermeer's computer: see the date 2/28/2013 appearing at AB 267, the date 9/23/2014 appearing at AB 270, and the date 1/5/2015 appearing at AB 273, all in Exhibit 16. Although Sgt. Rostie testified in chief that she had not detected any usage of Reg.Cleaner "in the past", this was prior to the disclosure and introduction into evidence of the log files that constituted Exhibit 16. (Exhibits 16-18 were, it will be recalled, adduced into evidence by the defence after the long break in the cross-examination of Sgt. Rostie.) Sgt. Rostie was not asked about Reg.Cleaner after the point at which Exhibit 16 was introduced.

- [55] The appellant contends that the judge made an adverse credibility finding against him because she did not accept his testimony that he had purchased Reg.Cleaner only a few days before he used it on April 20. She noted the evidence in the logs that he had used Reg.Cleaner as early as 2013. The appellant says the judge failed to appreciate that the cleaner he used in 2013 was a different version, Reg.Cleaner Pro, and that he had indeed purchased the version in issue, Reg.Clinic, only days before using it on April 20, 2015. Even if the judge failed to make this distinction, in my view it would not have amounted to a material error. The judge did not believe Mr. Vermeer primarily because his testimony that he did not know what the software did was inconsistent with his level of expertise, including his prior use of the similar software.
- [56] Second, the appellant asserts that the trial judge misapprehended the capabilities of Reg.Clinic. When Sgt. Rostie was asked in chief about the ability to delete files, she agreed with the suggestion that "sometimes when a file is deleted it's just sort of disconnected its name from its address so it can't find itself" and that "the image still exists and our forensic software can sometimes join them up if the file table entry hasn't been overwritten and if the file hasn't been overwritten." She agreed that generally, deleting a file would have to be done manually, but added that "there [is] some software that you can use, there's anti-virus or like we'll talk about later, Reg.Clinic that can delete certain files. But you still have to tell it to."
- [57] The appellant contrasts Sgt. Rostie's evidence with his own testimony that Reg.Clinic "does not delete actual physical files or data" but "cleans" one's registry. When asked by Crown counsel what the program does with the data that it cleans out, he said he had "... no idea how it processes, I don't know. I didn't write the program, I just bought the program." The following question and answer followed shortly thereafter:

Q All right. And Reg.Cleaner then can delete material out of those files. If it doesn't delete data, sir, how can it speed up the computer?

A Mainly system performance isn't necessarily reliant on junk and corrupt data so there's a number of factors that go into system performance so I mean, again, I can't comment on how the program writes or deletes or overwrites data that it -- or information that it doesn't require in order to operate smoothly, I don't know. [TS 603; emphasis added.]

[58] The appellant takes the position that his evidence concerning Reg.Clinic in fact corroborated Sgt. Rostie's evidence that Reg.Clinic could "delete certain files" but not "normal files" without the user's pushing a button to delete. (As may be seen from the Reg.Clinic interface, the program requires the user to press "fix all" and lists among the "system issues" that will be "fixed" the deletion of "sensitive and confidential information".)

[59] The trial judge reviewed the evidence of the experts and of Mr. Vermeer extensively in her reasons, both in connection with her credibility findings and her substantive findings of fact. She was aware of the distinction Mr. Vermeer sought to make between "registry files" and "normal files" but she was not convinced at the end of the day that Reg.Cleaner had not deleted files of which traces remained and which were suggestive of child pornography. I am not persuaded that the trial judge misapprehended any evidence in any material way or that she "speculated" or relied on matters not raised by counsel. There was evidence to support the conclusions she reached and no particular error of law or fact has been shown on her part.

[60] The judge also acknowledged some unanswered questions regarding "oddities" in the computer-based evidence, but since alternative explanations were suggested for them, she was satisfied they did not raise a defence or negate the Crown's proof of the essential elements of the offences. As she stated at para. 220:

The Crown evidence of Sgt. Rostie and the Empyrion technicians amply demonstrates that Mr. Vermeer downloaded and accessed the child pornography found in this investigation. Based on the evidence I accept, this is the only reasonable conclusion. I come to this conclusion despite the unexplained evidence about the dates of access on the laptop computer. In different situations this very well may have introduced a reasonable doubt. However, in this case there is an abundance of other evidence associating Mr. Vermeer to the illegal material. The reliability of the computer data generally is not fatally impacted because of the strong markers of consistency and internal integrity in the data as a whole. [Emphasis added.]

In the result, I would not accede to the third ground of appeal.

Disposition

[61] For these reasons, I would dismiss the appeal. We are grateful to counsel for their helpful submissions.

"The Honourable Madam Justice Newbury"

I agree:

"The Honourable Madam Justice Fenlon"

I agree:

"The Honourable Mr. Justice Voith"

Source & reproduction note

Judgment wording, source notices and original paragraph numbers are retained. Esheria supplies the layout and this PDF's page numbers; these are not the source pagination. This is a research copy, not an official or certified court document. Check quotations, citations and publication restrictions against the original source before relying on it.

ORIGINAL SOURCE <https://www.bccourts.ca/jdb-txt/ca/23/02/2023BCCA0206.htm>

CASE PAGE <https://chat.esheria.ai/case-law/canada/r-v-vermeer-2023>

Prepared on 29 October 2026 · Esheria