Proof and Progress: Coping with the Law of Evidence in a Technological Age

David M. Paciocco[*]

INTRODUCTION: THE PROBLEM AND THE GUIDING PRINCIPLES

The law of evidence was not designed to deal with new technologies. Its rules and principles were born in simpler times when the primary source of information was human memory of events communicated orally by God-fearing witnesses, and where copies of documents were penned by hand, commonly using quills. We are now trying to use the "modern issue" of these same rules and principles in a world where a telephone provides instant access to a library of information; where that phone can work like an ankle bracelet tracking the movements of its carrier; where records are stored not just on computers but in clouds; and data is transmitted instantaneously using invisible signals. It is not surprising that this causes enough disquiet to inspire judges to dedicate conferences to the problem of coping with new technology. It is important, however, to gain insight into why technologies rightfully make us uncomfortable enough to feel the need for retraining.

This insecurity exists not because the law of evidence is out-dated or difficult to apply to new technologies. The root of our insecurity is that many of us do not understand information technology, yet it is necessary to understand information technology to apply the law of evidence in an intelligent manner. The reason many of us do not understand information technology is that it takes many years to become jurists and even longer to become judges. This, of course, is my polite and indirect way of admitting that most judges are old enough to think that information technology is new and mysterious. We never trained the muscles in our thumbs to type 70 words a minute, we do not think in Boolean logic, and we simply cannot relate to the openness of younger generations who are prepared to post their most intimate and personal moments on social media and tweet their every move. Most of us still crave the musty smell of law books in libraries and some of the more eccentric among us miss leafing through citators — okay, at least one of us does. My point is that it is the technology and the brave new world that we do not understand. There is nothing in the law of evidence arising from these new technologies that should scare us.

I make this point not only to give some comfort to those of us who need to know the law and who already struggle with complex rules of proof. I make this point to underline that the challenge is not primarily to learn more law or new law, although there is some of that. What has to be learned are the functions and basic

---

[*] Ontario Court of Justice and Professor Emeritus, University of Ottawa. An earlier version of this article was presented at the Canadian Association of Provincial Court Judges Conference, 2012, cosponsored by the National Judicial Institute; it was also presented at the Alberta Provincial Court Judges Conference in May 2013.

operations of new technologies and the cultural changes that technological developments have inspired. A decade ago in *R. v. Rose* Fraser-Martin J. gently chided defence counsel who demanded hard copy disclosure because he was not computer literate.[1] The judge, with typical judicial understatement, said "it is probably now incumbent on those of us who are of a somewhat older generation to get with the program." He noted by way of example that the Statutes of Canada are no longer published in hard copy, and he called this "progress." His point, of course, is that those who will not learn will be left behind. Information is the stock and trade of the business of law and information technology is ubiquitous. Electronic filing is becoming a mundane requirement for lawyers. And yellow pads are no match for iPads as court tools. As a result, law societies now recognize it to be a professional obligation to stay sufficiently attuned with new technologies to be able to serve the needs of clients in an electronic world.

The same ethical obligation applies, no doubt, with equal intensity to professional judges. We don't have to post pictures of our drunken revelry on social media to "get with the program" but we do need to know what "social media," including Facebook, is, and how it works. We need to know that Twitter is not one of the seven dwarves. We need to accept that our phones are smarter than we are and we need to know why. And we need to know when we are posting information on a cloud, and what that entails. If we do not, we will not have the context and comprehension required to cope.

The second reason why it is important to appreciate that the real challenge lies in our lack of familiarity with new technology is that, if the state of the law is blamed, the law will be vulnerable to unnecessary reform which can only increase its complexity. Our rules and principles of evidence do not have to be retooled to cope with this brave new world. With rare exception, most evidentiary rules and principles apply the same way to new technology as they did in simpler times. This is because it is not information that has changed. The change that has occurred through new technologies is in the mode of delivery of information, and its ease of access.

The only rules that needed recalibration to deal with this relate to mundane matters such as authentication and the antiquated "best evidence" rule, a rule that had already lost its teeth more than 50 years ago with the advent of the Gestetner. As will be explained, the approach to expert evidence has also been modestly revised in Ontario to ensure that evidence generated using new technologies is accessible and efficiently received. It is also possible that changes to our social conception of privacy wrought by the ubiquity of information technology will impact on the law of privilege and the ultimate admissibility of seized information. Beyond this our base rules and principles relating to things such as judicial notice, hearsay, character, and judicial discretion require no refinement. They are fine the way they are. The law of evidence as we know it can be invoked to cope with technological evidence without the need for reconstructive surgery.

This is not to say that evidentiary rules and principles do not have to be applied in an accommodating way. If a rigid and narrow approach were to be taken it

---

1 *R. v. Rose*, [2002] Q.J. No. 8339, 2002 CarswellQue 2936 (Que. S.C.); leave to appeal refused 2003 CarswellQue 67 (S.C.C.).

could result in the exclusion of much information created with or collected by new technology. As absurd as it now sounds, for years we debated whether photographs and video-recordings were evidence, trying to treat them as if they were visual aids to assist testimony. We now accept, with good reason, that photographs and video-recordings can be used as "silent witnesses" in preference to testimony.[2] When we started storing data on computers some courts initially rejected computerized documents, being intimidated by continuity concerns and feeling insecure about what computer generated thing would constitute the "original" record. Would it be a print out, or must it be a copied file, or the hard drive? For a time we feared the use of technology by lawyers in court to display information, even though PowerPoint and computer generated documents can aid in the presentation and comprehension of a case. The point is that fear of what is new cannot be allowed to impede the incorporation of newer technologies. After all, law is a practical discipline and it functions in the real world. It would be unrealistic to reject electronic documents and emails, notwithstanding realistic fears of ease of manipulation. Similarly it would be unrealistic to deny privilege because of concerns arising from the insecurity of data storage. And, as already intimated, it will become unrealistic in the long run to stick to rigid and narrow ideas about expectations of privacy when dealing with information pirated from social media.[3] We need to leave our rules and principles open enough to accommodate new technologies and the culture they bring about, lest the law of evidence become irrelevant. To achieve this we will, for example, have to find comfort in weighing rather than excluding evidence to cope with continuity concerns. We will also have to take a functional approach to judicial notice and expert evidence lest our trials get bogged down or defeated by insistence, where it is not truly required, that technological experts testify. Ultimately the law of evidence is a tool-kit used in a practical enterprise — the resolution of conflicts through adjudication. It has to operate in the real world as it is, not as it was. We will make it fit because we must, but take heart in knowing that the changes required are modest at best and few are conceptual or elusive.

This article outlines those rules of evidence that are most likely to be called upon to fit new technologies. It identifies some of the challenges that are presented, and identifies modest techniques or suggestions for coping. Those suggestions include taking the kind of relaxed view as to when expert evidence is being offered illustrated by the Ontario Court of Appeal in *R. v. Hamilton*;[4] taking a functional approach to judicial notice; ensuring that authentication and the "best evidence" rule for electronic records are not applied in a highly technical fashion; understanding the law of hearsay and remaining familiar with key hearsay exceptions; apply-

---

2 See *R. v. Nikolovski*, [1996] 3 S.C.R. 1197, 1996 CarswellOnt 4425, 1996 CarswellOnt 4426 (S.C.C.).

3 *United States v. Jones*, 565 U.S. ....., 132 S.Ct. 945 (2012) (Slip Opinion per Sotomayor, J., concurring).

4 See *R. v. Hamilton*, [2011] O.J. No. 2306, 2011 CarswellOnt 3491 (Ont. C.A.); leave to appeal refused 2012 CarswellOnt 10888, 2012 CarswellOnt 10889 (S.C.C.); leave to appeal refused 2012 CarswellOnt 10890, 2012 CarswellOnt 10891 (S.C.C.); leave to appeal refused 2012 CarswellOnt 10921, 2012 CarswellOnt 10920 (S.C.C.); leave to appeal refused 2012 CarswellOnt 10892, 2012 CarswellOnt 10893 (S.C.C.) [*Hamilton*].

ing the law of privilege in ways that reflect the new realities that compromise privacy; understanding the limits of character evidence and the opportunities for the exclusionary discretion; and recognizing the utility in the technological presentation of evidence.

I. ADAPTING THE LAW TO NEW TECHNOLOGIES: THE MOST AFFECTED RULES

(a) Expert Evidence and Testimony by those with Special Knowledge

Put in its simplest terms, "expert evidence" is offered by those who are trained, to those who are not. As a result, the more training that occurs in our society, the greater that the opportunities for expert evidence become. And so it is with technology. The increase in learning that accompanies technological innovation increases the amount of expert evidence that will be offered in the courts.

Without question technological advances have enriched the pool of helpful information. Most notably, new forms of "technological forensic evidence" are being offered by experts. DNA evidence is the most important example, but there are a wide range of analytical and diagnostic techniques that are now being employed to resolve cases. And the ground is still breaking. For example, phylogenetic testing to determine "evolutionary distance" was admitted in the HIV infection case of *R. v. Aziga*[5] as circumstantial evidence linking Aziga to the infection of complainants. In *R. v. Tremble* "real time PCR Polymerase Chain Reaction DNA," a new form of DNA testing, was offered but rejected as its reliability was inadequately demonstrated.[6] Motor vehicle EDT (Electric Data Recorder) or "black box" evidence is commonly presented in motor vehicle cases.[7] Meanwhile, computers can be used by persons with expertise to generate demonstrative evidence,[8] including computer animations that go well beyond the charts and graphs once relied upon, and enrich the trial process.

Then there is "computer by-product evidence." The simple use of computers and similar devices generates a treasure trove of forensically useful information that can be offered to courts by persons with special knowledge. Those with training can use coded Internet Service Provider information to identify the computers another computer has communicated with. The origin of websites that have been visited can be traced. The date computer documents were created or modified can

---

5 *R. v. Aziga*, [2008] O.J. No. 5131, 2008 CarswellOnt 7630 (Ont. S.C.J.)

6 *R. v. Tremble*, [2010] O.J. No. 5957, 2010 CarswellOnt 11085 (Ont. S.C.J.); additional reasons 2010 CarswellOnt 4071 (Ont. S.C.J.)

7 See, for example, *R. v. Delorey*, [2012] N.S.J. No. 90, 2012 CarswellNS 122 (N.S. C.A.)

8 See, for example, *R. v. Suzack*, [1995] O.J. No. 4237, 1995 CarswellOnt 1350 (Ont. Gen. Div.); affirmed 2000 CarswellOnt 95 (Ont. C.A.); leave to appeal refused 2001 CarswellOnt 1076, 2001 CarswellOnt 1075 (S.C.C.); *R. v. Scotland*, [2007] O.J. No. 5305, 2007 CarswellOnt 8877 (Ont. S.C.J.).

be determined, and so can the last time the computer was logged into or shut down.[9] Information hidden or previously deleted can often be resurrected.[10]

Of course it is a good thing when expertise improves knowledge and therefore the accuracy of fact-finding. Yet expert evidence comes with a price. It is typically time-consuming, raising trial efficiency and cost issues. It is most often expensive, raising important access to evidence issues. Expert evidence is also capable of distorting outcomes. Expert evidence is not always accurate evidence, but it is difficult to challenge and assess given its technicality and the daunting credentials of many expert witnesses.

It is important, for these reasons, that expert evidence and expert evidence rules be neither underused, nor overused. Most attention has been given in the law of evidence of late to preventing its overuse. Judges have been cautioned repeatedly to be vigilant gatekeepers[11] to prevent unreliable, unnecessary, or prejudicial expert evidence from being admitted.[12] Yet judges also need to avoid complicating trials with unnecessary and unhelpful *Mohan* admissibility *voir dires*.[13] It is not an easy matter to achieve an appropriate balance. As always, practical thinking can guide the way.

To assist in this exercise it is helpful to recognize that technological information comes in different forms. It includes not only the "technical forensic evidence" and "computer by-product evidence" I have described. There is also what I call "mundane technology evidence."[14] "Mundane technologies" are the day-to-day uses to which information technology is put. It includes the use of social media such as Facebook and Twitter; the operation of search engines to retrieve data; the operation of computers, tablets, and smart phones; and the use of digitized technology to take and edit photographs, digitized movies, and audio-recorded information, including computer stored 911 calls. These are things that require special training to use or understand, yet they are not the stuff of expert evidence. No *Mohan* vetting is required before testimony about their use or operation is offered. For example, no expertise is required to explain Facebook to a judge, including how it works or how access is granted, or how messages are posted, sent, or re-

---

9 See, for example, *R. v. Winchester*, 2010 CarswellOnt 397, [2010] O.J. No. 693 (Ont. S.C.J.).

10 See, for example, *R. v. Bishop*, 2007 ONCJ 441, 2007 CarswellOnt 6385 (Ont. C.J).

11 *R. c. J. (J.-L.)*, [2000] 2 S.C.R. 600, 2000 CarswellQue 2310, 2000 CarswellQue 2311 (S.C.C.), at para. 28.

12 This trend began, of course, in the leading decision in *R. v. Mohan*, 1994 CarswellOnt 66, 1994 CarswellOnt 1155, 29 C.R. (4th) 243 (S.C.C.) [*Mohan*].

13 In *R. v. Abbey*, [2009] O.J. No. 3534, 2009 CarswellOnt 5008 (Ont. C.A.); leave to appeal refused 2010 CarswellOnt 4828, 2010 CarswellOnt 4827 (S.C.C.) an improved analytical structure was developed for *Mohan* expert evidence *voir dires* that involves exploring whether four straight forward prerequisites are satisfied before balancing the costs and benefits of admission. For a more complete discussion see David M Paciocco & Lee Stuesser, *The Law of Evidence* (6th ed), (Toronto: Irwin Law, 2011) at 193–201 [Paciocco & Stuesser, *The Law of Evidence*].

14 I am not suggesting there is a legal rule that uses this structure or that there should be. I am offering a heuristic or model for making sense of the role of expert evidence and technology.

ceived. Any witness who uses Facebook can offer this information. Similarly, iPhone users can explain what "apps" are and what use they make of them, without furnishing expert evidence. Ultimately courts requiring help in understanding "mundane technologies" can rely on ordinary members of the public to describe those uses that ordinary members of the public make of the technology in question. It is only when subjects move into the more rarified and technical questions, such as what time and date stamps attached to messages signify, that ordinary witnesses are not apt to have the expertise to assist.

It can be protested that individuals who acquire knowledge that is held solely by those who are users of technology are in some sense "experts" because what separates expert witnesses from lay witnesses is "special skill or knowledge," whether acquired through formal training or not.[15] Yet those who understand and use mundane technologies are not expert in any real sense. "Experts" are those with "*special*" skill or knowledge. The "special" qualification connotes exclusivity or uniqueness. The ability to understand and use commonplace technology is not special. Moreover, experts possess skill or knowledge "beyond the ken of ordinary people."[16] The simple fact that many will not have knowledge or skill does not put it beyond the ken of ordinary people. The ordinary person, like the reasonable person, is a fictitious objective measure. And like the reasonable person, the ordinary person is not found at the ends of the spectrum. Ordinary persons are a composite of people generally, including those with easily acquired skills and knowledge, even when not possessed by others.

In spite of this there is an understandable but unfortunate tendency to engage the expert evidence rules and conduct a *voir dire* whenever anyone sets about to explain anything that not everyone will know. In *R. v. Pelich*[17] for example, a *Mohan* expertise *voir dire* was conducted to determine whether a police officer working in the child pornography section could explain how "LimeWire" peer-to-peer file sharing worked. "LimeWire" is widely available software designed to be accessible to computer users and arguably did not require expertise to explain. Similarly, in *R. v. Pasqua*[18] an expert evidence *voir dire* was held before allowing computer enhanced photos to be presented. The officer who did the enhancement was not purporting to identify a doctored photo or video, something that would truly have required expertise. He had used software to improve security images, software that employed the same technology that is available commercially and

---

15 See *Mohan*, *supra* note 12. In *R. v. O. (N.)*, [2009] A.J. No. 213, 2009 CarswellAlta 288 (Alta. C.A.), for example, the Alberta Court of Appeal commented that "The designation of expert is a modest status that is achieved when a witness possesses special knowledge going beyond that of the trier of fact [in the subject of the proposed testimony]."

16 See, for example, *R. v. Sekhon*, 2012 BCCA 512, 2012 CarswellBC 4005 (B.C. C.A.) and *R. v. Lewis*, 2012 ONCA 388, 2012 CarswellOnt 7105 (Ont. C.A.) as contemporary examples of where the "beyond the ken of ordinary" people standard is applied. See *R. v. Currie* (2002), 166 C.C.C. (3d) 190, 2002 CarswellOnt 1841 (Ont. C.A.) at para. 67, ; leave to appeal refused 2004 CarswellOnt 440, 2004 CarswellOnt 439 (S.C.C.) for a general discussion of when expert evidence may be necessary.

17 *R. v. Pelich*, 2012 CarswellOnt 6875, [2012] O.J. No. 2467 (Ont. S.C.J.).

18 *R. v. Pasqua*, 2008 CarswellAlta 221, [2008] A.J. No. 184 (Alta. Q.B.).

which requires no specialized knowledge or training to utilize. Arguably no expert evidence was at stake in what he was offering.

The concern for overuse of *Mohan voir dires* where technological evidence is offered is not just a question of efficiency. It is also a question of credibility. The repute of the administration of justice could not endure, in this modern age, courts that refuse to recognize and utilize technologies that are widespread and mundane. Risking exclusion by conducting *Mohan voir dires*, or setting up appeal opportunities by requiring them to be had is contrary to the public interest. Courts must conduct their business effectively and realistically.

This kind of practical thinking appears to have inspired the Ontario Court of Appeal in *R. v. Hamilton*.[19] The trial judge permitted representatives of cellphone service providers to testify and use cellphone tower records to triangulate the location of particular cellphones at the time of a shooting. These witnesses explained the technical principles that operate to route cellphone calls to particular towers[20] and interpreted computerized records to permit the triangulation. The Crown had sought to qualify the representatives as experts to give this evidence but the trial judge admitted the evidence without a *Mohan* inquiry. The Ontario Court of Appeal upheld that decision, saying:

> Even if evidence about the general rule [that cell phones use the closest tower] and its exceptions could at one time have been considered opinion evidence, it is now simply factual evidence that witnesses with the knowledge and experience . . . can testify about. [These witnesses] were not proferring a novel scientific or behavioural theory that was open to debate. They were testifying about uncontroversial facts related to the operation of cell phone networks.[21]

The significance of the *Hamilton* decision is unclear. It is unlikely that the Court intended to reserve expert evidence scrutiny solely for cases where overt "opinions" are offered, regardless of the special training it may take to make and offer relevant factual observations. It is doubtful, for example, that a lay witness could qualify to describe the algorithms used in a computer program, even if no expression of opinion is involved.[22] Nor is it likely that the Court intended to confine the application of the expert evidence rule to "novel scientific or behavioural theory." Established rules of expert evidence apply to all evidence that requires

---

19 *Hamilton*, *supra* note 4.

20 These witnesses were allowed to explain the basic principle that an operating cell phone will register at the tower with the strongest signal, which will be the closest tower, unless: (1) the closest tower is at capacity; (2) there is a body of water between the cell phone and the closest tower; or (3) there is a large obstruction such as multi-story building between the cell phone and the closest tower, in which case a more distant tower with an unobstructed line of sight or a flat path of elevation may end up serving the cell phone.

21 *Hamilton*, *supra* note 4 at para. 279.

22 The inaptly named "expert opinion evidence" rule has long been applied to factual observations both because the line between fact and opinion is unreliable, and because there are factual observations that require special skill and knowledge to understand, observe, and explain, raising most of the risks that expressions of expert opinion present.

special education or training that goes beyond the ken of ordinary persons, with more intense application in the case of "novel scientific or behavioural theory."[23] It is best to read *Hamilton* as holding that a full-bore *Mohan voir dire* may not be required where the kind of evidence in question is familiar to courts, where it is presented as circumstantial evidence rather than as a direct opinion on an issue to be decided, and where it is based on uncontroversial principles that can be easily understood. The subsequent decision in *R. v. Cyr*,[24] again dealing with "cellphone propagation maps" that merely plot the locations from which calls could have been made, endorsed the *Hamilton* approach but confined its application. On the facts, the decision to admit the evidence without a *voir dire* was upheld in large measure because the trial judge addressed an issue of unreliability arising from an error rate as high as 40% by assessing whether the evidence was probative enough to admit, the same kind of inquiry that *Mohan* would have required. Justice Watt also qualified *Hamilton* by noting that "More precise evidence may require expert opinion."[25]

The *Hamilton/Cyr* rationale may press the edges of the traditional law of expert evidence, but the cases are poignant examples of what can be expected in matters of technology. Courts will accommodate it unless there are real concerns about its reliability, and they will be practical in the approach that is taken.

Even when a *Mohan voir dire* is truly needed, it is important to conduct it efficiently There is no need for court after court to plow the same ground. A threshold reliability inquiry, for example, need only be conducted where scientific or technological technique is still novel as a form of evidence before Canadian courts, or the party opposing admission provides a foundation for casting the reliability of the evidence into question.[26] Absent this, a court can take its cue from prior decisions and treat technological evidence that is becoming familiar before courts as sufficiently reliable to admit.

(b) Judicial Notice

Judicial notice, in my view, plays a central role in coping with new technology. Given the distrust many jurists have of judicial notice, a concise overview of judicial notice doctrines is warranted before the use of judicial notice in a technological world is explored directly.

Judicial notice occurs, of course, where a court relies on a fact that has not been proved through evidence. It is a functional doctrine designed to promote an efficient and sensible trial process. If a fact is notorious and incontrovertible there is no point in requiring it to be proved. The doctrine of judicial notice can also

---

23 *Mohan*, *supra* note 12.

24 *R. v. Cyr*, 2012 CarswellOnt 16386, [2012] O.J. No. 6148 (Ont. C.A.).

25 *Ibid.*

26 *R. v. Trochym*, 2007 CarswellOnt 400, 2007 CarswellOnt 401, 43 C.R. (6th) 217 (S.C.C.) at para. 31. "Novel evidence" has still not been authoritatively defined. The best approach is to treat evidence as novel, not when it derives from a new theory or technique within the profession, but where it is novel as a form of evidence before the courts. See Paciocco & Stuesser, *The Law of Evidence*, *supra* note 13 at 207–209 for a more complete discussion.

enhance the accuracy of trial outcomes. If a court could not rely on a notorious and incontrovertible material fact because it had not been proved, verdicts would not conform to reality. The repute of the administration of justice would be harmed.

In spite of its importance, the problem with judicial notice is that it is antithetical to the adversarial theory of litigation in which the parties bring forward the proof. Jurists are trained to let the parties control the record and are therefore suspicious of judicial notice. They tend to believe that judicial notice is rarely taken. In fact it is constantly taken.[27] No item of circumstantial evidence could be used unless jurists drew inferences from that evidence based on their understanding of unproved facts — things such as human behaviour, the observable and broadly understood laws of physics, and the functioning of the human organism. Judicial notice is taken repeatedly not only when drawing inferences from circumstantial evidence but also when understanding direct evidence. For example when someone describes putting the brakes on in a car no-one offers expert testimony that the function of brakes is to slow or stop vehicles, that brakes are typically controlled by foot-pedals that are depressed in order to slow or stop the vehicle, or that brakes are depressed gently to come to a gradual stop and aggressively for an emergency stop. The judge can picture the braking event testified to and understand its significance only by putting it into the context of relevant information not proved in evidence but which the judge and everyone else would readily know. Many facts not proved in evidence but required to understand those facts that have been proved in evidence enter the picture in this way, often almost subconsciously, and they are used in resolving cases.

No-one should therefore be afraid of judicial notice. Without it, the process would not function. The only caveats are related to the need for judges to respect the adversarial system and the need to maintain the appearance of justice.

First, judges should take judicial notice only of those facts and propositions of fact that are beyond reasonable controversy.[28] That way everyone will understand why proof has been dispensed with and no party can complain that the facts in question should have been the subject of adversarial debate.

Moreover, judges should take judicial notice only of facts that are "notorious."[29] The concern is that if a judge initiates information about facts and propositions that impact an outcome and the result favours one of the parties, the judge will appear to be biased. No reasonable apprehension of bias occurs, however, if those facts and propositions are so widely known that observers would accept them to be true beyond reasonable dispute. In such cases reasonable observers would understand why an adversarial contest was not invited.

Yet the reality is that levels of knowledge vary within a community, as does the degree of interest taken about court proceedings. So the law must be sensible. If something is broadly known that will be enough, even if it is not universally

---

27 I discuss the reality that judicial notice is commonly taken in "The Promise of *R.D.S.*: Integrating the Law of Judicial Notice and the Apprehension of Bias" (1998) 3 Can Crim L Rev 319 at 326–328.

28 *R. v. Spence*, 2005 SCC 71, 2005 CarswellOnt 6824, 2005 CarswellOnt 6825 (S.C.C.) [*Spence*].

29 *Ibid.*

known. It is also acceptable if the fact or proposition is confirmed in commonly consulted sources that are trusted to be accurate.[30]

Finally, judicial notice operates on a sliding scale. It has to in order to function. The more central the matter judicially noted is, the stricter the requirements of "indisputability" and "notoriety."[31] The requirements are strict when it comes to centrally important facts that impact on the ultimate findings of fact in the case.[32] When it comes to more peripheral matters such as the propositions required in order to understand and to draw inferences from evidence that has been led, the standards are not exacting.[33]

Without generous reliance on judicial notice the sensible resolution of disputes would be impaired, adversarial principles notwithstanding. It would also make it next to impossible for courts to adapt to new technologies. It is important to bear in mind that if judges cannot use judicial notice to work with evidence produced by new technology, it may become necessary to call expert witnesses to assist, which impedes the efficient and cost-effective administration of justice.

That is why I have concerns about broad statements made in pockets of Canadian case law that "courts cannot take judicial notice of functioning of machines."[34] While there are functions that machines perform that certainly do require expert evidence, courts take judicial notice of the functioning of machines routinely. Take the telephone for example. No-one would think it necessary to call evidence about the functioning of a telephone. Everyone understands that individuals have assigned telephone numbers that are exclusive to them, that telephones are dialled to

---

30 A lesser known foundation for notoriety was endorsed in *R. v. Cobham*, [1994] 3 S.C.R. 360, 1994 CarswellAlta 748, 1994 CarswellAlta 326 (S.C.C.). The Court said that the availability of duty counsel was so notorious among criminal lawyers and judges that Cobham did not have to lead evidence of its availability in order to maintain a *Charter* challenge based on the failure of the police to notify him of the availability of free immediate legal assistance. The unspoken theory has to be that what is widely known in the justice system is information that can readily be known by members of the public with an interest in the matter. Canadian courts have been reluctant to use this authority.

31 *Spence*, *supra* note 28 at para. 60.

32 *Ibid.* at para. 62.

33 It is similar thinking that makes me feel liberated enough to rely in this paper on "Wikipedia" as authority for mundane explanations about basic matters such as the functioning of telephones, and the difference between analog and digital transmission. While it would be more perilous to consult Wikipedia on politically charged or esoteric matters, it is a convenient, readily accessible, and reliable enough source to warrant using for secondary or illustrative purposes.

34 See *R. v. Newton* (August 30, 1996), [1996] O.J. No. 5360, Flaherty Prov. J. (Ont. Prov. Div.) and *R. v. McCoy* (December 3, 2004), [2004] O.J. No. 6224, F.L. Forsyth J. (Ont. C.J.). I want to thank Aaron A Fox, QC, for drawing these and some of the other cases referred to in this section to my attention. The *Newton* and *McCoy* decisions are no doubt correct because they dealt with the synchronization of red and green lights in the particular traffic lights in question. The issue I have is with the overbreadth of the courts' suggestion that "the functioning of machines" is taboo when it comes to judicial notice.

make contact, and that they need to be answered either manually or mechanically for that contact to occur. When we accept the testimony of a witness that they were speaking to a particular individual by telephone we rely on our knowledge that voices can be transmitted by telephone instantaneously or with only immaterial delay. And if a witness testifies that they observed the caller's number on their phone display we understand that the number displayed during a call is related to the phone being used by the caller. If the witness testifies to a phone message that has been recorded we listen without adverting to our basic understanding that phone messaging devices are capable of capturing "a voice" instantaneously, as it is speaking. Courts also take judicial notice about the ability of phones to accurately recreate the sound of particular human voices. No-one questions this even though modern phone systems digitize and then decode sound waves during transmission in much the same way that computers convert information into code to be reconstituted as legible or audible data when displayed or broadcast,[35] a point I will return to below when discussing the "best evidence" rule for computer records. So long as someone testifies that a voice was heard on a telephone, it is simply accepted that the phones and transmission services were functioning properly. This is as it should be. Courts could not function without taking judicial notice of the functioning of machines, including in this day and age of computers, emails, text messaging, and the like.

Not surprisingly, this is happening. Documents secured by computers are received without evidence about the capacity or function of computers or how computer evidence is generated. Email correspondence is admitted without lessons relating to the functioning of emails. And the same holds true of text messages. Even more sophisticated technological aspects are noted. In *R. v. Woodward*,[36] for example, the Ontario Court of Appeal took judicial notice that all computers work using logic functions. And in *R. v. Ranger*[37] the Ontario Court of Appeal accepted that a trial judge could take judicial notice that cell phones are being operated in the general geographical location of the cell phone towers that receive their transmissions, even without the technical testimony offered in *R. v. Hamilton*.[38] The Court also accepted that "cell phone users engaged in a cell phone call who are travelling from point A to point B will find their cell phone signal passes from one cell phone tower to another at different locations along the route from Point A to Point B."[39] This makes it possible for a trial judge to infer that at a particular point in time a cell phone user was in a location generally proximate to the tower (such as downtown Ottawa) and that the user was travelling in a given direction over a given period of time. These are incredibly generous propositions of judicial notice but they are pragmatic and safe applications of the doctrine.

To understand how important it is to take a functional approach to judicial notice consider the example of Google Maps. These helpful documents have be-

---

35 "Telephone" *Wikipedia*, online: Wikimedia Foundation <http://en.wikipedia.org/wiki/Telephone>.

36 *R. v. Woodward*, 2011 CarswellOnt 9823, [2011] O.J. No. 4216 (Ont. C.A.).

37 *R. v. Ranger*, 2010 CarswellOnt 8572, [2010] O.J. No. 4840 (Ont. C.A.) [*Ranger*].

38 *Hamilton*, *supra* note 4.

39 *Ranger*, *supra* note 37 at para. 16.

come ubiquitous in court. Indeed, in *R. v. Calvert*[40] the trial judge reviewed a Google map on his own initiative to ascertain the distance between the scene of arrest and the police station to determine whether a breath sample had been taken as soon as practicable. The Ontario Court of Appeal was fine with this since "generally speaking maps may be relied on by courts when taking judicial notice because maps are a readily accessible source of indisputable accuracy."[41] The fact that this particular map was downloaded by computer — that it would have been input and then converted to code and then reconstituted by elaborate technology into a discernible image before being displayed and printed — gave the Court no reason to pause. A map is a map, and a map service that is widely recognized and relied upon by ordinary persons as authoritative is a reliable enough source to admit its products into evidence. *Calvert* makes clear that judicial notice is the key doctrine relied upon to access this important litigation tool, even if courts rarely pause before admitting Google Maps to question their authority.

The same principles would apply to Google Earth images. In a case I was presiding over a self-represented accused wished to admit into evidence satellite images he had downloaded. He had images taken on two occasions to show changes in the terrain relevant to the case. The Crown objected as there was no-one there to authenticate the images or verify the date stamps. The self-represented accused was incredulous. He said that his township no longer sends building inspectors but relies on Google satellite images taken over time to verify compliance with municipal work orders and zoning restrictions on new construction. The public readily consults Google Earth images, a widely known service. And he could testify to the accuracy of the structures and road configuration depicted, verifying that the Google satellite images called up were the one's sought when the search was conducted. I admitted the satellite images without any evidence confirming the process by which they were captured.

Without taking a functional approach to technology that enables courts to educate themselves about and rely on the basic properties and capacities of technology, courts would either have to lose step with the real world, or pointlessly increase their dependency on expert evidence and foundational technical evidence to get things right.

(c) Electronic Records, Authentication and the Best Evidence Rule

(i) Overview

There is a network of rules relating to the proof of documents secured from computers and similar devices. Together these rules appear to be complex. In fact, if interpreted sensibly the electronic document rules rarely impede admission and can be dealt with efficiently, even summarily.

The statutory provisions about to be examined create two special hurdles where electronic documents are being offered — authenticity rules and "best evidence" rules. As will be seen, the statutory authentication rule mirrors the common law rule for ordinary documents. It adds nothing of significance.

---

40 *R. v. Calvert*, 2011 CarswellOnt 3470, 2011 ONCA 379 (Ont. C.A.).

41 *Ibid.*

As for the "best evidence" rules, their name is misleading. At common law "best evidence" rules are designed to promote the use of original documents. The best evidence rules applicable to electronic documents from computer and similar devices are not concerned with requiring original documents to be proved, but instead seek to ensure that an electronic document offered in court accurately reflects the original information that was input into a document. To be clear, these best evidence rules are not concerned with whether the original information that was input was accurate information. Documents containing inaccurate information, even a completely forged document offered as a genuine document, can satisfy the best evidence rules. The electronic best evidence rules are concerned with what might happen after the information has been input.

As indicated, each provision is facially intricate but they are not difficult to satisfy. Two of the best evidence avenues are particularly simple, and widely available. First, if someone familiar with the information originally input testifies that the document being offered accurately records that information, authenticity and best evidence standards will have been met, for this is evidence that the computer system, having faithfully reproduced the information, must have been functioning as it should.

Alternatively, if a document appears on its face to be what it is claimed — for example, an email or a text — testimony that it is the document that was received or sent by email or text will be presumed to satisfy the authenticity and "best evidence" requirements, unless the opposing party raises a doubt about whether the computer system was operating properly. Again, the apparent coherence of the document coupled with the fact that it was produced or retrieved in the fashion that a functioning computer would produce or retrieve documents is evidence that the electronic document system was functioning as it should.

The relevant provisions, about to be described, do not lay any of this out in simple terms, but interpreted sensibly this is all they require, leaving the law simple, accessible and practical.

(ii) The Statutory Regime and its Role

Like most provincial evidence statutes, the *Canada Evidence Act* has provisions addressing issues related to the admissibility of "electronic documents."[42] This is where the rules I have just introduced can be found.

To be clear, subsections 31.1 to 31.8 do not authorize the ultimate admission of electronic documentary evidence. These provisions deal solely with issues concerning the integrity of the document being offered as proof, not with the admissibility of the document's contents. "These sections must [therefore] work in conjunction with either some common law general rule of admissibility of documents or some other statutory provision"[43] in order to make the document admissible.

For example, in *R. v. Morgan*[44] the Crown wanted to admit documents secured from Department of Fisheries and Oceans computers showing the status and

---

42 *Canada Evidence Act*, R.S.C. 1985, c. C-5.

43 *R. v. Morgan* (January 10, 2002), [2002] N.J. No. 15, Flynn Prov. J. (N.L. Prov. Ct.) [*Morgan*].

44 *Ibid.*

terms of Mr. Morgan's fishing licence. Sections 31.1 to 31.8 were used to resolve authentication and "best evidence" concerns while the business records exception in section 30 of the *Canada Evidence Act* was used to permit the records to be used as hearsay proof of their contents. It is helpful to consider it this way. The evidence did not consist of "electronic records" *per se*. Electronic records were merely the delivery mechanism for the evidence, namely the information about Mr. Morgan's licence. Section 31.1 to 31.8 deal with the propriety of the delivery mechanism for evidence. They do not determine whether the evidence being delivered is itself admissible. Other relevant rules, such as the hearsay rule or the opinion evidence rule, will determine this.[45]

(iii) The Reach of the Statutory Regime

Subsections 31.1 to 31.8 apply solely to "electronic documents." The definition is broad enough to cover copies of all documents stored in a computer, such as business records, bulletin boards from Facebook or other social media, emails and or "tweets" (being messages exchanged using Twitter). Subsection 31.8 defines "electronic document" as follows:

> "Electronic document" means any 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, a printout or other output of that data.

This is a definition of imposing breadth, particularly when combined with the definition of "data" in subsection 31.8 — "representations of information or of concepts, in any form." The statutory provisions do not therefore catch only documents in the conventional sense. They also catch at least some audio and video recordings. In *R. v. Nichols*,[46] for instance, the Court applied these provisions to a 9-1-1 tape, presumably stored and retrieved from a computer.[47]

---

45 By the same token, the authenticity and best evidence requirements for electronic documents do not become immaterial because other rules may provide for admission of documents. These rules address different evidentiary issues. In *Morgan*, *supra* note 43 it was arguably incorrect for the Court to treat the provisions in subsection 30(3) of the *Canada Evidence Act* for the filing of copies as an alternative basis for admitting the electronic records that were offered into evidence. The generic provision for copies in subsection 30(3) applies to otherwise admissible documents. If those documents are electronic documents they are not otherwise admissible unless the requirements of subsections 31.1–31.8 are met.

46 *R. v. Nichols*, [2004] O.J. No. 6186, 2004 CarswellOnt 8225 (Ont. C.J.).

47 In *R. v. Adams*, 2011 CarswellNS 363, *(*sub nom. *R. v. Murphy)* [2011] N.S.J. No. 302 (N.S. C.A.) the Court resolved the admission of a CD of photographs without resolving compliance with subsections 31.2-31.8 of the *Canada Evidence Act* because the application of those provisions was not argued at trial.

While these provisions would appear to apply to "digitized" recordings,[48] "analog" recordings[49] captured by conventional audio and video recorders should not qualify as "electronic documents." They are not recorded or stored "on any medium in or by a computer system or other similar device."

Not only is the definition of "electronic document" too narrow to catch data stored using analog technology, the most significant "electronic document" provisions address concerns about the integrity of documents that have been converted from code so that they can be read or perceived by a person. Analog recordings do not use code. They imitate the conditions that created the sound or image. Analog devices therefore do not create the same mischief that most of the "electronic document" provisions are meant to address.

As the definitions of "electronic document" and "data" reveal, these provisions are also broad enough to catch data secured from computers or captured from smart phones or similar devices, even if not saved in the form of self-contained documents. *R. v. B. (L.)*[50] illustrates the point. There the Crown wished to tender selected information produced and assembled by Telus from its computer records as a result of a production order. The defence objected that this was not admissible because no existing document contained the information. The printout was created from diverse information contained in the computer, assembled into a single document printout as a result of the police investigation. The Court held that the printout was an "electronic document" as defined in subsection 30.8 even though it had not previously been in document form because the definition speaks not of documents *per se* but of "data that is recorded or stored." This data fit the bill.[51]

The definition of "electronic document" is also broad enough to permit a court to use directly as evidence the information that is stored on a computer system rather than a printout of the data of the contents of the system. This is because the definition of "electronic document" "includes a display." For example, subject to other rules of admissibility a judge is free to rely on these provisions to have the data on a smart-phone called up and read into the record from the witness stand, or

---

48 Digitization occurs "when diverse forms of information such as text, sounds, image or voice are converted into a single binary code." These codes are stored in a computer system or other similar device and can be reconverted and displayed in the form of reproductions of the recorded texts, sounds, image or voices: "Digitizing" *Wikipedia*, online: <http://en.wikipedia.org/wiki/Digitizing>.

49 An analog recording is a created by capturing changes in physical phenomena (sound, light, temperature, position, pressure) using a device that imprints those changes. The recording device can be mechanical or electronic and is able to recreate relevant sounds and images by recreating the same changes in physical phenomena that produced the sounds or images. There is no reconversion of data as there is in a computer system or other similar device: "Analog" *Wikipedia*, online: Wikimedia Foundation <http://en.wikpedia.org/wiki/Analog>.

50 2009 CarswellBC 2298, [2009] B.C.J. No. 1741 (B.C. S.C.)

51 Moreover, the collected data was admissible as a business record under section 30 of the *Canada Evidence Act* even though it was assembled for the prosecution. Since the record that was admitted simply collated existing data, it was not "a record made in the course of an investigation or inquiry," which would have been inadmissible under subsection 30(10).

to have data displayed in court from a computer system that has been made an exhibit, without violating rules of authenticity or "best evidence" considerations. A judge can no doubt, in their trial management discretion, insist on the production of copies where possible,[52] but this is not required.

(iv) Authenticity

(A) The test for authenticity

As indicated one of the functions of the electronic document provisions is to deal with the "authenticity" of electronic documents. This is the role of subsection 31.1, in particular. This provision does nothing more than repeat the "low"[53] common law authenticity standard. At common law authenticity is established for the purposes of admissibility if the trial judge is satisfied that there is some evidence to support the conclusion that the thing is what the party presenting it claims it to be. In *R. v. Donald*, for example, the New Brunswick Supreme Court (Appeal Division) described the common law standard by calling for "some apparently sound reason" in the evidence for believing the item to be authentic:

> Positive identification is not required. The fact an article has been admitted in evidence does not, of course, establish that it is the article involved. After its reception it is a question of fact to be determined by the judge or jury as to whether or not it is, in fact, such article.[54]

Section 31.1 embraces the same test:

> 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.

(B) Purpose-based Admissibility

In a book on documentary evidence Douglas Ewart cautioned that "when considering the admissibility of a document, it is important to keep in mind the purpose for which it is offered in evidence."[55] A document may be a forgery, but if it is being offered as proof of a forgery it can be authentic. "This is the very forged document that the accused relied upon." Do not confuse genuineness with authenticity. Is there evidence supporting a finding that the electronic document is the thing which it is purported to be?

---

52 The authority to do so is no doubt supported by the reasoning in *R. v. Felderhof*, 2003 CarswellOnt 4943, [2003] O.J. No. 4819 (Ont. C.A.).

53 Alan W Bryant, Sidney N Lederman & Michelle K Fuerst, *Sopinka, Lederman & Bryant The Law of Evidence in Canada*, 3rd ed, (Toronto: Lexis-Nexis, 2009) at para 2.14 [*Law of Evidence*] make this point citing *R. v. Staniforth*, 1979 CarswellOnt 45, [1979] O.J. No. 1026 (Ont. C.A.). In that case, even though a knife was only tentatively identified by a witness, its presence under clothes in a bedroom permitted it to be adduced in a case where the Crown alleged the victim had been threatened with a knife in the bedroom.

54 *R. v. Donald*, 1958 CarswellNB 4, 121 C.C.C. 304 (N.B. C.A.), at para. 7.

55 Douglas Ewart, *Documentary Evidence in Canada* (Toronto: Carswell, 1984) at 20.

(C) Authentication and genuineness

Evidence can be "authenticated" even where there is a contest over whether it is what it purports to be. This is so even though there have been situations where individuals have created false Facebook pages in the name of others, or where information has been added by others to someone's website or social medium home page,[56] and there have been cases where email messages have been forged.[57] These false documents may easily gain admission under the rules. If the party offering the electronic document offers evidence capable of supporting a finding that it is genuine, section 31.1 will be met regardless of the strength of the case to the contrary. This is not because the law is disinterested in false documentation. It is simply that the law prefers to see disputes about authenticity resolved at the end of a case, not at the admissibility stage. Disputes over authenticity tend to turn on credibility, and credibility is best judged at the end of the case in the context of all of the evidence. "Authentication" for the purposes of admissibility is therefore nothing more than a threshold test requiring that there be some basis for leaving the evidence to the fact-finder for ultimate evaluation. In *R. v. Butler*,[58] for example, the Court recognized where there was a live issue about whether the accused generated the Facebook entries in question that would be for the jury to decide.

(D) Circumstantial Evidence and Authenticity

The authenticity of an electronic document can, of course, be established circumstantially. For example, in *R. v. Sandham* e-mails were authenticated as having been exchanged by members of the Bandidos by "matching specific email addresses to specific computers at specific residences" that were linked by other evidence to the individuals in question.[59] Alternatively, the presence of numerous documents containing the name of an individual can provide a circumstantial link to the reputed author.[60]

At common law, correspondence can be authenticated as having been sent by an individual by showing that it is a reply to a letter sent to that individual. The same logically holds true for emails and text messages. If evidence shows someone sent a text or email to an individual they believe to be linked to that address and

---

56 For example, a New Jersey woman Dana Thornton was convicted of identity theft for creating a fake Facebook page in the name of her former boyfriend, a police detective, in order to embarrass him. "Belleville woman accused of creating fake Facebook page to mock her ex-boyfriend gets probation" NJ.com (19 March 2012), online: NJ.com <www.nj.com/news/index.ssf/2012/3/bell>.

57 For example, *Sports Illustrated* reported that sexual assault complainant Zach Tomaselli doctored emails to appear as though they came from the police in order to convince the media that his former basketball coach, Bernie Fine, sexually molested him. *Sports Illustrated*, (30 January 2012) at 14.

58 See *R. v. Butler*, 2009 CarswellAlta 1825, [2009] A.J. No. 1242 (Alta. Q.B.).

59 *R. v. Sandham*, 2009 CarswellOnt 6608, [2009] O.J. No. 4527 (Ont. S.C.J.) [*Sandham*].

60 See *R. v. Winchester*, 2010 CarswellOnt 397, [2010] O.J. No. 693 (Ont. S.C.J.) where this kind of evidence was relied on at the end of a case to link a seized computer to the accused.

there is a response from the person purportedly written to, that is some evidence of authenticity.

Similarly, text messages can be linked to particular phones by examining the recorded number of the sender and receiving evidence linking that number to the person in question. And Facebook and blog entries can be circumstantially authenticated by examining the contents of the home page identifying whose home page or blog it is. This requires reliance on the notorious and incontrovertible fact that the accepted, routine and widely dependable way to identify the individuals who operate social network pages and blogs is to examine the identifying information supplied.

All of this is a liberal way of doing things but it is in keeping with ordinary standards of authentication.

(E) Authenticity and the Accuracy of "Computer By-Product Evidence"

Authenticity is about whether the electronic document is that which it is purported to be. It is not concerned with whether the "computer by-product evidence" associated with the document is accurate. As explained when discussing expert evidence, "computer by-product evidence" is information generated by the operation of computers. Date and time stamps are an example. When an email or text message is sent or when a file is created, a date and time record is apt to be created automatically. These records may not be accurate. If the date and time set for the computer is set inaccurately, the date and time records created by the computer will reflect this inaccuracy. It is also possible for the metadata containing the date and time information, or even reporting the file type such as "doc" (for document file) or "jpg" (for image file) to be altered. Errors in the computer by-product evidence has no bearing on whether the file or documents itself has been authenticated.[61]

---

61 Care must be exercised with date and time stamps, even when the computer is properly synchronized and no-one tampers with the meta-date. The date and time recorded by the recipient of a text message sent to an iPhone, for example, shows when the phone received a text-message, not when it was sent. If the iPhone was not turned on at the time the message was sent, the sending and receiving times will not correspond. It is therefore important to clarify by evidence or admission what the relevant date and time stamp purports to show. This caused me confusion in a case involving a text message exchange printed by the accused person. The complainant acknowledged sending the message but was adamant she had not sent it in the morning hours because she is never awake at that time. I now understand that the timing discrepancy recorded in the document generated using the accused persons' phone reflects when the accused person turned his phone on. Other things can go wrong. In a case I recently presided over the police used a computer program to extract and record all text message exchanges between the cellphone and a particular number linked to the accused. That program automatically converted all date and time stamps to Greenwich Mean Time, creating a four hour discrepancy. This did not make the text messages inadmissible. It did, however, require care. Fortunately a combination of judicial notice about relative time zones, circumstantial evidence, and testimony about the timing of events allowed the time and date stamps to be verified and converted.

(v) The Best Evidence Rule

The second role played by subsections 31.1 to 31.8 in electronic documents is to satisfy the "best evidence rule." To appreciate the implications of these provisions and to apply them sensibly, the limited role of the "best evidence rule" must be understood.

(A) The Limited Role of the Best Evidence Rules

At common law that rule was once of general application. It required a party to produce the best evidence available. It was both a rule of exclusion (do not produce inferior evidence if you have better) and a rule of inclusion (if you do not have better, the evidence you have is acceptable if otherwise admissible).[62] These conceptions of the best evidence rule gradually fell into disuse. Now its only remnant is "if an original document is available in one's hands, one must produce it."[63] If it is not available a copy can be admitted unless the document is a contract whose terms are in dispute or the integrity of a will or affidavit is at issue. Concerns about fraud and error in copying go only to weight.[64]

Subsections 31.1 to 31.8 of the *Canada Evidence Act* do not resurrect the ancient common law conception of the best evidence rule. Compliance with its provisions in no way verifies that the evidence in question is better than other proof. It was therefore perilous to declare, as the Court did in *R. v. Morgan*, that evidence complying with subsections 31.1 to 31.8's best evidence rules is "considered to be the best evidence available."[65] This connotes that electronic documents proved using these provisions trump other evidence. They do not. They bear the weight they warrant and the information they contain may ultimately be rejected because of competing proof.

The significance of the best evidence rule, both at common law and under subsections 31.1 to 31.8 of the *Canada Evidence Act*, is further limited by a generous conception of what qualifies as an "original document." This makes it easier to comply with the rule. At common law if documents are executed in duplicate, all duplicates are originals.[66] Since the advent of modern methods for mechanically producing faithful copies of documents, a variety of rules of practice and statutory provisions have been created to provide a generous gateway to the admission of copies in lieu of an original.[67]

The advent of computerized documents loosened the noose of the rule even more. The computerization of documents creates significant ambiguity about what the original is. Is it the actual hard drive containing the code, the translation of the

---

62 See Bryant, Lederman & Fuerst, *Law of Evidence*, *supra* note 53 at paras. 18.4 to 18.8.

63 *Garton v. Hunter* (1968), [1969] 1 All E.R. 451 (Eng. C.A.), at 453 per Denning L.J., followed in Canada. See, for example *R. v. Shayesteh*, 1996 CarswellOnt 4226, 111 C.C.C. (3d) 225 (Ont. C.A.), at 253 [C.C.C.].

64 See Bryant, Lederman &Fuerst, *Law of Evidence*, *supra* note 53 at paras. 18 to 24.

65 *R. v. Morgan*, *supra* note 43.

66 *R. v. Walsh*, 1980 CarswellOnt 16, [1980] O.J. No. 809 (Ont. C.A.).

67 See Bryant, Lederman & Fuerst, *Law of Evidence*, *supra* note 53 at paras. 18.24 to 18.42.

code that is displayed by the electronic device, a copy of the file, or the first print out? The common law was arriving at the generous point that any of these things will do. In keeping with this the *Canada Evidence Act* provisions treat print-outs from electronic storage devices the way the common law treats duplicates. As indicated above, the statute accepts any observable translation of the computer code as sufficient — a live display on the computer using the original device, a file on a memory stick, or a printed representation of the computer-stored information. Given the generous statutory conception of an original document, the primary role the "best evidence" provisions of the *Canada Evidence Act* play is as merely as an adjunct to authenticity. The provisions exist, not so much to assure that the best evidence is presented, but to provide some further assurance that the document provided to the courts is the same as the one that was input into the computer.

There are four ways in which this can be done. Specifically, the "best evidence rule" requirements of the *Canada Evidence Act* can be met by:

> 1. Proving the integrity of the document system that recorded or stored the document by evidence (s.31.2(1)(a));
>
> 2. Proving the integrity of the document system that recorded or stored the document by relying on one of the three presumptions provided for in subsection 31.3 (subsection 31.2(a)), namely the "functioning system" presumption, the "opposing party" presumption, and the "third party business record" presumption;
>
> 3. In the case of documents bearing secure electronic signatures, by relying on a presumption provided for by regulation pursuant to subsection 31.4 (subsection 31.2(b)); and
>
> 4. In the absence of evidence to the contrary, by proving that the document has been manifestly or consistently acted on, relied on or used as a record of the information recorded or stored in a printout (subsection 31.2(2)).

In effect, these rules augment the authentication process by providing some assurance of "continuity" between the data that was input, and the information on the electronic document being offered in court. Method 1 and the first presumption in Method 2 require evidence of the capacity of the document system to capture, store and retrieve information accurately. This is similar to demonstrating authenticity by proving a "chain of custody" by showing that a toxicological sample went from hand to hand, except that the chain of custody of the electronically recorded information is from input data, to computer code, to computer code translated for display or copying. Showing that the document system was functioning properly is evidence that it was able to, and did maintain the data. These methods address the risk of technical failure.

The second and third presumption in Method 2, as well as Methods 3 and 4, provide some assurance that no changes in the document information have been caused either by technical failure or human intervention. These methods rely on circumstantial indicia of reliability associated with the electronic document. If it is a document from the opposing party litigant who will be familiar enough with it to raise accuracy concerns, or if it is used as a business record by a third party or is a printout that has been consistently acted on as an accurate record, or if it has been

signed electronically, this provides some assurance the document is an accurate reproduction of the input data and was in no way changed.

The "best evidence" requirements can be satisfied by meeting any one of these 4 methods. Paradoxically if Method 1 or the first presumption in Method 2 are employed a document can gain admission without any indication that no human intervention occurred.

These various methods of satisfying the best evidence rule can be achieved by calling live evidence to prove their preconditions, or by filing affidavit evidence under subsection 31.6. When proof by affidavit is offered, the opposing party can seek leave to cross-examine the affiant.

In spite of the elaborate statutory scheme, the daily practice in the courts is for electronic documents to be admitted without formal compliance with these provisions. This is easily demonstrated. Everyone who works in our courts recognizes that electronic records are becoming a staple in modern courtrooms. Electronic documents — emails, text messages, tweets, Google maps, Google earth images, 9-1-1 calls, recorded phone messages, digitized photographs — are admitted routinely. Yet there are few reported cases dealing with these "best evidence" provisions, and I venture to say that most lawyers and judges would confirm that it is uncommon to see submissions or rulings in court relating to the application of these "best evidence" provisions, let alone "best evidence" affidavits. Electronic documents are being admitted either (1) without appreciation of the statutory provisions, (2) through the practice of interpreting the absence of objection on these grounds as tacit implicit consent to admissibility, or (3) through the applications of an unstated, liberal conception of judicial notice.

There is some peril in proceeding in each of these ways, but particularly the first two. These provisions create a legal prerequisite to admissibility. Technically, the party with the onus should discharge that onus unless opposing counsel formally agrees on record that the documents satisfy statutory "best evidence" requirements. Absent formal agreement that the best evidence rules have been satisfied, there must be an evidentiary basis supporting admission. In *R. v. Bellingham*,[68] for example, an expert forensic accountant's report offered to prove the theft of lottery tickets was excluded. It contained information generated by Lottery Alberta purporting to confirm lottery ticket sales but the only evidence called to support the data was the complainant's testimony that she received the information from sheets Lottery Alberta provided. No evidence was led relating to how Lottery Alberta generated the information and so it was inadmissible.

Having said this, the best evidence standards of admissibility are not exacting. This is because the law of evidence is intended to be functional and to aid in the efficient presentation of relevant information that can be rationally evaluated. When these provisions are given an overlay of common sense, they can perform their function unobtrusively. This can be seen by examining the technical requirements of these provisions and considering their application.

---

68 *R. v. Bellingham*, 2002 CarswellAlta 487, [2002] A.J. No. 476 (Alta. Prov. Ct.).

(B) Method 1 — Proving the integrity of the document system

Subsection 31.2(1)(a) provides:

> 31 (2) The best evidence rule in respect of an electronic document is satisfied
>
> (a) on proof of the integrity of the electronic document system by or in which the electronic document was recorded or stored.

"Integrity" is not defined but clearly refers to the ability of the system to record and store information accurately. "'Integrity' is a concept of consistency of actions, values, methods, measures, principles, expectations and outcomes."[69] If evidence shows on the balance of probability that the electronic document system had the capacity accurately to record, maintain and display the data, proof of the "integrity of the electronic document system" will be demonstrated.

The degree of proof of the integrity of the electronic document is not specified in the section. Where a statutory rule of evidence does not specify a standard that has to be met when proving prerequisites to admissibility, the "balance of probability" standard is to be applied.[70] Method 1's reference to "on proof" therefore requires that the party seeking admission establish that it is more probable than not that the electronic document system had integrity. As will be seen, this can be done with the aid of the presumptions provided for in Method 2 below.

Evidence of the "integrity of the electronic document system" can be provided through direct testimony about the actual operation of the system or it can be proved circumstantially with the aid of subsection 31.5. Subsection 31.5 specifically invites a court to receive and act upon circumstantial evidence of the integrity of the system, namely, that the electronic document system operated according to relevant standards, procedures, usage or practices used in the relevant type of business, enterprise or endeavour.

The integrity of the system can also be proved by inference from other evidence. In *R. v. Nichols*,[71] for example, the Court held that a 9-1-1 recording system was functioning properly because individuals who heard the call live said that the recording reproduced what they heard at the time. This reasoning is circular in the sense that the purpose of these provisions is to ensure that the electronic documents system is functioning so that the accuracy of the displayed record can be assured. In *Nichols* evidence of the accuracy of the record was used to prove that the electronic system had integrity, thereby enabling the court to conclude that the record was accurate enough to admit. Yet this reasoning is appropriate and to be encouraged. It would be preposterous to reject the admission of an "electronic record" that is attested by a witness with first-hand knowledge to be an accurate reproduction of a document, sound, or image simply because the technical capacity of the electronic recording device to do what the witness said it did has not been demonstrated.

---

69 "Integrity" *Wikipedia*, online: Wikimedia Foundation <http://www.en.wikipedia.org/wiki/integrity>.

70 See Paciocco & Stuesser, *The Law of Evidence*, *supra* note 13 at 45–47; *R. v. Oakes*, 1986 CarswellOnt 95, 1986 CarswellOnt 1001, [1986] 1 S.C.R. 103 (S.C.C.).

71 *R. v. Nichols*, 2004 CarswellOnt 8225, [2004] O.J. No. 6186 (Ont. C.J.).

This approach is comparable to common law authentication practices. At common law there is no need to prove the accuracy of the system used to record information if there is direct testimony from a witness that the event was recorded accurately. In *R. v. Murphy*, for example, the person who took the photos testified that they accurately depicted what he had seen when taking them. The trial judge initially excluded the photos on the basis that the integrity of the system used to record and store them had not been demonstrated.[72] The Nova Scotia Court of Appeal held that the trial judge had erred. Technical proof of the operation of the system was not needed given that there was direct evidence of accuracy from a witness to the event recorded.

The same approach must apply to electronic documents. Where there are witnesses attesting directly to the accuracy of the electronic record it can be inferred that the electronic recording system had integrity. Any other conclusion would pointlessly complicate the trial and produce the indefensible outcome that different standards of admissibility would apply to analog and digital photos and recordings. Analog recordings, not being electronic documents, could be admitted using the generous common law standards, but digital recordings would have to comply with a pointlessly grudging requirement that the integrity of the electronic document system be addressed directly.

For this reason, there should never be "best evidence" concerns arising for emails, texts, tweets or Facebook messages that a witness claims to have sent or posted. If a witness authenticates the electronic documents being offered to the court as "accurate" the integrity of the electronic document system can be inferred, and the "best evidence" provisions can be treated as satisfied.

(C) Method 2 — the presumptions of integrity of the electronic documents system

According to the statute, the integrity of the electronic documents system can be proved if any one of three presumptions contained in subsection 31.3 applies. If this occurs and the presumption is not "rebutted," the "integrity of the documents system" will be established thereby satisfying subsection 31.2(1)(a), the provision just described.

A "presumption" is a legal shortcut to proving a desired fact. It permits the desired fact to be established indirectly. A rule of evidence creating a presumption enables a party wanting to prove Fact "B" [call it "the presumed fact"] to achieve this by proving a different fact, Fact "A" [a "basic fact"]. If the party proves that basic fact, the presumed fact is inferred to exist unless the accuracy of that presumed fact is rebutted by the opposing party.

In the current context this means that if the party tendering the evidence proves the basic facts outlined in one of the evidentiary presumptions in subsection 31.4, the presumed fact — that the electronic documents system by or in which an

---

72 *R. v. Adams*, 2011 CarswellNS 363, *(*sub nom. *R. v. Murphy)* [2011] N.S.J. No. 302 (N.S. C.A.). This case actually dealt with electronic documents as the photos had been digitized and were being presented in the form of a CD, but the Court applied the common law standard as the application of subsections 31.3–31.9 had not been addressed at trial.

electronic document is recorded or stored has integrity — is deemed to be "proven," "in the absence of evidence to the contrary." Where the term — "evidence to the contrary" appears in a presumption, a "mandatory presumption" has been created. This means that once the basic facts have been demonstrated, the presumed fact will be inferred unless the opposing party points to evidence in the proceedings that raises a reasonable doubt about the accuracy of the presumed fact.[73]

The presumptions created by subsection 31.3 provide different standards for proving the requisite basic facts. Presumption 31.3(a), about to be described, calls for "evidence capable of supporting a finding that. . .[the electronic documents system] was operating properly." The term "evidence capable" suggests a threshold level of proof comparable to the legal standard required for authentication and similar to the *prima facie* case and "air of reality standards." Even if the court itself would not conclude that the basic fact has been proved, if there is evidence capable of satisfying a reasonable trier of fact that it has been proved, then the basic fact will be taken to have been established.

By contrast, the second two presumptions provided for in subsection 31.3 call for the basic facts to be "established." Whenever someone is called upon to "show" "demonstrate" "prove" or "establish" a fact and no standard of proof for doing so is expressed, the default standard of proof that applies to admissibility preconditions generally applies; the party must "establish" the evidentiary precondition "on the balance of probabilities."[74]

(ii) Presumption 1 — the functioning system presumption

Subsection 31.3(a) provides:

> 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 an 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 documents and there are no other reasonable grounds to doubt the integrity of the electronic documents system.

As this section indicates, this presumption is triggered by admissible information capable of proving that the electronic documents system was operating properly at all material times. If the electronic documents system had any problems, the presumption would not be triggered unless there is a foundation for concluding that the

---

73 See the discussion of law relating to presumptions in Paciocco & Stuesser, *The Law of Evidence*, *supra* note 13 at 535–541.

74 Standards of proof applicable to admissibility and preconditions are discussed in some detail in Paciocco & Stuesser, *The Law of Evidence*, *supra* note 13 at 43–48 and 535–541.

problems did not affect the integrity of the electronic documents that have been recorded, stored and displayed.

The presumed fact, that the electronic document system had integrity, can be rebutted even if these basic facts are satisfied where there is evidence raising a reasonable doubt about the ability of the document system accurately to record, store or display the data accurately.[75]

This particular presumption should serve as a commodious way of proving the integrity of electronic documents. It should not take considerable evidence to prove the material basic fact. If a witness provides evidence that an email or image was received on a device that functions as a computer, or that a text or tweet was received on a phone, this is circumstantial evidence that the computer systems or other similar devices that sent or received the message were operating properly. If that document is legible or readable and coherent this is some evidence that the integrity of the document was unaffected by any problems that may have affected the computer system. After all, it is certainly incontrovertible and notorious that the function of an email system is to send and receive messages, or that a smart phone can send and receive texts and tweets. Simple proof of the receipt of a coherent document should work with this background information to satisfy the basic fact required by this presumption.

Although the case did not involve a best evidence presumption, this is essentially the kind of reasoning used in *R. v. Woodward*[76] by the Ontario Court of Appeal. The issue there was whether a child-luring text message met the requirement in the child luring offence that child-luring was done by a computer system. Extensive expert evidence was given about how text messaging operates. Woodward argued, however, that the expert failed to give credible evidence that the text messaging system uses "logic" which is a condition of satisfying the definition of a computer system. The Court responded, "It is beyond all controversy that all computer software programs follow basic logic functions. . . . The fact that the voluminous text messages in this case were successfully sent and received by their intended recipient is evidence that the computer program used in the routing process performed "logic and control" functions . . ."[77] Although the Ontario Court of Appeal did not say so expressly, this same reasoning is available to prove the basic fact in the presumption in subsection 31.3(a), that the computer system or device was working properly at the material time. The fact that the voluminous text messages in the case were successfully sent and received by their intended recipient, precisely what text messaging systems are meant to achieve, is evidence that the computer system was functioning properly.

The same should hold true for computer generated documents. If a witness testifies that a facially coherent document was downloaded from a Facebook or

---

75 In this regard the qualification expressed in subsection 31.3(a), "there are no other reasonable grounds to doubt the integrity of the electronic documents system," is redundant. The chapeau to the presumption already provided that, like the other presumptions in subsection 31.3, it would operate only "in the absence of evidence to the contrary."

76 *R. v.Woodward*, 2011 CarswellOnt 9823, [2011] O.J. No. 4216 (Ont. C.A.).

77 *Ibid.*

other home page or blog or a website such as Google maps, a court should be able to infer that the electronic document system was working at the material times and is unaffected by any problems that site or the internet provider may have experienced. Again, judicial notice can be taken that computers function by downloading information on command. If targeted information is discovered in response to a command that is some evidence of functionality. The very retrieval of the data provides confirmation that the "electronic documents system" was operating properly as it demonstrates that the "electronic documents system" successfully performed the function it was intended to perform.

This appears to be what some courts are doing in practice, without articulating their reasoning. In *Girouard v. Druet*,[78] for example, the Court applied the *New Brunswick Electronic Transactions Act* after referencing the similar *Canada Evidence Act* provisions for guidance. It then admitted emails shown to have been exchanged between two parties. The only comment the Court made relating to the evidentiary basis supporting their admission was to observe that "there were no submissions that the e-mails had been altered." Although the Court did not put it this way, its finding was effectively that there was evidently nothing to rebut the inference available on proof of the receipt of the emails that the system of recording, storing and retrieving the emails was obviously working properly. Similarly in *Izyuk v. Bilousov* the fact that the parties frequently exchanged emails sustained a finding that they were accurate.[79]

This is a sensible way of proceeding. As the Court in *Girouard*[80] remarked, courts encounter emails on a daily basis as their use has become a way of life. The same holds true with social media and downloaded information. It would not be realistic, indeed it would be counterproductive, to expect individuals who rely on such information to produce witnesses or even affidavit evidence from Internet Service Providers that their systems were functioning properly, or to present the courts

---

78 *Girouard v. Druet*, 2011 CarswellNB 402, [2011] N.B.J. No. 260 (N.B. Q.B.); reversed 2012 CarswellNB 227, 2012 CarswellNB 228 (N.B. C.A.) [*Girouard*]. But see *Narayan v. Canada (Revenue Agency)*, 2009 CarswellNat 1158, 2009 CarswellNat 1159, [2009] C.P.S.L.R.B. No. 40 (Can. P.S.L.R.B.) where the Board excluded an email after citing this section because there was no evidence of the integrity of the computer system used by the grievor. The Board did not use this provision properly. It appears to have assumed incorrectly that subsection 31.3(a) is a necessary condition to admissibility when it is only one path to satisfying the best evidence rule. In *Narayan* there was evidence calling into question the integrity of the email as it did not reflect the characteristics of "normal printouts for AOL subscribers" but this should not have rebutted this "best evidence" presumption. The presumption is concerned not with whether the information input is genuine but with whether the computer system or other device was operating properly. Still, the case does reflect an insistence on direct proof the computer system was working before this presumption can become engaged, an approach I would not encourage.

79 *Izyuk v. Bilousov*, 2011 CarswellOnt 14392, [2011] O.J. No. 5814 (Ont. S.C.J.). The *Ontario Evidence Act*, whose provisions largely mirror those of the *Canada Evidence Act* would have applied in this civil case.

80 *Girouard*, *supra* note 78.

with pointless recitals by witnesses about the history of problems they have experienced with their computers or smart phones.

To feel fully comfortable with all of this it is important to reinforce the limits of the "best evidence" requirement in question. What has to be shown is the integrity of the electronic documents system by which an electronic document is "recorded or stored." The thing that was recorded may have been input inaccurately by the individual typing the message or selecting the image for downloading but this is not a matter affecting the best evidence rule. This may affect the admissibility of the information based on other evidentiary principles such as relevance concerns, or the weight of the evidence may be undermined, but if it is presumed that the data displayed is the data that was recorded and stored, "best evidence" principles have been satisfied.

The same is true with concerns about whether the person identified as the sender of the email really sent it, or whether a Facebook page was really authored by the person who is identified as the owner. These are matters of relevance and would not impact on the operation of this presumption. These concerns have nothing to do with the functionality of the electronic document system.

Similarly, a court may have concerns about whether the information that was posted is accurate — for example, is the distance between two points really what Google maps claims it to be — but that is not a "best evidence" consideration. It is a hearsay consideration governed by other rules of admissibility.

(ii) Presumption 2 — the opposing party litigant presumption

Subsection 31.3(b) provides:

> 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
>
> > (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.

Unlike the presumption in subsection 31.3(a), the basic facts required to trigger this presumption must be proved on the balance of probabilities. This requires credibility issues relating to those components to be resolved at the admissibility stage.

This presumption is tremendously useful to the Crown in criminal cases. Any electronic document seized from a computer or smart phone or similar device that was probably used by the accused will be presumed to satisfy the best evidence requirements of admissibility unless the accused can show that the electronic documents system was not able to record and store information accurately. Any electronic document that other witnesses can link to the accused as probably recorded or stored by him will receive the same treatment. *R. v. Sandham*[81] is an illustration of an email that would satisfy subsection 31.3(b), even though the application of the electronic document best evidence provisions of the *Canada Evidence Act* do not appear to have been in issue in that case. The Crown produced an unsent email found on a computer at the home of a third party. It was sent from an email account

---

81 *Sandham*, *supra* note 59.

held by the accused, and in this gang-related prosecution the email was helpfully signed "Prospect Bandido Bill," an identifier consistent with evidence that the accused, Bill Sandham, held himself out to be a prospect Bandido. Since the electronic document was probably recorded by the accused it satisfied the best evidence provisions of subsection 31.3(b).

The theory underlying this presumption is not unlike the theory that supports the "statements by opposing party litigant" exception to the hearsay rule. If the source of the information is the opposing party, the opposing party is best able to explain the evidence away if it is unreliable. They know better whether their electronic documents system has integrity and if they wish to rebut the inference that it does, they can present evidence.

The fact that an accused person may have to testify in order to rebut this presumption where it is relied upon by the Crown does not constitute an unconstitutional reversal of onus. The principle against self-incrimination is infringed only where the legal burden is reversed — in other words, where a legal rule requires the accused to testify. It is not offended where tactically the accused may feel it necessary to testify.[82] Under this rule the accused is free to rebut the presumption by relying on other sources of evidence. If there are no other ways to rebut the presumption in the particular circumstances of the case, that is the accused's misfortune. He has to make a tactical decision whether to testify in order to rebut the provision, or to let the presumption operate.

(iii) Presumption 3 — the business records presumption

Subsection 31.3(c) provides:

> 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
>
> > (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.

Like subsection 31.3(b), the basic facts required to trigger the presumption have to be proved on the balance of probabilities. Reliance on the document as a business record is some circumstantial evidence of its accuracy on the theory that if it is sufficiently accurate for a business to use it, it must meet admissibility thresholds of reliability.

---

82 See *R. v. Darrach*, [2000] 2 S.C.R. 443, 2000 CarswellOnt 3321, 2000 CarswellOnt 3322 (S.C.C.) at paras. 47–52 for a description of the difference between legal and tactical burdens.

(D) Method 3 — the presumption for documents signed with secure electronic signature

The third method of satisfying the "best evidence" requirements relating to electronic documents is supplied by subsection 31.2(b). It provides as follows:

> 31.2 (1) The best evidence rule in respect of an electronic document is satisfied
>
> (b) if an evidentiary presumption established under subsection 31.4 applies.

Subsection 31.4 creates yet another exception. It states:

> 31.4 The Governor General in Council may make regulations establishing evidentiary presumptions in favour in relation to electronic documents signed with secure electronic signatures, including relations respecting
>
> (a) The association of secure electronic signatures with persons; and
>
> (b) The integrity of information contained in an electronic document signed with secure electronic signatures.

On 10 March 2011 the *Secure Electronic Signature Regulations*, initially adopted in 2005 as SOR/2005-30, were revised and annexed to the *Canada Evidence Act* and the *Personal Property Information Protection and Electronic Documents Act*. The only presumption included in the regulation is found in section 5. This presumption does not expressly presume the integrity of information that is signed with an electronic signature as provided for in the statute.[83] Instead it provides:

> 5. When the technology or process set out in section 2 is used in respect of data contained in an electronic document, that data is presumed, in the absence of evidence to the contrary, to have been signed by the person who is identified in, or can be identified through, the digital signature certificate.

Finding that data was signed by the accused is obviously useful in authenticating that data. Although there is no case law dealing with the issue, the signing of data would appear to be sufficient circumstantial evidence of its integrity. This is because data is signed either when it is recorded or at some later point where it is displayed after being stored. Either way, if it is presumed that the data presented in evidence above or under an electronic signature was the same data signed by the person identified, it can be inferred that the data was recorded, stored, and has been displayed with integrity. That being said, this is not apt to be a common or convenient gateway for establishing admissibility. To rely on this presumption the electronic signature would have to be authenticated.

(E) Method 4 — electronic document print outs

The final method of satisfying the best evidence elements for electronic documents is by relying on yet another statutory presumption, this one found in subsec-

---

83 Sections 2–5 provide statutory preconditions for the certification and use of electronic signatures.

tion 31.2(2). It is useful only where relying on "printouts" of documents initially recorded or stored in a computer or other similar device.

> 31 (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.

The theory is evidently that if a printout of the information is manifestly or consistently acted on or relied on or used as a record of the information recorded or stored, errors in the information are apt to be discovered and corrected. In effect, if the document is a reliable enough record for those who are keeping it, it has sufficient integrity to be admitted into evidence.

What makes this provision unique among the relevant "best evidence" presumptions is that the presumed fact is not that the electronic document system has integrity. It is that the "printout satisfies the best evidence rule." It is unusual to see an evidentiary tool such as a presumption used to presume a legal outcome rather than a factual finding, so the provision is somewhat curious. What makes the provision doubly curious is that it provides for a rebuttable presumption without identifying what fact is to be rebutted. If the party presents evidence of a printout manifestly and consistently relied upon or used as a record of the information recorded or stored on the printout, the printout is said to be admissible in the absence of evidence to the contrary, but the provision does not specify "to the contrary" of what. How does one rebut a legal conclusion provided for by statute — that the best evidence rule is satisfied — with evidence?

The only sensible interpretation is that when the drafters used the term "satisfies the best evidence rule" in subsection 31.2(2) they were referring to the indirect definition of that rule contained in subsection 31.2(1)(a) — that the best evidence rule is satisfied upon proof of the integrity of the electronic document system. This would enable the presumption to be interpreted as providing that if there is evidence raising a reasonable doubt about the proper functioning of the electronic document system at the material times, this provision cannot be relied upon to satisfy the best evidence rule, even if a printout is manifestly or consistently acted on, relied on or used as a record of the information recorded or stored in the printout.

(d) The Law of Hearsay

(i) Hearsay and Computer Generated Information

A great deal of technological evidence will be presented in the form of data generated using computers. This data will typically be offered as representing accurate factual information. In other words, it will generally be admitted for the truth of its contents. This does not necessarily make it hearsay evidence. While statements of fact recorded by humans on computer-like devices will be hearsay if offered to prove those recorded facts to be true, information created by mechanical means by a computer-like device — "computer generated information" — is not hearsay. This kind of information, including date and time stamps attached to emails or text messages, or coded address information used to identify Internet Ser-

vice Providers and accounts, is original or real evidence.[84] This is because the hearsay rule captures only information communicated by human beings and is based on the inability to cross-examine the human witness who purports to know the information. For this reason the classic definition of hearsay in *Subramaniam v Public Prosecutor* identifies hearsay by examining whether "a statement made to a witness by a person" is hearsay or not.[85] Computer generated information, even though produced using a program designed by a person, is not the statement of a person. Think of it this way. Computer generated information is no more hearsay than the ring of an alarm clock communicating it is 7:00 a.m. There is no risk of dishonesty and no hearsay rules are engaged.

The only admissibility issues arising from the fact that relevant information is "computer generated" relate to the accuracy and reliability of the technology that produced the information. For example, in *R. v. Gratton*[86] a printout of the "sensory diagnostic module" of a computerized system in a truck purported to record the speed of a vehicle five seconds prior to airbag deployment. This evidence was excluded not as hearsay but because expert evidence was required to establish the reliability of the technology.

This does not mean that expert evidence is always required. Judicial notice can be taken of the reliability of some such information. For example, it is notorious that a phone number recorded on a digital phone display while the phone is ringing is a reliable indication that the call that is occurring is from the number displayed. The same would hold true with numbers displayed by the "recent calls" function of digital phones or answering machines.

It can also be accepted, one would suppose, that computer generated date and time displays are reliable enough to admit. This is so notwithstanding the cautions expressed above about the potential imprecision of date and time displays. In spite of this, it is widely understood that computer devices incorporate time and date features that are reliable enough to use in the ordinary conduct of business. There are, however, issues of weight. As explained above, dates and times displayed by a computer-system are only as accurate as the general date and time setting on the computer or program, as the case may be. The risk that the time may not be entirely accurate is not necessarily a basis for exclusion though. Just as courts receive times recorded by wrist watches without evidence of their synchronization, computer generated times should not become inadmissible because precision is not validated. If precision is required to give the evidence full weight, evidence of synchronization may however be required. In *R. v. Hamilton*,[87] for example, times recorded in electronic cell-phone records of service providers were out of sync with the electronic 9-1-1 records. This did not render the records inadmissible but did limit the precision of the time/location inferences relating to cell-phone users that could be drawn from the evidence.

---

84 See Paciocco & Stuesser, *The Law of Evidence*, *supra* note 13 at 469, citing JW Strong ed, *McCormick on Evidence*, 4th ed (St Paul, MN: West, 1992) at 505-506 and *R. v. Spiby* (1990), 91 Cr. App. R. 186 (Eng. C.A.).

85 *Subramaniam v. Public Prosecutor*, [1956] 1 W.L.R. 965 (Malaysia P.C.), at 969.

86 *R. v. Gratton*, 2003 ABQB 728, 2003 CarswellAlta 1241 (Alta. Q.B.).

87 *Hamilton*, *supra* note 4.

(ii) Proving the Fact that Statements were Made

When electronic records that were initially in-put by humans are being offered as an accurate record of facts or events, hearsay exceptions will generally have to exist before the evidence is admitted. By contrast hearsay rules are not engaged if what is being proved is the simple act of recording specific words into a text message or other computer record. For example, it is not hearsay to prove the electronic record of a text message if that is being done to prove that an accused person attempted to make contact with someone in breach of an undertaking. The message is not coming in to prove the truth of what it is meant to communicate. The message is being proved to demonstrate the fact that attempted communication occurred.

(iii) Circumstantial Evidence Statements

There are also times where recorded information can be used as circumstantial evidence without violating the hearsay rule, and this can occur with electronically recorded documents. The hearsay/circumstantial evidence divide can be conceptually challenging because it involves using evidence that can serve as hearsay, in a non-hearsay way. It is often difficult for jurists to disregard the hearsay use when trying to recognize the non-hearsay application. Consider, for example, an airline ticket. It will record the name and destination of the traveller and identify the carrier and travel date. If the information recorded on the ticket were to be relied upon as a simple declaration of the facts it records in the same way a diary entry by the traveller recording their flight details might be used, it would be hearsay. But an airline ticket is different than a diary entry. The airline ticket itself has meaning. An airline ticket is required before the bearer is permitted to board a flight. If someone carries an airline ticket in their own name which authorizes travel the next day on a particular flight, the nature and role of that document constitutes solid circumstantial evidence that the person is intending to travel the next day. Similarly, if a discarded plane ticket is found on an airplane it is circumstantial evidence that the named bearer was likely on that plane. While the recorded information is used to draw these inferences, this information is not being relied upon as a simple assertion of fact. It is the fact that this information is found on a document recognizable as an airline ticket that yields the material inferences. Relying on the airline ticket to draw inferences from the fact that the document is a ticket capable of being transacted by the named individual does not involve hearsay uses.

By the same token, evidence that a document containing a radio frequency identification tag linked to a person was used at a particular location is circumstantial evidence that the document was scanned at that location, and can be circumstantial evidence that person was there at the time the document was scanned. This is not hearsay. It is circumstantial evidence.

(iv) Hearsay Exceptions

There are, of course, numerous hearsay exceptions, apart from the principled exception, that can result in admissible hearsay drawn from electronic documents. A number of these exceptions are particularly important.

(A) The "Statement by Opposing Party Litigant" exception

The "statement by opposing party litigant" exception, sometimes called the "admission exception," will permit electronic communications by accused persons to be admitted for hearsay purposes. If those statements are made to persons in authority the voluntariness rule will generally have to be satisfied but it is rare for individuals to communicate with justice officials electronically. This exception is therefore apt to capture the vast majority of electronic communications authored by accused persons.

The requirements of the exception are simple. If it can be proved on the balance of probabilities that the accused authored or made a relevant, authenticated electronic communication, it can come in.[88] It does not matter whether the accused thought he was making an incriminating admission at the time. If the opposing party, the Crown, wants to use an electronic communication authored by the accused, it can be admitted. It does not even matter whether the accused had personal knowledge of the factual claims made in the electronic communication. If the accused asserts a fact, even based on his belief, that assertion is evidence against him. The fact it is a statement about something the accused does not have personal knowledge about goes to weight alone, not admissibility.[89]

The utility of this exception to electronic communications is revealed in *R. v. Sandham*.[90] All email communications written by accused persons were admitted for their hearsay use. All of the factual claims they made in their various statements could therefore be used as proof of those facts.

The *Sandham* court ruled, appropriately, that the entire email exchange in which those statements were made, including statements made by other parties to the email exchange, were also admissible to give context to the comments of the accused. "As in any conversation, it is essential to hear what both parties are saying in order to understand the meaning of either side of the conversation."[91] Care is required however. Typically where the other side of an electronic conversation with an accused party is admitted, it comes in solely to give context to the statements made by the accused, and not as evidence in its own right. It would ordinarily be an error to treat the conversation as evidence of the truth of what other parties to the conversation have claimed. Exceptionally, however, if it is apparent that the accused person is adopting as true what another party to the conversation is saying, the facts that have been adopted as true should be treated as an admission made by the accused, and therefore as admissible hearsay evidence.

(B) The Business Records Exception

The business records hearsay exceptions are also commonly engaged where electronic documents are in issue. This is because most business records are now created and stored electronically. If a record was created in a computer or similar

---

88 *R. v. Evans*, [1993] 3 S.C.R. 653, 1993 CarswellAlta 111, 1993 CarswellAlta 567 (S.C.C.).

89 *R. v. Streu*, 1989 CarswellAlta 615, 1989 CarswellAlta 514, 70 C.R. (3d) 1 (S.C.C.).

90 *Sandham*, *supra* note 59.

91 *Ibid.* at 34.

device in the usual and ordinary course of business it will generally be admissible. In criminal cases two distinct business records exceptions are available.

The most commonly relied upon business records exception is section 30 of the *Canada Evidence Act*.[92] So long as the notice requirements of this provision are complied with and proved,[93] a record made in the usual and ordinary course of business by someone under a business duty[94] will generally be admissible,[95] even if it contains double hearsay.[96] The concept of business is broad. It includes any calling or undertaking, including any calling or undertaking carried on by governments and non-profit groups. The records that are generated, including electronic records, in order to assist in the conduct of that calling or undertaking, will be admissible as business records. The transaction or event or fact recorded need not relate to the core business undertaking or calling. It is enough that it is related to activities connected to the business.[97] Nor is there any requirement that the business usually keeps records of the kind in question. The exception is generous.

The common law exception for declarations in the course of duty is also available. It is stricter than section 30 in some respects. It requires that the record in question be made reasonably contemporaneously to the event, and that it be made as a matter of duty.[98] Although in *Ares v. Venner*[99] the Supreme Court of Canada held that the recorder had to have personal knowledge, in *R. v. Monkhouse* the Court accepted a compiled record of employment made by someone without personal knowledge where the person originally recording the employment information would evidently have been under a business duty as well.[100] This is sensible.

---

92 There are, of course, other statutory exceptions, including section 29 of the *Canada Evidence Act*, R.S.C. 1985, c. C-5, dealing with records of financial institutions.

93 Subsection 30(7) of the *Canada Evidence Act*, R.S.C. 1985, c. C-5 provides for seven days of notice and an opportunity to inspect the records within five days of receiving notice of a request to inspect, although these time limits can be abridged by the court.

94 Section 30 does not expressly require that the person making the record be under a duty to the business to do so. It is an implicit requirement, however, as this is the thing that provides the most central indicia of reliability: *R. v. Wilcox*, 2001 CarswellNS 83, 152 C.C.C. (3d) 157 (N.S. C.A).

95 Subsection 30(1) of the *Canada Evidence Act*, R.S.C. 1985, c. C-5, prohibits the admission of some business records, most importantly, records made of an investigation or inquiry into an event; records that contravene other rules of admissibility such as privilege or the testimonial incompetence of the maker, and transcripts of evidence.

96 *R. v. Martin*, 1997 CarswellSask 144, 8 C.R. (5th) 246 (Sask. C.A.). In Paciocco & Stuesser, *The Law of Evidence*, *supra* note 13 at 172, the case is made that unless there is some other foundation for finding the initial statement to be reliable, double hearsay should be admitted only if both the recorder and the initial maker of the statement are under a business duty to ensure the accuracy of the record.

97 See *Setak Computer Services Corp. v. Burroughs Business Machines Ltd.*, 1977 CarswellOnt 626, 15 O.R. (2d) 750 (Ont. H.C.).

98 *Ares v. Venner*, 1970 CarswellAlta 142, 12 C.R.N.S. 349, 1970 CarswellAlta 80 (S.C.C.).

99 *Ares v. Venner*, 1970 CarswellAlta 142, 12 C.R.N.S. 349, 1970 CarswellAlta 80 (S.C.C.).

100 *R. v. Monkhouse*, 1987 CarswellAlta 248, 61 C.R. (3d) 343 (Alta. C.A.).

Although stricter than the statutory exception, subject to the courts exclusionary discretion this exception should be available where the notice requirements in section 30 of the *Canada Evidence Act* have not been complied with.[101]

(C) The Res Gestae Exceptions

The *res gestae* exceptions to the hearsay rule will also be important for business records. *Res Gestae* is a generic term used to signify that something is part of the material story or event. Not all *res gestae* statements are admissible as hearsay. There are three key hearsay exceptions linked to the *res gestae* concept, "statements of present physical condition," "statements of present mental state," and "excited utterances."[102] The last two of these exceptions are the most apt to arise where information technology is being used.

The "statements of present mental state" exception permits hearsay use to be made of statements made by any person — charged or not — that describe that persons relevant, present mental state of mind (such as emotion, intent, motive, plan), provided those statements are not made in circumstances of suspicion.[103] In *R. v. P. (R.)* the Ontario Court of Appeal held that this exception is useful where statements expressly describe a present state of mind.[104] For example, the statement "I am feeling depressed" is admissible as direct evidence of the speakers depression.

Statements that do not directly assert a state of mind can also be proved provided they permit a relevant state of mind to be inferred. The conventional view is that those statements are not hearsay but rather circumstantial evidence, and therefore this hearsay exception is not technically required.[105] In *R. v. Sandham*, for example, the Court admitted email correspondence between two other persons but found in the home of one of the accused. These emails reflected tension between the two groups involved in a mass killing. The emails were therefore admissible as

---

101 Subsection 30(11) provides that the statutory business records exception is in addition to and not in derogation of any other rule of law that would render a record admissible.

102 The first two exceptions permit the hearsay admission of statements made by individuals while experiencing the relevant thing — a physical sensation in the first exception, and a mental state in the second exception. Since these statements accompany the relevant thing, they are *res gestae*, or part of the material event, for example, "I have pain in my head," or "I intend to go to meet Stan." Such statements are reliable enough to admit because the context in which they were made — during the event — permits their credibility and reliability to be evaluated, and no issues of memory can arise as the facts narrated are current at the time the statement is made.

103 *R. v. Starr*, 2000 CarswellMan 450, 2000 CarswellMan 449, 147 C.C.C. (3d) 449 (S.C.C.).

104 *R. v. P. (R.)*, 1990 CarswellOnt 2696, 58 C.C.C. (3d) 334 (Ont. H.C.) [*P. (R.)*].

105 Personally, I have difficulty with this. Arguably, to serve as circumstantial evidence of a state of mind a statement must be true. For example, "I do not want to be alone with Larry" is not circumstantial evidence of fear of Larry unless the speaker truly does not want to be alone with Larry. Since the statement must be true to be relevant, it is being proved for a hearsay purpose. This is not a quibble of substance, however. As Justice Doherty said in *R. v. P. (R.)*, *supra* note 104, "the result is the same whichever route is taken." The statement would come in under this hearsay exception even if the circumstantial evidence theory was not available.

circumstantial evidence that this accused knew of that tension, thereby helping to fuel his motive to participate in the killing.[106]

The "excited utterances" exception will often be encountered with electronic evidence. It is particularly useful where 9-1-1 and other electronically recorded emergency calls are recorded. So long as the communication is made by a person who is still under the stress or excitement of a startling event or condition — even if some time has passed — that communication may be admitted as hearsay if it describes or comments upon the startling event. In order to be admitted the declarant must be so caught up in the pressure of the event at the time the statement is made that they would not have time for reflection.[107] Often where 9-1-1 calls are made, this is the case, although this will not invariably be so.[108]

(e) The Law of Privilege

Naturally some electronic communications are privileged. Not surprisingly, the law of privilege tends to apply in the same way to electronic communications as it does to paper communications. In *R. v. Docherty*,[109] for example, the accused sent an incriminating email to his spouse. He tried to assert spousal privilege over the document but the court, applying ordinary principles, held that this privilege did not apply. It is testimonial in nature. It enables spouses to refuse to testify about their marital communications. It does not protect previously recorded communications, including emails intended to be confidential.

Still, there is the potential that the law of privilege could be altered radically as the result of technology. Much of the law of privilege is premised on privacy, yet privacy as we have known it is under attack by technology. In a world where computer chips with personal information are embedded in passports and enhanced driver's licences, where communication using everyday methods of social discourse invariably leaves trace evidence, where a message can be disseminated to thousands simultaneously by private individuals, and where so much of our personal information is stored in the computer systems of those we interact with, privacy is becoming harder to maintain. Meanwhile social media users are increas-

---

106 *Sandham*, *supra* note 59. Consistent with the view I express in the preceding footnote, the Trial Judge described this evidence as coming in under the "state of mind" exception to the hearsay rule even though the statement was only circumstantial evidence of a state of mind.

107 *Ratten v. R.*, [1971] 3 All E.R. 801 (Australia P.C.), approved in *R. v. F. (G.)*, 1999 CarswellOnt 129, 132 C.C.C. (3d) 14 (Ont. C.A.) and *R. v. Nicholas*, 2004 CarswellOnt 823, 182 C.C.C. (3d) 393 (Que. C.A.); leave to appeal refused 2004 CarswellOnt 4003, 2004 CarswellOnt 4004 (S.C.C.), where a 9-1-1 call was admitted.

108 In *R. v. Pattison*, 2011 CarswellBC 3415, [2011] B.C.J. No. 2231 (B.C. S.C.), at paras. 39–41 the accused called 9-1-1 to report the killing and blame others. The call was not admitted under this exception but did come in as evidence under other rules. Specifically, since the Crown was relying on Pattison's callous and calm demeanour after his arrest as proof of his intention, his anxious emotional behaviour during the 9-1-1 call became admissible rebuttal evidence.

109 *R. v. Docherty*, 2010 CarswellOnt 542, [2010] O.J. No. 382 (Ont. S.C.J.).

ingly apt intentionally to share information with large numbers of select individuals.

The inability to control the dissemination of information coupled with the growing sense that individuals should be able to disseminate information quite broadly but selectively has the potential to alter what our reasonable expectations of privacy are and this can affect the way the law of privilege operates. It has been suggested, for example, that the concept of privacy is shifting from "confidentiality, anonymity and seclusion" to "informational self-determination." "In other words, having greater control over how your personal details are shared with others, and holding information custodians accountable for what they do with them."[110] While this can influence what the law of privilege chooses to protect in the future, it has yet to happen. Courts have, for example, denied privilege claims relating to Facebook information, even information not generally available through the public profile that Facebook users post.[111] This is an issue that will likely be revisited as privacy practices within society continue to change.

While the rules of privilege have remained stable in the face of new technology, the application of those rules can be affected by the realities of new technology. In *Eizenstein v. Eizenstein*,[112] for example, Mr. Eizenstein, a husband engaged in acrimonious family law litigation, may have secured the assistance of his then girlfriend in typing and sending email communications to his lawyer as he was not completely computer literate. Mr. Eizenstein and his girlfriend had a falling out and the girlfriend sent the emails to Mrs. Eizenstein. Mrs. Eizenstein wanted to use them during the litigation. Her argument that if her husband shared this information with his girlfriend the privilege was lost was rejected, even though ordinarily privilege is lost when the information is shared with third parties. The Court took a pragmatic view, holding that even if Mr. Eizenstein had asked an intimate friend for assistance in coping with technology in transmitting information, this is the equivalent of an illiterate person finding help reading a legal document. It would unfairly defeat access to privilege to find that relying on necessary assistance would defeat the privilege.

Solicitor-client privilege is an area where new technology could imperil the privilege. Solicitor-client privilege requires that a privileged communication relates to the provision of legal services and is made by the client with the intention and in the reasonable expectation that it will remain private. Yet privacy in its pure sense is often put at risk or even compromised when new technologies are used by lawyers. Lawyers are increasingly using the internet to handle client information. Lawyers working in collaboration on files may use password protected shared files available through commercial electronic document services. Some lawyers also use

---

110 Misty Harris, "Privacy becoming scarce in digital world" *The Ottawa Citizen*, (2 April 2012) at A4.

111 See, for example, *Frangione v. Vandongen*, 2010 CarswellOnt 5639, [2010] O.J. No. 2337 (Ont. Master), *Sparks v. Dubé*, 2011 CarswellNB 80, [2011] N.B.J. No. 38 (N.B. Q.B.); *Bishop (Litigation Guardian of) v. Minichiello*, 2009 CarswellBC 871, [2009] B.C.J. No. 692 (B.C. S.C.); leave to appeal refused 2009 CarswellBC 3301 (B.C. C.A. [In Chambers])

112 *Eizenstein v. Eizenstein*, 2008 CarswellOnt 3822, [2008] O.J. No. 2600 (Ont. S.C.J.).

"SaaS Enterprise platforms" such as CLIO to manage their documents and practice systems. Many are using "cloud computing" in their offices in which data is stored remotely and routed using the facilities and soft-ware of web-based service providers. Hotmail, Gmail, and Yahoo employ cloud computing for email messages. While the lawyer is the data controller who in-puts and directs the dissemination of data in cloud computing systems, information input into these systems falls outside of the immediate control of the lawyer. Arguably the information is typically safer "in the cloud" than it is in a law office given the availability of encryption and the security policies of cloud providers but the fact is the lawyer who uses cloud computing forfeits autonomous control over the information and has intentionally relinquished it in order to use the service. Often the web-based service provider, the data processor, is even located outside of Canada where Canadian law does not apply.

What does this mean for the integrity of solicitor-client privilege? I agree with the sentiments expressed by Trent Skanes. "The test for communications 'made in confidence' [that is used to identify solicitor-client privilege] needs to have broad application to be effective."[113] As technology advances the standard for finding communications to have been made in confidence must be flexible enough to apply in all mediums and situations. Judges need to ensure that their privilege-based decisions reflect the realities of document management in a technological age. Failing this, the function of solicitor-client privilege in encouraging the candid exchange of information will be defeated.

A related issue arises with respect to unintentional disclosure of privileged information. The opportunity for the accidental transmission of privileged information has increased dramatically with the internet and with electronic discovery, disclosure, and file management. In a case I was involved in, the disclosed CD ROM containing the Crown file inadvertently included the Crown's litigation privileged research memoranda as well as solicitor-client communications with investigators.[114] In addition, "metadata" including information deleted from earlier generations of documents can easily be revealed using ordinary computer programs unless it is "scrubbed" before electronic documents are disseminated.

Historically, the law of privilege was harsh when privileged information had been accidentally disclosed. The privilege was lost. This unremitting approach no longer applies. Courts asked to enforce privilege involving inadvertently disclosed information are now making discretionary determinations about whether inadvertent disclosure defeats a privilege claim.[115] There have even been civil cases where lawyers inadvertently receiving solicitor-client information have been removed

---

113 Trent Skanes, student-at-law, Memorandum to Professor Adam Dodek, Faculty of Law, University of Ottawa, Re: SCP and Technology, 14 June 2011 at 9. I have benefited tremendously in this privilege section from Mr. Skanes' paper, from its research, and in identifying issues of concern as well as gaining an understanding of relevant technology.

114 The CD was returned unread but had it been retained, complex litigation could have resulted over its status.

115 *Airst v. Airst*, 1998 CarswellOnt 2630, [1998] O.J. No. 2615 (Ont. Gen. Div.).

from a case.[116] Courts making discretionary decisions about whether privilege will be protected over inadvertently disclosed information will consider the intensity of the legal policy underlying the privilege (with solicitor-client privilege being particularly jealously guarded) how the document came to be released (with misconduct by the party gaining possession playing a large role in supporting continued privilege and carelessness in disclosure weakening the claim), how prompt the efforts to gain its return were, how widely the privileged information has come to be disseminated, and how important and necessary the information is to the party who inadvertently received it.[117] In criminal cases, the principles of full answer and defence and the presumption of innocence would assist in supporting the use of otherwise privileged information that could be important in the defence of a case, even, arguably, where the information falls short of satisfying the "innocence at stake" standards that courts would otherwise insist upon before disregarding privileges.[118]

(f) Exclusionary and Procedural Discretion

(i) The Range of Discretionary Authority

Courts in the modern era have potent authority to make discretionary, context-based procedural decisions to assist in the sensible application of technological evidence.

While there is no "inclusionary" discretion, the discretionary authority of courts includes the power to exclude technically admissible evidence. It is now widely understood that this discretion applies to any kind of evidence. The formula that applies to the exclusionary discretion is familiar to all jurists and involves balancing the probative value of the evidence against the prejudice its admission could cause. "Probative value" describes the contribution the evidence could make to the case, and includes an evaluation of how important the issue the evidence addresses is, how compelling the evidence is in resolving that issue, and the credibility and reliability of the evidence. "Prejudice" describes all of the adverse costs involved in admitting the evidence, including (1) the adverse costs to parties and witnesses such as the degree of embarrassment it will cause or the extent of any privacy invasion its presentation entails, (2) the adverse practical implications for the trial in calling the evidence including the undue consumption of time or distraction from the issues at hand, and even (3) prejudice to the administration of justice, such as the degree to which the evidence may be inflammatory or potentially distorting in its impact, as well as the prospect that admitting it could discourage future criminal complaints.[119]

---

116 *Celanese Canada Inc. v. Murray Demolition Corp.*, [2006] 2 S.C.R. 189, 2006 CarswellOnt 4623, 2006 CarswellOnt 4624 (S.C.C.).

117 See *Metcalfe v. Metcalfe*, 2001 CarswellMan 104, 198 D.L.R. (4th) 318 (Man. C.A.).

118 See *R. v. Brown*, [2002] 2 S.C.R. 185, 2002 CarswellOnt 916, 2002 CarswellOnt 917 (S.C.C.), where the "*McLure* test" that applies for court-based applications to dismantle privilege is most fully explained.

119 The law relating to the exclusionary discretion is described in detail in Paciocco & Stuesser, *The Law of Evidence*, *supra* note 13 at 34–42, including the controversial authority to evaluate credibility and reliability at the admissibility stage.

Once these factors are evaluated a simple balancing is undertaken. With respect to Crown evidence the formula for exclusion is simple. Does the prejudice in admitting the evidence outweigh its probative value? When the evidence in question is being presented by the accused person the exclusionary discretion is to be used more circumspectly. In the interests of full answer and defence it should be excluded only if the prejudicial effect of the questioning substantially outweighs its probative value.[120]

There are fixed rules of evidence that incorporate a similar balancing exercise. The admissibility of similar fact evidence, expert evidence, and even hearsay evidence applying the principled exception invite assessments of probative value and prejudice.

There is also the discretion that judges have to manage the trial. Appellate Courts have come to recognize that given the complexity of first instance trials in a *Charter* era this power includes not only the traditional authority to control the admissibility of evidence, but also such things as "the power to place reasonable limits on oral submissions, to direct that submissions be made in writing, to require an offer of proof before embarking on a lengthy *voir dire*, to defer rulings, to direct the manner in which a *voir dire* is conducted (especially whether to do so on the basis of testimony or in some other form) and exceptionally to direct the order in which evidence is called."[121] In *R. v. Hamilton* the Ontario Court of Appeal recently added the following remarks:[122]

> A trial judge may properly intervene to focus the evidence on the matters in issue, to clarify evidence, to avoid irrelevant and repetitive evidence, to dispense with proof of obvious and agreed matters, and to ensure that the way a witness is answering questions does not unduly hamper the progress of the trial.
>
> At a time when we are concerned about the increasing cost and length of criminal trials as well as their drain on resources and the pressures they may bring to bear on the administration of justice, appropriate trial management is to be encouraged, not muted.

These discretionary powers that judges have over admissibility and process are tremendously important in coping with technological evidence.

(ii) Character Evidence and the exclusionary discretion

Information posted by someone on social media can disclose a tremendous amount about their character. That is why potential employers consult it when they can. Social media postings as well as emails and texts, which are used in notoriously less discrete ways than paper correspondence or even face-to-face conversations, can provide a treasure trove of information useful in discrediting witnesses by exposing their general character or proving character where character is relevant.

---

120 *R. v. Seaboyer*, 1991 CarswellOnt 1022, [1991] 2 S.C.R. 577, 1991 CarswellOnt 109 (S.C.C.) [*Seaboyer*].

121 *R. v. Felderhof*, 2003 CarswellOnt 4943, [2003] O.J. No. 4819 (Ont. C.A.)

122 *Hamilton*, *supra* note 4.

Defence lawyers therefore often search the public Facebook sites of complainants and important witnesses for data. Some seek out "friends" willing to share access to non-public postings. When this does not work they may have someone contact the complainant or witness electronically to ask to be added as a "friend." It is not uncommon for this ruse to work. Many people are garrulous when it comes to social media.

Social practices surrounding social media can therefore result in the discovery of a rich catalogue of relevant information. It can also lead to the production and potential presentation at trial of an array of tangential, time consuming or pointlessly embarrassing information.

The general exclusionary discretion gives the courts the tools to deal with this, particularly where this information is used to discredit a witness. The virtue in using a discretionary approach rather than to prohibit uninvited access to social media absolutely is that this practice of scouring Facebook and social media has, in some cases, produced extremely probative information. Social media postings can be important in child protection cases,[123] and in access cases.[124] They can also produce information with specific relevance to the case. In *R. v. De Finney* Facebook was used by a victim to identify her assailant[125] and in *R. v. B.B.* Facebook postings were useful in demonstrating the animus the complainant had against the accused.[126] Where social media information is most apt to be used, however, is in discrediting witnesses on the basis of their character.

Ordinarily character evidence of this kind is presented during cross-examination. This kind of information is used to confront the witness with their discreditable conduct, associations or lifestyle. On its face the law of evidence has been generous in permitting lawyers to cross-examine opposing witnesses other than accused persons using this kind of information. It has historically been considered relevant in showing a court the kind of person they are being asked to believe. Still, discreditable conduct questioning has never been without its limits. Judges have long recognized the discretion to prevent or abridge cross-examination that is irrelevant, prolix or insulting.[127] The legal test for exercising that discretion is now clearly defined. Courts simply apply the formula used in the general discretion to exclude evidence — probative value balanced against prejudice. If the line of questioning is prejudicial and not probative enough, it can be easily controlled.

---

123 See *Children's Aid Society of Northumberland v. T. (H.)*, 2009 CarswellOnt 23, [2009] O.J. No. 15 (Ont. S.C.J.); affirmed 2011 CarswellOnt 213 (Ont. Div. Ct.).

124 See, for example, *R. (A.) v. R. (A.M.)*, 2009 CarswellAlta 1965, [2009] A.J. No. 1332 (Alta. Q.B.).

125 *R. v. De Finney*, 2011 CarswellOnt 12057, [2011] O.J. No. 4926 (Ont. C.J.).

126 See *R. v. Bryan*, 2011 CarswellOnt 3359, [2011] O.J. No. 2204 (Ont. S.C.J.) and see *R. v. Rowe*, 2010 CarswellNfld 441, [2010] N.J. No. 442 (N.L. Prov. Ct.).

127 *R. v. Anderson*, 1938 CarswellMan 23, 70 C.C.C. 275 (Man. C.A.).

Here are some key questions the trial judge might pose in deciding whether to permit cross-examination on character information derived from social media:

> (1) Probative Value — the materiality of the evidence (How important is the issue the evidence addresses?)
>
> > a. First, judges need to ensure that the stated purpose for which the evidence is offered is genuine. They therefore need to identify the actual purpose the evidence is apt to serve. For example, evidence offered as a basis for discrediting a testifying sexual assault complainant that discloses the complainants attitudes about dress or sexuality are apt, in substance, to be about sexual reputation or to invite the prohibited twin myth inferences identified in *R. v. Seaboyer*,[128] and should generally not be allowed.
> >
> > b. Second, where evidence is directed at the credibility of a witness, judges need to evaluate how important the credibility of that witness is by examining how central or important the testimony of the witness is.
>
> (2) Probative Value — the influence of the evidence (How compelling is the evidence in resolving the issue it addresses?)
>
> > c. Judges need to evaluate the impact the information could have on the credibility of the witness, even if true. Can the subject of inquiry truly have a material impact on the readiness of the court to believe the witness? The greater the prospect that it will, the more probative the evidence is.
>
> (3) Probative Value — the credibility and reliability of the evidence (Is the information the questioning is based upon compelling enough to warrant exploration?)
>
> > d. Is there a realistic foundation for believing the information being relied upon by the cross-examiner could be true? If the foundation for the line of questioning appears to lay in internet gossip there may not be a sufficient "good faith" foundation for the questioning to satisfy the requirements of *R. v. Lyttle*.[129] Counsel should not make suggestions unless they have a good faith basis for believing that those suggestions bear a reasonable likelihood of accuracy. Where no good faith basis is apparent, courts are free to ask counsel to make their foundation clear.[130] Even if there is a good faith basis, the exclusionary discretion still permits the exclusion of unreliable information. Great care should be exercised before cutting off lines of in-

---

128 *Seaboyer*, *supra* note 120.

129 *R. v. Lyttle*, 2004 CarswellOnt 511, 2004 CarswellOnt 510, 180 C.C.C. (3d) 476 (S.C.C.).

130 *Ibid.* at para. 52.

quiry, particularly inquiries undertaken by or on behalf of accused persons.

(4) Prejudice — adverse consequences to parties and witnesses

e. Does the manner in which the information was obtained constitute an inappropriate violation of the privacy interests of the witness or complainant? Where the authorities are involved in securing non-public information from social media the *Charter* may be implicated. Even where the *Charter* does not apply, a consideration in permitting the line of inquiry is the fairness of the manner in which the evidence was secured. Subterfuge to gain access to information not publicly shared is a factor that could support an exclusionary decision;

f. Is the information itself embarrassing or damaging to the reputation of the witness? If so, consideration has to be undertaken as to whether the information is probative enough to warrant this result.

(5) Prejudice — adverse practical implications

g. Will the presentation of the information be time-consuming or distracting or open collateral issues that may require exploration? If so, is the information probative enough to warrant the inquiry?

(6) Prejudice — prejudice to the administration of justice

h. Does the information exploit prejudicial stereotypes, or is it inflammatory enough to provoke a more emotional than rational reaction?

i. Is the information complex enough that it could confuse the decision?

j. Is the information apt, given its nature, to discourage future complaints to the criminal justice system from being made, or to damage socially useful activities such as counselling and therapy from being undertaken?

If the questioning is permitted and the witness denies suggestions made about their discreditable character, the "collateral facts" rule is engaged. This is because the "character" of a witness is generally considered to be a collateral fact. It is "not relevant to matters which must be proved for the determination of the case."[131] If strictly applied the collateral facts rule would mean that while counsel can use information derived from Facebook and other electronic media that reflects adversely on the character of a witness in order to frame the questions asked, if the witness denies the suggestion, that denial cannot be challenged. If the collateral facts rule is applied with full vigour, the cross-examiner cannot simply take a print-out of the Facebook page and thrust it before the witness in an effort to prove the allegation and thereby contradict the witness.

---

131 *R. v. Krause*, 1986 CarswellBC 761, 1986 CarswellBC 330, 54 C.R. (3d) 294 at 301 (S.C.C.).

The precise definition of a collateral fact is, however, a matter of controversy. In practice courts tend to exercise discretion whether to permit a witness's answers to be contradicted. Again, if the exercise could be a productive one in exposing relevant information about the credibility or reliability of the witness, courts may permit the contradiction evidence to be used, particularly where the accused person is the one seeking to lead the evidence.[132]

(iii) Demonstrative Evidence

Computer graphics and animation can make a significant contribution to the presentation of evidence in courtrooms. They can be used to assist in demonstrating what the evidence purports to show. These graphics and animations are not evidence, *per se*. They are instead, "testimonial aids."

The admission of computer graphics, such as computer-generated charts and graphs, is simple. They are nothing more than mundane examples of demonstrative evidence operating in much the same way poster-board graphs and charts or three-dimensional anatomical models do. The foundational question for determining their admission is whether the chart or diagram would assist the trier of fact in understanding the evidence. This inquiry includes an evaluation of whether the graphic is presented in a misleading manner. If so, the trial judge has the discretion to exclude the visual aid as too prejudicial to the administration of justice to admit. For example, a graph purporting to plot subjects having values of 103, 107, 102 and 109 would be misleading if it began with a baseline of 100. The visual image would suggest differences of 10 to 60 per cent when the actual differences are a fraction of that.

Computer animations involving moving objects can also be powerful litigation aids. Probably because of their production costs they are uncommonly used in Canadian courts. The most famous Canadian illustration, *R. v. Suzack*,[133] involved the use of computers to demonstrate the trajectory of bullets, something that can be testified to but is difficult to picture without such assistance. This kind of evidence is more dangerous than stationary computer graphics because it can overwhelm the testimony that it is supposed to aid, particularly where full computer animation purports to constitute the recreation of events. It therefore has to be treated as a video re-enactment would. The probative value and prejudicial effect of the evidence must be closely scrutinized, with probative value being linked inextricably with accuracy.[134] If it is based on disputed facts or purports to depict events that are too complex and dynamic to permit fair reproduction it may not be probative enough to

---

132 See David M Paciocco, "Using Collateral Facts with Discretion" (2002) 46 Crim LQ 160.

133 *R. v. Suzack*, [1995] O.J. No. 4237, 1995 CarswellOnt 1350 (Ont. Gen. Div.); affirmed 2000 CarswellOnt 95 (Ont. C.A.); leave to appeal refused 2001 CarswellOnt 1076, 2001 CarswellOnt 1075 (S.C.C.).

134 See *R. v. MacDonald*, 2000 CarswellOnt 2416, 146 C.C.C. (3d) 525 (Ont. C.A.) for an example of these principles applied to a physical as opposed to computer-generated re-enactment.

admit.[135] Moreover, since it is the product of computer generation, the images shown require authentication. The computer programmer may have to be called to explain the process of preparing the simulation and to identify its shortcomings.[136]

(iv) Visual Presentation Aids

Computer presentation tools can provide clarity and emphasis not only during argument but also during the presentation of evidence. It is now common for prosecutors to present identification evidence in electronic format, and many courtrooms are now wired. *R. v. MacKay*[137] was an early case dealing with this kind of practice, decided only a decade ago. The Court engaged in a careful evaluation of the costs and benefits involved in permitting the Crown to present its photographic evidence using a computer program that could enhance viewing. Of concern to the defence was that only the Crown had access to this technology. The Crown agreed, however, to make available a technology expert to assist the accused when it used the photographs, ameliorating this unfairness. The Trial Judge ensured that the use of the technology was fair and ordered that it could be used as requested. The decision effectively involved the discretion the judge had in trial management, informed by the familiar probative value, prejudice inquiry.

The same holds true with PowerPoint and other visual presentation aids. Most often such tools are used by experts to assist in presenting their evidence. This is not always so. In *R. v. Hamilton*,[138] for example, PowerPoint was used by a police witness in explaining the location, timing and pattern of telephone calls between those alleged to have been involved in a robbery, after the supporting background testimony had been provided by representatives from the relevant cell phone service providers. This assisted the Ontario Court of Appeal in rejecting an appeal that the evidence should not have been admitted without a *voir dire*. The Court described the cell phone evidence as factual and not opinion evidence, saying this:

> Additionally, the jury would have had no difficulty in understanding the cell phone location evidence, especially after it was summarized in a PowerPoint presentation. That presentation undoubtedly clarified the evidence and put to rest any possibility the jury might have been confused by it. The presentation of the cell phone evidence did take a fair amount of time, seven days. But in the context of a four-month trial, this was not an overly long amount of time.[139]

In the May 2009 trial of Ottawa Mayor, Larry O'Brien, defence counsel used PowerPoint effectively to project the documents and media reports it was using to cross-examine the key Crown witness. Contradictions were displayed for the judge and witness to see. This was not done simply to increase the impact of the exercise

---

135 See *Green v. Lawrence*, 1996 CarswellMan 217, 109 Man. R. (2d) 168 (Man. Q.B.) where the computer program created an unfair impression of the relative size and strength of the combatants.

136 See *Owens (Litigation Guardian of) v. Grandell*, 1994 CarswellOnt 3918, [1994] O.J. No. 496 (Ont. Gen. Div.).

137 *R. v. MacKay*, 2002 CarswellSask 490, [2002] S. J. No. 459 (Sask. Q.B.).

138 *Hamilton*, *supra* note 4.

139 *Ibid.* at para. 282.

for the judge. Having a highly visible display of the relevant passages ensured that the line of questioning could be easily followed and arguably had some psychological impact on the witness during cross-examination, given that his prior comments were so tangibly presented. Courts, exercising their discretion to control the process, clearly have the discretion to allow or refuse this kind of tactic, after evaluating its utility and its costs.

II. CONCLUSION

As can be seen, for the most part the laws of evidence are suitable without radical transformation to cope with new technologies. While their application can be affected when challenged with technological evidence, the rules themselves remain familiar. The following propositions can assist in simplifying the law of evidence as it applies to new technologies:

(a) Limits on Expert Evidence

(1) Not all technology needs to be explained by expert witnesses. Expert evidence rules apply solely to "special skill or knowledge," or skill or knowledge that is exclusive or unique rather than held by many members of the public. Similarly, the expert evidence rules apply only if that special skill or knowledge is "beyond the ken of ordinary people." Lay witnesses can therefore offer evidence about the mundane operation of technologies commonly used by ordinary people, such as social media programs, smart phones or commercially available computer software.

(b) Judicial Notice

(2) Courts should take a functional approach to judicial notice that will permit them to cope with technology that is broadly relied upon by ordinary persons. This includes accepting, without the need for proof, the capabilities and operation of new technologies that are broadly used or understood by members of the public.

(c) Electronic Records, Authentication and the Best Evidence Rule

(3) As a general rule, the party presenting an electronic document is required to furnish an evidentiary foundation capable of supporting a finding that the electronic document is that which it is purported to be, coupled with compliance with the "best evidence" requirements described in propositions 9 and 10 below.

(4) Where such evidence has been presented, a factual controversy about the whether the document is genuine in its entirety is best resolved at the end of the case as a matter of fact rather than as a question of admissibility.

(5) The same holds true where there is a contest over whether the electronic document may have been altered, such as a doctored email. This is ordinarily a matter of weight and not admissibility.

(6) While the continuity of the condition of an exhibit is not ordinarily a precondition to its admissibility, if there is no witness who can verify the authenticity of an electronically recorded document with direct testimony, those documents may have to be authenticated as a matter of fact by showing the *continuity of their chain of custody* from recording, to storing, to retrieval from a computer system. The way this is done is to demonstrate that the electronic document system was functioning

properly, which can be achieved using the "best evidence" requirements described in propositions 9 and 10 below.

(7) Exceptionally, the continuity of the condition of electronically recorded photographs, videotapes and audiotapes must be demonstrated before they are admissible. As artificial reproductions of actual images or sounds, their authenticity depends on their accurate representation of what they purport to depict. Accordingly, the party offering the electronically recorded photographs, videotapes or audiotapes must present evidence capable of showing that the photograph, videotape or audiotape remains an accurate and fair reproduction of the thing it purports to recreate.

(8) There is a distinction between authenticity and the accuracy of the contents of the documents. If the document is authenticated, it is admissible even though some of the information that was input into the document may be inaccurate. The proper way to deal with the risk of inaccuracy is to bear it in mind when ultimately deciding what weight to give to the evidence in question. This proposition is particularly important for time and date stamps generated by computer. Their potential imprecision should not affect the admissibility of the relevant electronic document, but care must be taken when relying on the time and date stamps.

(9) The statutory best evidence rules applicable to electronic documents, including digitized audiotapes, photographs and videotapes are easily met, subject to rebuttal, by:

a. The evidence of witnesses who can testify directly to the accuracy of the document, including audiotapes, photographs and videotapes; or

b. The evidence of witnesses that they sent or received a relevant and coherent electronic document as an email, text message or attachment by cellphone or computer system, or that they successfully downloaded a responsive and coherent document after putting appropriate commands into a search engine; or

c. Evidence that the electronic document was recorded or stored in a computer system belonging to the opposing party litigant; or

d. Evidence that the electronic document was recorded or stored in the usual and ordinary course of business independently by a person who is not a party to the litigation.

(10) The statutory best evidence rules that apply to electronic documents can alternatively be complied with by proving, subject to rebuttal, that:

a. the relevant document was signed with a "secure electronic signature" or

b. by using a print out of an electronic document where the printout has been manifestly or consistently acted on, relied on, or used as a record of the information recorded or stored in the print out.

(d) The Law of Hearsay

(11) Computer Generated Information consisting of data created by a computer system is not hearsay even when offered to prove the facts it asserts. Admissibility depends on its reliability which can be established by expert evidence, or in appropriate cases, by taking judicial notice.

(12) Electronic documents which contain statements of fact may nonetheless be admitted without hearsay exception if, by their nature, they lead to relevant circumstantial inferences, for example, airline tickets or proof of the use of bar coded frequency identification tags linked to individuals.

(13) The most commonly relevant hearsay exceptions apart from the principled exception include admissions by opposing party litigants, the business records exceptions to the hearsay rule, and the *res gestae* exception — most notably the "statement of present mental state exception" and the "excited utterance exception." The latter exception is useful in admitting 9-1-1 calls as evidence of the truth of the facts claimed during the 9-1-1 call.

(e) The Law of Privilege

(14) The law of privilege has yet to change even though new conceptions of privacy are developing as the result of new technologies. Courts nonetheless need to apply the existing rules with sensitivity to their underlying purpose so that reduced opportunities for privacy or the increased risk of unintentional disclosure do not defeat the policy objectives protected by the privileges in question. This is particularly so with solicitor-client privilege.

(f) Exclusionary and Procedural Discretion

(15) Courts can make profitable use of the exclusionary discretion in controlling the abusive or unproductive use of information secured from social media sites and other electronic databanks by excluding evidence whose probative value is outweighed by its prejudice. Probative value includes an assessment of how important the issue being address with that evidence is to the case, how informative the evidence is on that issue, and the credibility and reliability of the information. Prejudice includes the adverse consequences receiving the evidence would have for the parties and witnesses, the adverse practical effects of admission on the efficiency of the trial process, and prejudice to the administration of justice including misleading the decision-maker or discouraging future co-operation with the criminal justice system. A higher degree of prejudice is required to exclude defence evidence.

(16) Courts can make profitable use of their discretion to ensure that demonstrative evidence is used fairly, in a probative and productive way.

(17) Courts should exercise their discretion to control the manner in which evidence is presented to ensure that technological aids to the presentation of evidence, such as PowerPoint, are used appropriately.

None of this is radical surgery. All of it is entirely doable. The law is well equipped for coping with the law of evidence in a technological age.