Stockwoods.
Smart Litigation.

DECODING DIGITAL EVIDENCE

NADER R. HASAN
NADERH@STOCKWOODS.CA

GERALD CHAN
GERALDC@STOCKWOODS.CA

Criminal Lawyers' Association Conference, November 16, 2019

OVERVIEW

- Authentication of digital evidence
- Compelling passcodes
- Artificial Intelligence

SCENARIO #1: ADMISSIBILITY UNDER CEA

Your client's I-Phone call log shows that she never phoned the co-accused on the night in question. You want to get the call log into evidence. She has long since wiped the call log but took a screenshot of the call log before deleting it. Can you get the screenshot into evidence? How?

AUTHENTICATION & ADMISSIBILITY

Not knowing how to authenticate electronic evidence can lead to rulings of inadmissibility, which can further lead to a finding of ineffective assistance of counsel!

See: R. v. Gadam, 2019 ONCA 345

DEFINITIONS

Canada Evidence Act, s. 31.8

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

ELECTRONIC RECORDS INCLUDE…

- emails,
- all computer files,
- metadata connected to these files,
- browsing history,
- content posted online on Web forums and social media platforms (Twitter and Facebook, text messages, online chats),
- screenshots,
- hard copies electronic files.

See *R. v. Soh*, 2014 NBQB 20 at para. 21

AUTHENTICATION & ADMISSIBILITY: A 2-STEP PROCESS

Step 1: Establishing Authenticity

Step 2: Proof of Integrity/Reliability

STEP 1: AUTHENTICITY

Canada Evidence Act:

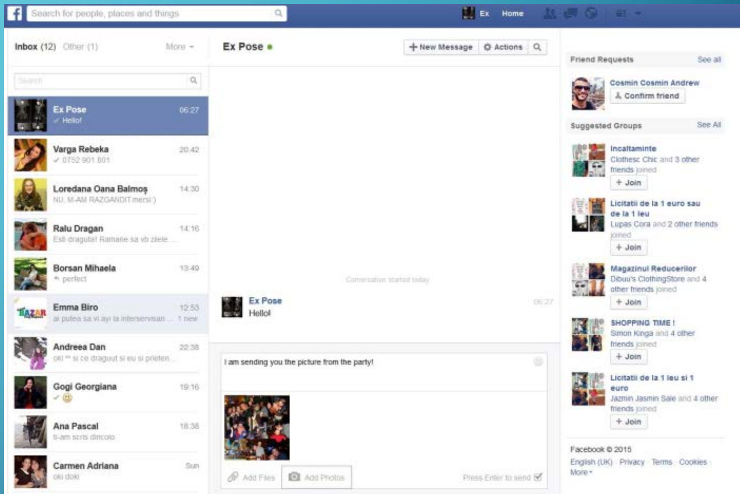
> 31.1 Any person seeking to admit an electronic document as evidence has the burden of proving its authenticity by evidence capable of supporting a finding that the electronic document **is that which it is purported to be**.

STEP 1: AUTHENTICITY

- This is a low threshold.
- Establishing authenticity requires only "some evidence" that the document being presented is what it is purported to be. (See *R v CB*, 2019 ONCA 380 at paras 66-67)
- The electronic document being tendered need not be identical to the digital file in question for purposes of authenticity. (See *R v Hamdan*, [2017] BCJ No 986 (Sup Ct).

R. V. HIRSCH - AUTHENTICATING ONLINE EVIDENCE

- Screen captures of the accused’s Facebook page were put to the complainant.
- The Court accepted her authentication based on her general knowledge of the accused and his postings in the past even though she did not write the posts or collect the screen shots.
- The Court stressed that the evidence need only be “capable of authenticating” the document.



Ex Pose 06:27 ✓ Hello!

Varga Rebeka 20:42 ✓ 0752 901 801

Loredana Oana Balmoș 14:30 NU, M-AM RAZGANDIT mersi :)

Ralu Dragan 14:16 Esti draguta! Ramane sa vb ziele ...

Borsan Mihaela 13:49 perfect

Emma Biro 12:53 ai putea sa vi ayi la interservisan ... 1 new

Andreea Dan 22:38 oki ** si ce draguut si eu si prieten...

Gogi Georgiana 19:16 ✓

Ana Pascal 18:36 ti-am scris dincolo

Carmen Adriana Sun oki doki

Conversation started today

Ex Pose 06:27
Hello!

I am sending you the picture from the party!

Cosmin Cosmin Andrew

Incaltaminte
Clothesc Chic and 3 other friends joined

Licitatii de la 1 euro sau de la 1 leu
Lupas Cora and 2 other friends joined

Magazinul Reducerilor
Dibuu's ClothingStore and 4 other friends joined

SHOPPING TIME !
Simon Kinga and 4 other friends joined

Licitatii de la 1 leu si 1 euro
Jazmin Jasmin Sale and 4 other friends joined

Facebook © 2015
English (UK) · Privacy · Terms · Cookies · More

STEP 2: METHODS OF ESTABLISHING INTEGRITY UNDER THE *CEA*:

1. Proving the integrity of the document system that recorded or stored the document by calling direct or circumstantial 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:
   i. “functioning computer system” presumption (s. 31.3(a)),
   ii. the “opposing party” presumption, (s. 31.3(b))
   iii. “third party business record” presumption (s. 31(3)(c).
3. 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)).

ESTABLISHING INTEGRITY UNDER THE CEA (*IN PLAIN ENGLISH*)

- Calling a witness to testify that the text messages in the screenshot are consistent with what they remember typing and the texts they remember receiving (s.31.2(1)(a)).
- Integrity presumed when evidence you seek to introduce comes from an adverse party's device(s. 31.3(b)).
- Calling a witness testify that when they examined the device from which the text messages were captured, the device appeared to be working properly (s. 31.3(a)).
- Calling a witness to testify that they logged into Facebook, which was functioning normally, and took screenshots of the Facebook Wall. (s. 31.3(a)).

SCENARIO #1: ADMISSIBILITY UNDER CEA

Your client says her I-Phone call log shows that she never phoned the co-accused on the night in question. You want to get the call log into evidence. She has long since wiped the call log but took a screenshot of the call log before deleting it. Can you get the screenshot into evidence? How?

Answer: *Most likely (s.31.2(1)(a)).*

SCENARIO #2: ADMISSIBILITY UNDER *CEA*

Your client, who has been charged with trafficking cocaine, shows you a text from a lady friend that reads, "*You are very handsome and definitely not a drug dealer.*" Can you get that text message into the record for the purpose of showing your client was not involved in the impugned transaction?

SECTION 31 IS NOT A HEARSAY EXCEPTION!

- Section 31 of the CEA establishes a means of *authenticating* electronic evidence and satisfying the best evidence rule. (See CEA, 31.7.)
- It is not a hearsay exception.
- Therefore, satisfying the authenticity and reliability thresholds are necessary but necessarily sufficient to admit electronic evidence depending on its purpose.

R V MONDOR, [2014] OJ NO 1392 (OCJ)

- Crown sought to introduce electronic evidence, which were purportedly invoices that showed that the accused had purchased child pornography.
- Satisfying authentication and integrity requirements of s. 31 of the CEA not enough to introduce to the records for the truth of their contents.
- Crown also needed to satisfy the business records exception under s. 30 of the CEA (or the common law business records exception).
- *See also R v Bridgman*, 2017 ONCA 940; *R v NW*, 2018 ONSC *774*.

- *R. v. Bridgman*, 2017 ONCA 940
  - text messages admissible under the principled approach to rule against hearsay and the "documents in possession" rule.

- *R .v. N.W.*, 2018 ONSC 774
  - Trial judge erred in admitting text messages for truth of their contents.

ADMISSIBILITY UNDER CEA

Does that mean that call logs, Internet search histories and Google maps print-outs, time stamps on text messages are hearsay?

IS THE DIGITAL EVIDENCE SPEAKING FOR ITSELF?

USER-GENERATED DATA

- Texts, Facebook posts, e-mails.
- Even if you meet requirements of CEA, s. 31, must still satisfy other rules of evidence (e.g. hearsay exception) for it to be admitted for truth of its contents.

DEVICE-GENERATED DATA

- Metadata; activity logs; browser history
- Akin to "real evidence".

SCENARIO #3: EXPERT EVIDENCE REQUIRED?

You want to introduce a Twitter thread into evidence. Do you need to call expert evidence on how Twitter works?

MUNDANE TECHNOLOGY EVIDENCE

- Use of social media
- Availability of apps
- General use of applications
- Appearance of data/information within these programs/applications
- *R. v. Hamilton*, [2011] OJ No 2306 (CA) : “simply factual evidence that witnesses with the knowledge and experience… can testify about” (para. 279)

IS AN EXPERT REQUIRED?

- What kind of evidence am I dealing with?
  - Metadata or user-generated data?
- Is it high-tech or mundane?
- Is it day-to-day computing?
- What can experts testify about?

CHECKLIST

- Can I establish authenticity? [CEA, s. 31.1]
  - Authorship or continuity issues?
- Can I establish integrity? [CEA, s. 31.2, 31.3]
  - Evidence of tampering?
  - What indirect or circumstantial evidence is available to help corroborate the evidence I am seeking to rely?
- Do I have a hearsay problem?
- Does the evidence speak for itself?
- Is there any other exclusionary rule that applies (e.g., CC, s. 278.1)?
- Do I need an expert to explain this evidence?

COMPELLING PASSCODES

SCENARIO #4: COMPELLING PASSCODES

You leave this conference later today. You visit an old friend and are hanging out in their backyard. The police show up, start asking questions, and seize everyone's phones. They want to know your passcode. Do you have to give it up?.

R V BOUDREAU-FONTAINE, [2010] QJ NO 5399 (CA)

[39]…[T]his order raises the issues of the right to silence, the right to be presumed innocent, the right not to be conscripted against oneself, and the protection against self-incrimination. Commanded to participate in the police investigation and to give crucial information, contrary to his constitutional rights, the respondent made a statement (identification of his password) that is inadmissible and that renders the subsequent seizure of the data unreasonable.

SELF-INCRIMINATION AND PHONES

- Right against self-incrimination prevents any order that compels the accused to *participate* in the investigation.
- Compelling disclosure of passcode = violation of s. 7
  - *R. v. Boudreau-Fontaine*, [2010] QJ No 5399 (C.A.)
  - *R v Shergill*, 2019 ONCJ 54
  - *R v Talbot*, 2017 ONCJ 814

DIRECT VS INDIRECT INCRIMINATION

- Statement or set of digits?

- *R v Shergill*, 2019 ONCJ 54 at para 19:

> "the protection against self-incrimination can retain its force even where the content of the compelled communication is of no intrinsic evidentiary value. This is particularly so where, as here, that communication is essential to the state's ability to access the evidence which they are "really after."

ASSISTANCE ORDER

- Breach of order likely an offence under s. 127

- Collateral attack doubtful: *R. v. Bird,* 2019 SCC 7

- Assert position early to oppose order before it's made

WHAT'S THE REMEDY?

- Derivative use immunity vs. use immunity

- *R v Shergill*, 2019 ONCJ 54 at paras 27-40

WHAT ABOUT THUMB PRINTS?

- Testimonial compulsion is distinct: *R v Shergill,* 2019 ONCJ 54 at paras 41-42
- Passive vs active: *R v Talbot,* 2017 ONCJ 814 at para 38
- Examples of bodily samples being compelled: breath samples, DNA, fingerprinting, etc.
- Go back to rationale of principle against self-incrimination: to prevent coercive methods to extract admissions

ALTERNATIVE ACCESS TO PASSWORDS

- *R v Crawley*, 2018 ONCJ 394

- Police observed swipe pattern through surveillance

- No breach of s. 8 of the *Charter*

AT THE BORDER…

AT THE BORDER…

- CBSA relies on sections 13 and 153.1 of *Customs Act* to demand cell phone passwords.
- Authority upheld in *R. v. Buss*, 2014 BCPC 16 at para. 33, *R. v. Whittaker*, 2010 NBPC 32 at para. 4.

REP AT THE BORDER

The CBSA asserts that its officers have the power to:

- Look at all e-mails on your phone;
- Look at your Internet browser history;
- Use a tool to engage in ***forensic examination*** of those devices, which results in looking at things that might be hidden on the computer; files that have been deleted from the computer; and examining all parts of the electronic device that would "be of interest" and "may conceal" illegal activities.

REP AT THE BORDER: *CUSTOMS ACT*

Section 99 (1)(a)

"An officer may at any time up to the time of release, **examine** any goods that have been imported and open or **cause to be opened** any **package or container** of imported goods and take samples of imported goods in reasonable amounts…"

Section 2

"***goods***, for greater certainty, includes conveyances, animals and any document in any form; (*marchandises*)"

LITIGATING ALGORITHMS

- Policing
- Risk assessments (bail, sentencing)
- Identifying the perpetrator (probabilistic genotyping, facial recognition)

LITIGATING ALGORITHMS

- Disclosure
- Expert evidence
- Cross-examining a computer