Canadian Journal of Law and Technology

Volume 19
Number 2 *Technology-facilitated Gender-based Violence*

Article 7

1-2022

On the Internet, Nobody Knows You are a Dog: Contested Authorship of Digital Evidence in Cases of Gender-based Violence

Suzie Dunn
Dalhousie University Schulich School of Law

Moira Aikenhead
University of British Columbia, Allard School of Law

On the Internet, Nobody Knows You are a Dog: Contested Authorship of Digital Evidence in Cases of Gender-based Violence

Suzie Dunn & Moira Aikenhead[*]

1. INTRODUCTION: HURDLES IN ESTABLISHING AUTHORSHIP OF DIGITAL EVIDENCE

Social media and other forms of digital communication have become a rich source of evidence in many modern-day trials.[1] The ephemeral and dynamic nature of digital evidence has raised novel evidentiary issues, and courts have begun to navigate how digital forms of evidence can be used in criminal cases.[2] Lisa Silver has discussed how social media, text, and email-based evidence have been appearing with increasing frequency in criminal cases, creating some challenges when applying traditional rules of evidence.[3] As evidentiary rules about electronic documents develop, and existing rules of evidence are applied to these documents, police, lawyers, and judges must familiarize themselves with evolving rules and practices.[4]

As with other areas of criminal law, digital evidence is beginning to play an increasingly significant role in gender-based violence ("GBV") cases.[5] New issues are arising around how this evidence should be collected and treated by the courts. Taking into consideration historical and ongoing barriers that complainants in GBV trials have faced, this article applies a feminist, equality-focused lens to identify existing and potential issues that the police,

---

[*] Suzie Dunn (she/her) is an Assistant Professor at Dalhousie University's Schulich School of Law and a PhD Candidate at the University of Ottawa, Faculty of Law. Moira Aikenhead (she/her) is a PhD Candidate at the Peter A. Allard School of Law at the University of British Columbia. The authors would like to thank Lisa Dufraimont, Jane Bailey, Mabel Lai, Gerald Chan, and an anonymous reviewer for their insightful guidance in improving this paper.

1 Hannah Claire Saunders, "Social Media as Evidence in Family Court: Understanding How to Find a Preserve Information" (2015) 40:1 Can L Libr Rev 11; Lisa A Silver, "The Unclear Picture of Social Media Evidence" (2020) 43:3 Man LJ 111; Alexa Dodge, "The Digital Witness: The Role of Digital Evidence in Criminal Justice Responses to Sexual Violence" (2018) 19:2 Feminist Theory 303 [Dodge, "Digital Witness"].

2 Gerald Chan & Mabel Lai, "Evidence: AI in the Courtroom" in Jill Presser, Jesse Beatson & Gerald Chan, eds, *Litigating Artificial Intelligence* (Toronto: Emond Publishing, 2021).

3 Silver, *supra* note 1.

4 David Paciocco, "Proof and Progress: Coping with the Law of Evidence in a Technological Age" (2013) 11 CJLT 181.

5 Alexa Dodge et al, "'This Isn't Your Father's Police Force': Digital Evidence in Sexual Assault Investigations" (2019) 52:4 Austl & NZ J Crim 499.

complainants, Crown counsel, defence counsel, and judges in GBV trials should be alert to when dealing with digital evidence. Specifically, this article focuses on challenges related to establishing authorship of digital evidence in GBV trails. Questions of authorship may arise when there are existing text messages, social media posts, or other digital content allegedly written by the accused or another witness. In many cases, such evidence may be crucial in proving the identity of the perpetrator, an essential element of every criminal offence. For example, a complainant may have received Facebook messages in which the accused appears to apologize for or admit to sexually assaulting them. In such a case, the Crown must ensure these relevant electronic documents are admitted at trial and must adduce evidence sufficient to establish the accused in fact wrote the messages. There are various evidentiary hurdles that must be met to have the evidence admitted, authenticated, and proven at trial.

There are numerous considerations justice system actors must take into account in order to properly address the issue of authorship of digital evidence at trial. In order to have relevant electronic documents admitted, and authorship of those documents established, police may need to undertake additional investigatory efforts to collect evidence that can assist in demonstrating authorship. In the case of the Crown, certain evidentiary burdens must be met, and complainants and other witnesses must be prepared by Crown counsel to address the accuracy of any digital evidence associated with them during their testimony. Defence counsel may contest the accuracy or reliability of digital evidence tendered by the Crown, including putting forward theories about alternative authors of the messages or asserting that the Crown has failed to prove the accused wrote the messages.

In the following sections, we examine various aspects of digital evidence at GBV trials, drawing on relevant Canadian criminal case law. First, we describe some of the unique challenges related to electronic documents generally with respect to determining authorship. Second, we review some of the historical and ongoing practices within the criminal justice system that rely on harmful gendered myths about GBV and note the potential for these myths to emerge in relation to digital evidence. Third, we discuss the duty of investigating police officers to gather the necessary available digital evidence to demonstrate authorship and note potential gaps in current investigatory practices that could negatively impact the trial outcome for victims of GBV. Fourth, we review some of the evidentiary rules for admitting and authenticating digital evidence at trial, discussing how these rules have been interpreted and applied in the GBV context. Fifth, we examine what evidentiary burdens the Crown faces in proving authorship at trial, highlighting the developing nature of law in this area. Finally, we conclude with several recommendations for various justice system actors on how to manage digital evidence in GBV cases where authorship may be contested.

While the focus of this article is on examining and making recommendations in relation to the use of digital evidence in GBV criminal trials, we recognize

significant systemic problems with the criminal justice system that make it an undesirable and unrealistic option for many victims of GBV.[6] Victims are not always believed by the police even when they have legitimate claims,[7] and many ongoing practices within the adversarial trial process create additional trauma for some GBV victims.[8] It is well documented that many Indigenous and Black individuals, people of colour, and members of the LGBTQ2s+ community have experienced discrimination when engaging with the police and justice system, and as such members of these groups may be particularly disinclined to rely on the criminal justice system to address violence against them.[9] In Canada, there is a long history of the justice system ignoring reports of violence against Indigenous women and girls, and in some cases police and other justice system actors have directly perpetrated this violence, leaving deep-seated distrust in the criminal justice system and a desire for alternative options for addressing GBV.[10] As a result, many advocates and victims have been exploring alternative methods of

---

6 See e.g. National Inquiry into Missing and Murdered Indigenous Women and Girls, *Reclaiming Power and Place: The Final Report of the National Inquiry into Missing and Murdered Indigenous Women and Girls* (National Inquiry into Missing and Murdered Indigenous Women and Girls, 2019) (also see *Supplementary Report: Quebec*); Human Rights Watch, *Those Who Take Us Away: Abusive Policing and Failures in Protection of Indigenous Women and Girls in Northern British Columbia, Canada* (New York: Human Rights Watch, 2013); Sherene Razack, *Looking White People in the Eye: Gender, Race and Culture in the Courtrooms and Classrooms* (Toronto: University of Toronto Press, 1999); Rebecca Rose, *Before the Parade: A History of Halifax's Gay, Lesbian, and Bisexual Communities 1972-1984* (Halifax: Nimbus Publishing, 2019).

7 Robyn Doolittle, "Why Police Dismiss 1 in 5 Sexual Assault Claims as Baseless" *The Globe & Mail* (3 February 2017), online: < www.theglobeandmail.com/news/investigations/unfounded-sexual-assault-canada-main/article33891309/ > [Doolittle, "Why Police Dismiss"]; National Inquiry into Missing and Murdered Indigenous Women and Girls, *ibid.*

8 Elaine Craig, *Putting Trials on Trial: Sexual Assault and the Failure of the Legal Profession* (Montreal: McGill-Queen's University Press, 2018) [Craig, "Trials on Trial"].

9 National Inquiry into Missing and Murdered Indigenous Women and Girls, *supra* note 6; Human Rights Watch, *supra* note 6; Razack, *supra* note 6; Rose, *supra* note 6; Craig, *supra* note 8; Jessica A Turchik, Claire L Hebenstreit & Stephanie S Judson, "An Examination of the Gender Inclusiveness of Current Theories of Sexual Violence in Adulthood: Recognizing Male Victims, Female Perpetrators, and Same-Sex Violence" (2016) 17:2 Trauma, Violence, & Abuse 133; Katie Edwards, Kateryna Sylaska & Angela Neal, "Intimate Partner Violence Among Sexual Minority Populations: A Critical Review of the Literature and Agenda for Future Research" (2015) 5:2 Psychology of Violence 112; Dora M Y Tam et al, "Racial Minority Women and Criminal Justice Responses to Domestic Violence" (2016) 31:4 J Family Violence 527; Natasha Bakht, "What's in a Face? Demeanour Evidence in the Sexual Assault Context" in Elizabeth A Sheehy, ed, *Sexual Assault in Canada: Law, Legal Practice and Women's Activism* (Ottawa: University of Ottawa, 2012) [Sheehy, "Sexual Assault"]; Lisa Dario et al, "Assessing LGBT People's Perceptions of Police Legitimacy" (2020) 67:7 J Homosexuality 885.

10 National Inquiry into Missing and Murdered Indigenous Women and Girls , *supra* note 6; Human Rights Watch, *supra* note 6; Razack, *supra* note 6.

justice[11] and calling for the transformation[12] or even abolition of criminal justice-based systems.[13] Many victims of GBV choose not to engage with the criminal justice system, and others continue to face discriminatory systemic barriers in accessing justice within that system. Within the context of these varied and valid critiques, the recommendations in this paper are premised on the notion that, so long as the criminal justice system remains the primary state-supported mechanism for dealing with GBV, it must be accessible to all victims, all of whom are entitled to investigatory and trial processes that are fair, treat them with dignity, and do not rely on discriminatory beliefs.

(a) Hurdles in Establishing Authorship of Digital Evidence

Proving authorship of a digital message may be crucial to the Crown proving its case against an accused. Establishing that it was the accused who authored a particular digital message or engaged in an online conversation may be a necessary component in establishing identity, which is an essential element of every criminal offence. This may be particularly so in circumstances where the offending behaviour occurred in a digital space, including certain cases of the non-consensual distribution of intimate images, uttering threats, or sexual exploitation.

One of the first evidentiary stages of a criminal trial is admitting evidence.[14] For evidence to be admissible it must be relevant to a material issue in the case, must not be excluded by an exclusionary rule such as hearsay, and must not be excluded through the judge's exclusionary discretion. Wherever there is a question as to whether a particular piece of evidence complies with these requirements, a *voir dire* should be held to determine its admissibility.[15] The standards of admissibility vary depending on the type of evidence and which party is tendering the evidence. For example, real evidence must be relevant, material, and authentic.[16] Authenticity shows that the evidence is what it

---

[11] Nicola Henry, Asher Flynn, & Anastasia Powell, "The Promise and Paradox of Justice" in Nicola Henry, Anastasia Powell, & Asher Flynn, eds, *Rape Justice: Beyond the Criminal Law* (London: Palgrave McMillan, 2015) at 1.

[12] Lise Gotell, "Reassessing the Place of Criminal Law Reform in the Struggle Against Sexual Violence" in Henry, Powell & Flynn, *supra* note 11 at 53.

[13] Moira Donegan, "'Who will Protect you from Rape Without Police?' Here's My Answer to that Question" *The Guardian* (17 June 2020), online: <www.theguardian.com/commentisfree/2020/jun/17/abolish-police-sexual-assault-violence>; Angela P Harris, "Heteropatriarchy Kills: Challenging Gender Violence in a Prison Nation" (2011) 37:13 Wash UJL & Pol'y 13; Kimberlé Crenshaw, "From Private Violence to Mass Incarceration: Thinking Intersectionally About Women, Race, and Social Control" (2012) 59 UCLA L Rev 1418.

[14] David M Paciocco, Palma Paciocco & Lee Stuesser, eds, *The Law of Evidence,* 8th ed (Toronto: Irwin Law, 2020) at 33-62.

[15] Paciocco, *supra* note 4; *R. v. Ball*, 2019 BCCA 32, 2019 CarswellBC 133 (B.C. C.A.) [*Ball*] at para. 67.

[16] Paciocco, Paciocco & Stuesser, *supra* note 14 at 59.

purports to be.[17] The party tendering the evidence, either the Crown or defence, bears the burden of establishing authenticity. There are special rules of authentication for electronic documents, which are governed by the *Canada Evidence Act* (*CEA*), as will be discussed further below. Once threshold admissibility is established, there may be additional hurdles to having the evidence admitted, such as establishing that hearsay evidence falls under an exception to the rule against hearsay. If evidence is ultimately admitted, the weight that the trier of fact will give to that evidence remains a live issue for trial. The standards for admitting evidence are different than the ultimate standards of proof for the case, and the Crown still bears the burden of proving the guilt of the accused beyond a reasonable doubt based on the evidence that was admitted.

Returning to the example of Facebook messages containing an apology for an alleged sexual assault, the messages will be relevant if they assist in proving that the author admitted to the offence and that the author is the accused, as this is material to the issue of identity. If the Crown wishes to tender such evidence, they bear the onus of establishing authenticity. Further, as such statements will constitute hearsay if admitted for the truth of their contents, the Crown also bears the burden of proving on a balance of probabilities that the messages fall within an exception to the rule against hearsay. Assuming the evidence is admitted, the Crown must still prove all elements of the offence, including identity, beyond a reasonable doubt, which may include proving beyond a reasonable doubt that the accused authored the relevant messages.

Electronic documents create certain unique evidentiary challenges in relation to admitting evidence and establishing authorship. While David Paciocco notes that many existing rules of evidence may be applied in the same fashion to electronic documents,[18] authors such as Lisa Silver have noted that electronic evidence lacks the stability, individuality, and access limitations of physical documents such as handwritten letters, creating new challenges for this type of evidence.[19] While disputes as to authorship of evidence at criminal trials are not new, they are occurring with increasing frequency given the societal pivot to digital communications in recent years,[20] and given certain features of digital communications that make authorship a live issue in many cases.

Establishing that a particular individual authored a digital message may be a difficult task for a variety of reasons. For one, it is not always apparent on the face of a digital communication who authored the message.[21] In their discussion

---

17 *R. v. Martin*, 2021 NLCA 1, 2021 CarswellNfld 2 (N.L. C.A.) at para. 47 [*Martin*]; *R. v. C.B.*, 2019 ONCA 380, 2019 CarswellOnt 7222 (Ont. C.A.) at para. 66 [*CB*]; Paciocco, Paciocco & Stuesser, *supra* note 14 at 59.

18 Paciocco, *supra* note 4.

19 Silver, *supra* note 1.

20 Fanny A Ramirez & Jeffrey Lane, "Communication Privacy Management and Digital Evidence in an Intimate Partner Violence Case" (2019) Intl J Communication 5140, online: < link.gale.com/apps/doc/A610340551/LitRC?u = ubcolumbia&sid = summon&xid = 67ebe4d0 > .

of social media and the law, Steve Coughlan and Robert Currie note that an individual's identity is not always clear when using social media but, depending on the type of social media used, there can be some ways to help identify them.[22] Certain social media platforms, such as Facebook, have "real name" policies, requiring users to use "the name they go by in everyday life,"[23] and others, such as LinkedIn, are generally associated with people using their actual name on their accounts.[24] It is quite common for people to use their real names on these sites and to post identifying information such as personal details and photographs identifying them as the owner of the account. Further, they may have a long history of communicating via these platforms, and such previous communications may contain information relevant to establishing their identity. On the other hand, "real name" policies are easy to circumvent and are not stringently enforced.[25] Many people use a pseudonym or a portion of their real name on their social media accounts for privacy or other reasons.[26] Others use multiple accounts on the same social media platform.[27] Further, it is relatively simple to create an account in someone else's name on many social media websites and to send messages that appear to be from that person.[28]

Certain social media platforms, such as Reddit, are designed to encourage anonymous or pseudonymous posting, which raises additional barriers to establishing authorship of content found on these sites, as no identifiable author will be associated with the name on a post or message.[29] In cases involving digital evidence from a website that encourages anonymity, such as Reddit, or from other anonymous phone numbers, social media accounts, or e-mail addresses, additional evidence may be necessary to link this evidence to a particular individual, such as an associated IP address or telecommunications records.[30] To

---

21 Aradhya Sethia, "Rethinking Admissibility of Electronic Evidence" (2016) 24:3 Intl JL & IT 229.

22 Steve Coughlan & Robert J Currie, "Social Media: The Law Simply Stated" (2013) 11:2 CJLT 229.

23 Facebook, "What names are allowed on Facebook?" (2021), posted on *Facebook Help Center,* online: *Facebook* < www.facebook.com/help/112146705538576 > .

24 Coughlan & Currie, *supra* note 22.

25 *Ibid.*; Torill Elvira Mortensen, "Anger, Fear, and Games: The Long Event of #GamerGate" (2016) 13:8 Games & Culture 787.

26 Cassie Cox, "Protecting Victims of Cyberstalking, Cyberharassment, and Online Impersonation through Prosecutions and Effective Laws" (2014) 54:3 Jurimetrics 277.

27 Brooke Erin Duffy & Emily Hund, "Gendered Visibility on Social Media- Navigating Instagram's Authenticity Bind" (2019) 13 Intl J Communication 4983, online: < link.gale.com/apps/doc/A610367795/LitRC?u = ubcolumbia&sid = summon&xid = -b3ef65ca > .

28 Dan Grice & Bryan Schwartz, "Social Incrimination: How North American Courts are Embracing Social Network Evidence in Criminal and Civil Trials" (2012) 36:1 Man LJ 221.

29 Ira P Robbins, "Writings on the Wall: The Need for an Authorship-Centric Approach to the Authentication of Social: Networking Evidence" (2011) 13:1 Minn J L Sci & Tech 1.

further complicate the issue, these types of messages can be sent from "spoofed" accounts, through Tor, or through virtual private networks (VPNs), where the message appears to be coming from a particular email, phone number, or IP address but actually originated from another source.[31] Considering all of these factors, it can be a complex exercise to determine who wrote a particular digital message and what evidence will be sufficient to prove authorship at trial.

Even where pseudonyms, fake accounts, spoofing, or digital manipulation is not an issue and the evidence significantly supports an inference that a message came from an account associated with a particular individual, the interconnectivity of the internet and the accessibility of devices makes it possible for people to access others' accounts with or without their consent.[32] Research by Karen Levy and Bruce Schneier describes how common it is for intimate partners or family members to share or learn one another's passwords and access one other's accounts and devices.[33] If a message is sent from a computer or device to which multiple people have access, this can raise questions about who in fact authored a message from an account accessible on that computer or device.

These realities of digital communications may create difficulties at trial for parties seeking to introduce and rely on potentially relevant digital evidence.[34] As who actually wrote a digital message will not always be readily apparent, parties seeking to tender and rely on such evidence may face evidentiary hurdles in having that evidence admitted or in proving an individual was in fact the author of the communication. Demonstrating or contesting the accuracy of digital evidence may require additional investigatory efforts and evidence.[35] In cases in which the Crown seeks to rely on incriminating digital evidence allegedly authored by an accused as part of a case against them, the Crown bears the onus of proving the accused authored the messages.[36] Defence counsel may need to

---

[30] Coughlan & Currie, *supra* note 22.

[31] Gabriella Sneeringer, "Contact that Can Kill: Orders of Protection, Caller ID Spoofing and Domestic Violence" (2015) 90:3 Chicago-Kent L Rev 1157; Cynthia Fraser et al, "The New Age of Stalking: Technological Implications for Stalking" (2010) 61:4 Juvenile & Family Court J 39; II Savchenko & O Yu Gatsenko, "Analytical Review of Methods of Providing Internet Anonymity" (2015) 49:8 Automatic Control & Computer Sciences 696.

[32] Ken Chasse, "Electronic Records for Evidence and Disclosure and Discovery" (2011) 57 CLQ 284.

[33] Karen Levy & Bruce Schneier, "Privacy Threats in Intimate Relationships" (2020) 6:1 J Cyber Security 1.

[34] As noted by Bennett J in *R. v. Hamzehali*, 2017 BCCA 290, 2017 CarswellBC 2119 (B.C. C.A.) at para. 64, leave to appeal refused *R. v. M.H.*, 2018 CarswellBC 639, 2018 CarswellBC 640 (S.C.C.), "the advent of social media, e-mails and text messages has made the prosecution and defence of charges far more complicated or cumbersome than prior to these new technologies."

[35] Nathan Wiebe, "Regarding Digital Images: Determining Courtroom Admissibility Standards" (2000) 28:1 Man LJ 61.

tender evidence to challenge the integrity or reliability of evidence indicating authorship.[37] Taking into consideration the challenges listed above, Crown counsel must gather evidence supporting a conclusion that the accused was in fact the author.

The types of evidence that will be sufficient to establish authorship of digital evidence at various stages of criminal legal proceedings and in various factual circumstances is still developing. Our exploration of these issues forms the subject of the remainder of this paper. While the nature of digital evidence itself creates a number of evidentiary hurdles, other systemic issues raise particular concerns in relation to establishing authorship in cases of GBV. In the following section, we examine some of these concerns before exploring the current state of the law regarding authorship of digital evidence in cases of GBV from the investigatory to the trial stage of criminal proceedings.

(b) Contested Authorship in the Gender-Based Violence Context

In the past decade, digital evidence has come to be frequently relied on in cases of GBV.[38] It is widely understood that cases involving GBV, particularly sexual assault, are some of the most challenging cases within the criminal justice system.[39] These cases are frequently characterized as "he-said-she-said," as the accused and complainant are often the only witnesses to the incident in question, and there may be no additional evidence corroborating a complainant's version of events.[40] As such, the credibility of the complainant will often be a central

---

[36] *R. v. Harris*, 2010 PESC 32, 2010 CarswellPEI 43 (P.E.I. S.C.) [*Harris*].

[37] *Canada Evidence Act,* RSC 1985, c C-5 , ss 31.1 & 31.3 [*CEA*].

[38] Dodge et al, *supra* note 5; Anastasia Powell, Gregory Stratton & Robin Cameron, "Liminal Images: Criminality, Victimisation and Voyeurism" in Anastasia Powell, Gregory Stratton & Robin Cameron, eds, *Digital Criminology: Crime and Justice in Digital Society* (New York: Routledge, 2018); Anastasia Powell, "Configuring Consent: Emerging Technologies, Unauthorized Sexual Images and Sexual Assault" (2010) 43 Austl & NZ J Crim 76.

[39] Susan Ehrlich, "Perpetuating — and Resisting — Rape Myths in Trial Discourse" in Elizabeth A Sheehy, ed, *Sexual Assault in Canada: Law, Legal Practice and Women's Activism* (Ottawa: University of Ottawa, 2012) [Sheehy, "Sexual Assault"]; Linda Baker, Marcie Campbell & Anna-Lee Straatman, *Overcoming Barriers and Enhancing Supportive Responses: The Research on Sexual Violence Against Women* (London, ON: Centre for Research & Education on Violence Against Women & Children, Western University, 2012); Melissa Lindsay, *A Survey of Survivors of Sexual Violence in Three Canadian Cities* (Ottawa: Department of Justice Canada, 2014); Haley Clark, "A Fair Way to Go: Justice for Victim-Survivors of Sexual Violence" in Henry, Powell & Flynn, *supra* note 11; Margaret Denike, "Sexual Violence and 'Fundamental Justice': On the Failure of Equality Reforms to Criminal Proceedings" (2000) 20:3 Can Woman Studies 151; Elaine Craig, "The Inhospitable Court" (2016) 66:2 UTLJ 197.

[40] Christine Boyle, "Reasonable Doubt in Credibility Contests: Sexual Assault and Sexual Equality" (2009) 13:4 IJEP 269; Jennifer Koshan, "The Judicial Treatment of Marital Rape in Canada: A Post-Criminalisation Case Study" in Melanie Randall, Jennifer Koshan & Patricia Nyaundi, eds, *The Right to Say No: Marital Rape and Law Reform in*

issue at trial. Historically, intrusive and harmful cross-examination by some defence counsel on issues such as a complainant's sexual history resulted in complainants facing such extensive scrutiny that they were essentially the ones "on trial" in these cases.[41] Many complainants find it difficult to participate in these trials, as they are expected to recount what was a personal and traumatizing experience in intimate detail and, due to the adversarial nature of our legal system, face rigorous questioning by defence counsel.[42] This can be an emotionally fraught experience for these witnesses, some of whom experience secondary trauma due to their involvement with the justice system.[43] The frustration and emotional harms many complainants experience are in part due to the highly personal and intimate aspects of the investigation and trial, but they can be compounded by failures in the justice system surrounding evidence collection, witness preparation, and the treatment of the witness while on the stand, particularly when these failures are linked to systemic discrimination against victims of GBV.[44]

As digital evidence is being increasingly relied on in cases of GBV, some authors have noted the potential for this evidence to provide corroboration of victims' versions of events in the context of "he-said-she-said" criminal cases involving sexual assault and other forms of GBV.[45] Violence and the resulting harms could be recorded or photographed, threats and harassing messages could be saved and tendered as evidence, and admissions of guilt could be captured via recordings or screenshots, showing that what victims were claiming was true.[46] However, while digital evidence has proven useful in many GBV cases, it is not a panacea and comes with a series of complexities at trial. Digital evidence must still be interpreted by judges and jurors, inevitably through the lens of their own experiences and biases.[47] Factors that impact the interpretive lens may include a lack of knowledge about modern technology or about the unique evidentiary

---

Canada, Ghana, Kenya and Malawi (Oxford: Hart Publishing, 2017) 139 [Koshan, "Judicial Treatment"].

41 See *R. v. Goldfinch*, 2019 SCC 38, 2019 CarswellAlta 1285, 2019 CarswellAlta 1286 (S.C.C.) at para. 33; *R. v. R.V.*, 2019 SCC 41, 2019 CarswellOnt 12413, 2019 CarswellOnt 12414 (S.C.C.) at para. 33.

42 Elizabeth Sheehy, "Evidence Law and Credibility Testing of Women: A Comment on the E Case" (2002) 2:2 Queensland U Technology L & Justice J 157 [Sheehy, "Credibility Testing"]; *R. v. G.F.*, 2021 SCC 20, 2021 CarswellOnt 6892, 2021 CarswellOnt 6893 (S.C.C.); Craig, "Trials on Trial", *supra* note 8; Ehrlich, *supra* note 39.

43 Craig, "Trials on Trial", *supra* note 8.

44 *Ibid.*

45 See Dodge, "Digital Witness", *supra* note 1; Dodge et al, *supra* note 5; Crystal Garcia, "Digital Photographic Evidence and the Adjudication of Domestic Violence Cases" (2003) 31:1 J Crim Justice 579; Powell, Stratton & Cameron, *supra* note 38.

46 Dodge, "Digital Witness", *supra* note 1.

47 Heather R Hlavka & Sameena Mulla, "'That's How She Talks': Animating Text Message Evidence in the Sexual Assault Trial" (2018) 52:2 Law & Soc'y Rev 401; Dodge,

standards that apply in relation to electronic documents.[48] Further, just as digital evidence can be used to assist the Crown in proving alleged offences committed against the complainant, digital evidence can be used to challenge the credibility and consistency of a complainant's evidence.[49] Crown counsel play a key role in ensuring a fair trial process, which includes preparing complainants for trial. However, as Elaine Craig notes in the context of sexual assault cases, many complainants are "woefully unprepared" for the trial process.[50] Crown counsel must prepare complainants to testify as to the accuracy of the digital evidence they tender at trial, including potentially explaining how the technology works or why they believe the accused is the author. In some cases, complainants will need to address accusations that they falsified information contained in the digital messages, or authored the messages themselves to set up the accused.

Defence theories that a complainant fabricated or manipulated digital evidence may prove particularly harmful in cases of GBV. Myths that women frequently lie about GBV remain prevalent within the legal system despite substantial feminist effort to combat these gendered stereotypes and research demonstrating that crimes like sexual assaults are significantly under-reported, and that false reports are relatively rare.[51] Historically, evidentiary rules allowed for the reinforcement of ideas that women frequently lied about sexual assault,[52] and that sexually active women were less worthy of belief.[53] Women's sexual

---

"Digital Witness", *supra* note 1; Alexa Dodge, "Digitizing Rape Culture: Online Sexual Violence and the Power of the Digital Photograph" (2016) 12:1 Crime Media Culture 65.

48 Paciocco, *supra* note 4.

49 See e.g. *R. v. Ghomeshi*, 2016 ONCJ 155, 2016 CarswellOnt 4246 (Ont. C.J.); *R. v. H.S.S.*, 2021 BCPC 90, 2021 CarswellBC 1118 (B.C. Prov. Ct.); *R. v. Jesso*, 2020 CarswellNfld 9 (N.L. Prov. Ct.).

50 Craig, "Trials on Trial", *supra* note 8 at 152.

51 David Lisak et al, "False Allegations of Sexual Assault: An Analysis of Ten Years of Reported Cases" (2010) 16:12 Violence Against Women 1318; Holly Johnson, "Why Doesn't She Just Report It? Apprehensions and Contradictions for Women Who Report Sexual Violence to the Police" (2017) 29:1 CJWL 36 [Johnson, "Why Doesn't She"]; Koshan, "Judicial Treatment", *supra* note 40; Holly Johnson & Myrna Dawson, "Intimate Partner Violence" in Holly Johnson & Myrna Dawson, eds, *Violence Against Women in Canada: Research & Policy Perspectives* (Oxford: Oxford University Press, 2011); Holly Johnson, "Limits of a Criminal Justice Response: Trends in Police and Court Processing of Sexual Assault" in Sheehy, "Sexual Assault", *supra* note 39 at 613 [Johnson, "Limits"]; Jennifer Koshan, "The Criminalisation of Marital Rape and Law Reform in Canada: A Modest Feminist Success Story in Combating Marital Rape Myths" in Randall, Koshan & Nyaundi, *supra* note 40 at 139; Ruthy Lowenstein Lazar, "The Vindictive Wife: The Credibility of Complainants in Cases of Wife Rape" (2015) 25 S Cal Rev L & Soc Justice 1; Karen Busby, "Every Breath You Take: Erotic Asphyxiation, Vengeful Wives, and Other Enduring Myths in Spousal Sexual Assault Prosecutions" (2012) 24:2 CJWL 328; Rosemary Hunter, "Narratives of Domestic Violence" (2006) 28 Sydney L Rev 733.

52 Lazar, *ibid.*; Busby, *ibid.*; Hunter, *ibid.*

53 Sheehy, "Credibility Testing", *supra,* note 42.

history and psychological background were used to undermine complainants' credibility at trial.[54] Efforts have been made to dispel rape myths from the criminal justice system, including limiting the use of sexual history and counselling records as evidence in cases of sexual assault.[55] Nevertheless, as demonstrated through Craig's research, harmful, sexist ideas about women continue to be relied on by certain defence counsel and other justice system actors, and these stereotypes cause unnecessary distress to many victims who have to respond to them on the stand.[56] These burdens are disproportionately borne by Indigenous women who are frequently targeted for sexual violence[57] and and who must confront systemic gendered racial discrimination.[58]

Reliance on sexist stereotypes in the legal system are not limited to sexual assault trials. In the domestic violence context, some defendants may attempt to undermine their credibility by characterizing their claims as fabricated, the idea being that complainants could be lying in order to gain an advantage in custody proceedings or punish their partners as a form of vengeance.[59] These issues make GBV trials notoriously demanding for complainants, and the criminal justice system has been widely critiqued for the systemic challenges victims face in seeking justice for the gender-based crimes committed against them.[60]

---

[54] Lise Gotell, "The Ideal Victim, the Hysterical Complainant, and the Disclosure of Confidential Records: The Implications of the *Charter* for Sexual Assault Law" (2002) 40 Osgoode Hall LJ 47; Lisa Dufraimont, "Myth, Inference and Evidence in Sexual Assault Trials" (2019) 44:2 Queen's LJ 316 [Dufraimont, "Myth, Inference and Evidence"]; Johnson, "Why Doesn't She", *supra* note 51; Melanie Randall, "Sexual Assault Law, Credibility, and 'Ideal Victims': Consent, Resistance, and Victim Blaming" (2010) 22:2 CJWL 397; Lise Gotell, "When Privacy is Not Enough: Sexual Assault Complainants, Sexual History Evidence and the Disclosure of Personal Records" (2006) 43 Alta L Rev 743.

[55] *Criminal Code,* RSC 1985, c C-46, ss 276, 278.1-278.92 [*Code*]; Elizabeth A Sheehy, "Rape Shield Laws: Canada" in Nicole Hahn Rafter, ed, *Encyclopedia of Women and Crime* (Phoenix: Oryx Press, 2000) 226.

[56] Craig, "Trials on Trial", *supra* note 8. See also Baker, Campbell & Straatman, *supra* note 39; Lindsay, *supra* note 39; Clark, *supra* note 39; Jo-Anne Wemmers, "Judging Victims: Restorative Choices for Victims of Sexual Violence" in Susan McDonald, ed, *Victims of Crime Research Digest 2017* (Ottawa: Department of Justice Canada, 2017); Jan Jordan, "The Long and Winding Road: Improving Police Responses to Women's Rape Allegations" in Holly Johnson, Bonnie S Fisher & Veronique Jaquier, eds, *Critical Issues on Violence against Women: International Perspectives and Promising Strategies* (New York: Routledge, 2015); Dufraimont, "Myth, Inference and Evidence", *supra* note 54; Johnson, "Why Doesn't She", *supra* note 51.

[57] Canada, Department of Justice, *JustFacts: Victimization of Indigenous Women and Girls* (Ottawa: Department of Justice, 2017); Loanna Heidinger, *Intimate Partner Violence: Experiences of First Nations, Métis and Inuit women in Canada, 2018* (Ottawa: Canadian Centre for Justice and Community Safety Statistics, 2021).

[58] National Inquiry into Missing and Murdered Indigenous Women and Girls, *supra* note 6.

[59] Lazar, *supra* note 52 at 9; Busby, *supra* note 52; Hunter, *supra* note 51.

[60] Craig, "Trials on Trial", *supra* note 8; Dufraimont, "Myth, Inference and Evidence",

The unique features of digital communications that make electronic messages vulnerable to manipulation and fabrication discussed in the first section of this paper, and the legacy of sexist myths that women frequently invent claims of sexual assault and intimate partner violence, combine to make digital evidence ripe territory for arguments by defence counsel that complainants authored or manipulated messages ostensibly sent by the accused. While in many cases alternative defence theories regarding authorship may be legitimate, there is a risk that baseless and speculative challenges to digital evidence in cases of GBV may improperly rely on sexist myths regarding false accusations and fabrication. In this way, digital evidence may become another area where victims of GBV must face unsubstantiated and harmful challenges to their experiences, which can be a distressing and re-traumatizing experience for many.

As noted in the previous section, demonstrating who authored relevant digital evidence may not be a straightforward process. As will be explored further throughout this paper, it is not uncommon for defence counsel to challenge the legitimacy of digital evidence or suggest someone else may have authored the messages in cases of GBV. Defence counsel may raise the possibility that someone else could have gained access to the accused's accounts or devices,[61] or they may suggest the victims themselves could have authored the messages to frame the accused or get revenge upon them.[62] In the remainder of the paper, we explore how authorship of digital evidence is being established and challenged in the GBV case law, from the investigatory to the trial stage. The cases discussed in the following sections represent a sample of recent Canadian criminal cases involving allegations of GBV in which concerns over the authorship of digital evidence were discussed. This is by no means a comprehensive sample of all cases meeting these criteria; rather, we selected these cases to demonstrate the varying approaches taken by judges in this developing area of law.

(c) Digital Evidence & Police Investigations of Gender-Based Violence

As sexual assault, intimate partner violence, and other forms of GBV frequently produce no or limited physical evidence, whatever evidence is available in these cases holds particular value. After reporting a complaint to the police, victims have relatively little influence on the manner in which police

---

supra note 54; Johnson, "Why Doesn't She", *supra* note 51; Koshan, "Judicial Treatment", *supra* note 40; Janine Benedet, "Judicial Misconduct in the Sexual Assault Trial" (2019) 52:1 UBC L Rev 1; Olivia Smith & Tina Skinner, "How Rape Myths are used and Challenged in Rape and Sexual Assault Trials" (2017) 26:4 Soc & Leg Stud 441.

[61] Steven M Cerny, "Discovery and Authentication of Social Media Evidence" (2011) 1:4 Reynolds Courts & Media LJ 479. See also *R. v. Moon*, 2016 ABPC 103, 2016 CarswellAlta 946 (Alta. Prov. Ct.) [*Moon*]; *R. v. MacDonald*, 2016 ABPC 142, 2016 CarswellAlta 1588 (Alta. Prov. Ct.) [*MacDonald*].

[62] See *R. v. S.S.*, 2018 ONSC 2299, 2018 CarswellOnt 5519 (Ont. S.C.J.) [*SS*]; *R. v. Lauck*, 2018 ABPC 260, 2018 CarswellAlta 2651 (Alta. Prov. Ct.) [*Lauck*]; *R. v. G.B.*, 2019 ONCJ 563, 2019 CarswellOnt 12997 (Ont. C.J.) [*GB*].

investigations and trials proceed, apart from providing evidence and testimony.[63] Victims rely on the police to determine if and how their complaints will be investigated.[64] Because digital evidence is easily deleted, accounts can be blocked, and digital devices are often lost or damaged,[65] it is critical that investigations involving digital evidence be managed swiftly and efficiently. As digital evidence becomes more prevalent in these cases, victims rely on police to ensure that such evidence is properly extracted, collected, and preserved. In some cases, the collection of digital evidence may be something that can only be undertaken with police assistance, such as requests to social media companies to access personal information associated with an account, or to fulfil a *Norwich* order to disclose the identity associated with an IP address from an internet service provider.[66]

While victims of GBV depend on police to conduct thorough investigations into their complaints, their faith that police will do so may be justifiably limited. Systemic bias in policing[67] has led to many cases of sexual violence being improperly labelled as unfounded, or being inadequately investigated.[68] Beliefs that women lie about sexual violence committed against them are deeply rooted in our society and the criminal justice system, and such beliefs have resulted in police taking limited investigatory steps when women report these crimes, and in legitimate complainants being dismissed altogether.[69] In her ground-breaking investigative journalism for the *Globe and Mail* in 2017, Robyn Doolittle found that one in every five sexual assault allegations in Canada is dismissed as baseless (and thus unfounded) by police officers, a rate significantly higher than most other crimes and one that does not match the statistics of false claims of sexual

---

63 Joanne C Minaker, "Evaluating Criminal Justice Responses to Intimate Abuse through the Lens of Women's Needs" (2001) 13 CJWL 74.

64 Cassia Spohn, Katharine Tellis & Eryn Nicole O'Neal, "Policing and Prosecuting Sexual Assault: Assessing the Pathways to Justice" in Johnson, Fisher & Jaquier, *supra* note 56.

65 Ramirez & Lane, *supra* note 20; danah boyd, "Social Network Sites as Networked Publics: Affordances, Dynamics, and Implications" in Zizi Papacharissi, ed, *The Networked Self: Identity, Community, and Culture on Social Network Sites* (New Haven, CT: Yale University Press, 2010).

66 See *Code, supra* note 55, ss 487.011-487.0199; Robert J Currie, "Cross-Border Evidence Gathering in Transnational Criminal Investigation: Is the *Microsoft Ireland* Case the 'Next Frontier'?" (2017) 54 Can YB Intl L 63.

67 Jodie Murphy-Oikonen et al, "Unfounded Sexual Assault: Women's Experiences Sexual Assault in Canada: Law, Legal Practice and Women's Activism of Not Being Believed by the Police" (2020) J Interpersonal Violence 1; Jordan, *supra* note 56; Johnson, "Limits", *supra* note 51.

68 Robyn Doolittle, *Had it Coming: What's Fair in the Age of #MeToo?* (Canada: Penguin Random House, 2019).

69 Jessica Shaw et al, "Beyond Surveys and Scales: How Rape Myths Manifest in Sexual Assault Police Records" (2017) 7:4 Psychology of Violence 602; Teresa Dubois, "How Far Have we Come Since Jane Doe?" in Sheehy, "Sexual Assault", *supra* note 39; Andrea Quinlan, "Suspect Survivors: Police Investigation Practices in Sexual Assault Cases in Ontario, Canada" (2016) 26 Women & Crim Justice 301.

violence.[70] Many police forces also have significant internal gender equity issues, as evidenced by recent class actions against the RCMP regarding the organization's failure to address allegations of sexual harassment and discrimination within the police force.[71] In cases involving digital evidence, if evidence is not collected in a timely manner, there is a significant risk that the evidence may not be available at all or will have been altered if collected at a date further into the future. If a case is unfairly classified as unfounded or not properly investigated due to sexist beliefs, digital evidence could be lost even if the case is later reopened or investigated at a later date.

When working with the police to collect digital evidence, victims face numerous challenges that can impact the results of the trial. Digital evidence can be difficult to preserve and capture. Social media platforms are not static, and relevant content may be deleted, altered, or unavailable in its original form by the time of the trial.[72] Victims may delete text threads, lose or break their devices, or get blocked from another user's account before realizing they needed to collect certain evidence they had not previously documented. Failing to collect relevant evidence early on can greatly impact the likelihood of their case being proven at trial if additional evidence such as the relevant conversation history, IP address, or other information linking the accused to an account has not been collected and is no longer available.

Presently, police forces are struggling to keep up with the new challenges posed by digital evidence in their investigations of GBV.[73] The influx of this evidence has created a demanding transition for police forces who are expected to stay on top of new and evolving investigatory techniques.[74] Alexa Dodge, Dale Spencer, Rose Ricciardelli, and Dale Ballucci report that digital evidence is now relied on in many, if not the majority, of sexual assault cases.[75] Their research shows that digital evidence can provide opportunities to help prove cases of GBV, but it also adds additional work for investigating officers, who need to know what digital evidence to collect and how to properly collect it. The large volume of evidence typically involved in digital evidence investigations and the

---

[70] Doolittle, "Why Police Dismiss", *supra* note 7. Following this report, over a 100 Canadian police services began reviewing their sexual assault cases in order to identify police bias and flaws in investigations, leading to hundreds of sexual assault cases being reclassified and reopened. See Robyn Doolittle, "The Unfounded Effect" *The Globe & Mail* (8 December 2017), online: <www.theglobeandmail.com/news/investigations/unfounded-37272-sexual-assault-cases-being-reviewed-402-unfounded-cases-reopened-so-far/article37245525/>.

[71] Deloitte, "RCMP Class Action Settlement" (2021), online: <www.classaction.deloitte.ca/en-ca/Pages/RCMPSettlement.aspx#head-Introduction>.

[72] Saunders, *supra* note 1.

[73] Dodge et al, *supra* note 5; Anastasia Powell & Nicola Henry, "Policing Technology-Facilitated Sexual Violence against Adult Victims: Police and Service Sector Perspectives" (2018) 28:3 Policing & Society 291.

[74] *Ibid.*

[75] Dodge et al, *supra* note 5.

novel investigatory skills required to adequately investigate this type of evidence mean that these investigations often require significant time and effort. The relevant investigatory skills are reportedly less common among average police officers, as there are limited officers with sufficient expertise on digital evidence collection practices.[76] The quantity of digital evidence also increases the amount of time police must spend on a case collecting evidence from digital devices, social media companies, and telecommunications providers. The officers interviewed by Dodge et al described "a need for new or modified forms of policing that respond to the influx of digital evidence."[77]

Even in circumstances where complainants' claims are swiftly investigated, and where police departments are equipped to handle the collection of digital evidence, there is currently a lack of clarity about what digital evidence must be collected and tendered at trial. Indeed, this uncertainty was evident in some of the GBV decisions we reviewed, as Facebook messages were ruled inadmissible in part because no investigation was undertaken by police to determine the account from which they were secured, and clear copies of the evidence were not made.[78] Judges were left with reasonable doubt as to the authorship of digital evidence due to police failures to search or properly extract data from relevant digital devices.[79] This risks creating unfairness for victims, who may have their digital evidence excluded or accorded little weight through no fault of their own.

Whatever digital evidence, including evidence of authorship, the police are able to collect, this evidence must be properly tendered by Crown counsel at trial and admitted by a judge and interpreted by the trier of fact. Further, the reliability of this evidence may be challenged by defence counsel, who may assert the Crown has not proven that the accused authored the relevant messages. In the following sections, we explore the approach being taken by criminal courts in Canada to authorship disputes in relation to threshold admissibility, admissibility as hearsay, and at trial in cases of GBV.

(d) Admissibility of Digital Evidence in the Gender-Based Violence Case Law

(i) Admissibility Under the Canada Evidence Act

The earliest stage at which authorship of digital messages was contested in the cases we reviewed was in relation to threshold admissibility. The admissibility of electronic evidence at trial is governed by the *CEA,* sections 31.3-31.8.[80] Despite the applicability of the *CEA* to all electronic documents, lawyers and judges do not always explicitly consider or apply this legislation in cases where

---

[76] *Ibid.* at 504.

[77] *Ibid.*

[78] *R. v. Donaldson*, 2016 CarswellOnt 21760, [2016] O.J. No. 7153 (Ont. C.J.) at para. 5.

[79] *SS, supra* note 62 at paras 104-105, 112; *R. v. Aslami*, 2021 ONCA 249, 2021 CarswellOnt 5561 (Ont. C.A.) [*Aslami* 2021] at para. 20.

[80] *CEA, supra* note 37.

parties seek to admit digital evidence.[81] This has resulted in inconsistency in the application of admissibility standards for social media evidence.[82] Judges in some of the cases we examined criticized counsel's failure to refer to *CEA* provisions when making submissions regarding electronic document admissibility.[83] Indeed, in a number of cases it appears trial judges themselves may have been unaware of the applicability of these provisions, as the *CEA* requirements were only discussed on appeal.[84]

Pursuant to the *CEA,* "electronic documents," which can include emails,[85] text messages,[86] social media content,[87] and audio-visual material[88] must meet the tests of authenticity and the best evidence rule in order to be admissible at trial. As per section 31.1 of the *CEA,* the party tendering the document must prove its authenticity "by evidence capable of supporting a finding that the electronic document is that which it is purported to be"[89] Authentication requires "convincing a court that a thing matches the claim made about it" and is connected to the evidence's relevance.[90] As noted by Graham Underwood and Jonathan Penner, proof of authenticity and reliability is not concerned with the substantive content of an electronic document, but where the document "comes from, how it was obtained and handled, whether it can be trusted to be what it purports to be, and how reliable a source of information it is about a material issue."[91]

The threshold for establishing authenticity of an electronic document under the *CEA* is low,[92] requiring only "some evidence that is logically probative of whether the electronic document is what it purports to be."[93] This evidence may

---

81 Silver, *supra* note 1.

82 Silver, *supra* note 1; Paciocco, *supra* note 4.

83 In *Donaldson,* for example, Paciocco J noted that neither counsel had referred to the *CEA* at trial, and while it was "not the first time [he had] encountered counsel who are unfamiliar with these provisions," it was incumbent on counsel to familiarize themselves with the *CEA* admissibility requirements (*Donaldson*, *supra* note 78 at para 3).

84 See *R. v. Hirsch*, 2017 SKCA 14, 2017 CarswellSask 77 (Sask. C.A.) [*Hirsch*]; *R. v. Durocher*, 2019 SKCA 97, 2019 CarswellSask 480 (Sask. C.A.) [*Durocher*]; *CB, supra* note 17.

85 *CB, supra* note 17 at para 57.

86 *Ibid.*

87 *Ball, supra* note 15 at para 67; *Durocher, supra* note 84 at para 80.

88 Chan & Lai, *supra* note 2.

89 *CEA, supra* note 37, s 31.1.

90 *CB, supra* note 17 at para 65, cited in *Martin, supra* note 17 at para 33.

91 Graham Underwood & Jonathan Penner, *Electronic Evidence in Canada* (Thomson Reuters, 2020) (loose-leaf) at 11-11.

92 See *Martin, supra* note 17; *Ball, supra* note 15*; CB, supra* note 17 at para 57*; Hirsch, supra* note 84 at para 18; *R. v. Kalai*, 2020 NSSC 351, 2020 CarswellNS 774 (N.S. S.C.) at para. 27.

93 *Martin, supra* note 17 at para 47.

be direct or circumstantial.[94] Evidence can be authenticated even where the Crown and defence positions differ as to whether it is genuine or not.[95] As noted by the Court in *Hirsch*, the "integrity (or reliability) of the electronic document is not open to attack at the authentication stage of the inquiry."[96]

Authentication under the *CEA,* as at common law, requires consideration of the purpose for which the evidence is being presented.[97] In some earlier cases, the *CEA*'s authentication requirement was interpreted as requiring proof of authorship — if the Crown's theory was that messages originated from the accused, what must be authenticated is "an evidentiary foundation upon which it could be reasonably inferred that the messages were sent" by the accused.[98] However, recent appellate jurisprudence indicates that proof of authorship will *not* be required to authenticate electronic documents.[99] While demonstrating authorship, something that will assist in assessing ultimate guilt or innocence, will be sufficient to establish authenticity, establishing authenticity will not necessarily be sufficient to establish authorship.[100] As the Newfoundland and Labrador Court of Appeal recently noted in *R. v. Martin,* concerns over authorship "might impact other evidentiary principles, such as the relevance, reliability and ultimate weight to be afforded to the evidence" but do not impact the applicability of the relevant admissibility considerations.[101] In *CB,* the Ontario Court of Appeal found that it is reasonable to infer at the authentication stage that a sender has authored a message sent from their number, even if there were an air of reality to a claim that this may not be so, as the low threshold for admissibility "would seem to assign such a prospect to an assessment of weight."[102] In that case, authenticity was established by virtue of the complainant acknowledging certain text messages were sent and received by her cell phone number.[103]

Circumstantial evidence was frequently sufficient to establish authenticity in the GBV case law we examined. This was true even in those cases where authenticity and authorship appeared to be conflated.[104] Relevant evidence relied

---

94 *CB, supra* note 17 at para 68; *Martin, supra* note 17 at para 34; *Hirsch, supra* note 84 at para 18; *R. v. Colosie*, 2016 ONSC 1708, 2016 CarswellOnt 21889 (Ont. S.C.J.) at para. 25 [*Colosie*].

95 Paciocco, *supra* note 4 at 197; *Martin, supra* note 17 at para 49.

96 *Hirsch, supra* note 84 para 18.

97 *Donaldson, supra* note 78 at 3; *Martin, supra* note 17 at para 89; *Durocher, supra* note 84 at para 81.

98 *Donaldson, supra* note 78 at 3-4. See also *Hirsch, supra* note 84 at paras 19-21, 29.

99 *Durocher, supra* note 84 at para 85*; Martin, supra* note 17 at para 73; *CB, supra* note 17 at paras 68, 72.

100 Underwood & Penner, *supra* note 91 at 13-11, cited in *Durocher, supra* note 84 at para 85.

101 *Martin, supra* note 17 at para 73.

102 *CB, supra* note 17 at paras 70, 72.

103 *Ibid.* at para 44.

on to establish authenticity in the GBV case law included complainant testimony that they recognize and can identify the electronic document,[105] testimony of the complainant or another witness about how the document was created,[106] evidence the complainant received previous communications from the contested account,[107] the messages or posts appearing to be from an account associated with the accused's name,[108] a reply to a message from the complainant,[109] consistency between the contents of the messages and the relevant events occurring at that time,[110] and consistency between the messages and how the accused communicates in person or on other platforms.[111] While expert testimony can bolster claims of authenticity, it is not necessary to meet the low threshold under the *CEA*.[112]

For the second step under the *CEA* admissibility requirements, the party seeking to admit the electronic document must prove that it satisfies the "best evidence" rule.[113] This rule is intended to ensure an electronic document accurately reflects the original information input into a digital device by the author.[114] Parties can satisfy the best evidence rule under the *CEA* by proving the integrity of the relevant electronic documents system on a balance of probabilities[115] or through reliance on a rebuttable statutory presumption of integrity under the *CEA*.[116] As Lisa Dufraimont notes in her case commentary on *Martin,* the presumption of system integrity may be relied on, in the absence of evidence to the contrary, wherever the electronic document is legible and coherent.[117] Witness testimony about the functioning of a device and coherent,

---

[104] See e.g. *Hirsch, supra* note 84 at para 21.

[105] *Hirsch, supra* note 84 at para 19; *Colosie, supra* note 94 at para 17; *Durocher, supra* note 84 at para 92; *GB, supra* note 62 at paras 39-40, 141; *R. v. Himes*, 2016 ONSC 249, 2016 CarswellOnt 238 (Ont. S.C.J.) at para. 48 [*Himes*]; *R. v. Phagura*, 2018 BCSC 2541, 2018 CarswellBC 4080 (B.C. S.C.) at para. 17 [*Phagura*].

[106] *Himes, supra* note 105 at para 48; *Phagura, supra* note 105 at para 16; *R. c. Soh*, 2014 NBQB 20, 2014 CarswellNB 69, 2014 CarswellNB 70 (N.B. Q.B.) [*Soh*] at para. 27.

[107] *Durocher, supra* note 84 at para 92; *Phagura, supra* note 105 at para 17; *Soh, supra* note 106 at para 27.

[108] *Hirsch, supra* note 84 at para 19; *CB, supra* note 17 at para 76; *Durocher, supra* note 84 at para 92; *GB, supra* note 62 at paras 42, 141.

[109] *Colosie, supra* note 94 at para 25; *Durocher, supra* note 84 at para 92.

[110] *CB, supra* note 17 at para 76; *Durocher, supra* note 84 at para 92.

[111] *Hirsch, supra* note 84 at paras 19, 20; *CB, supra* note 17 at para 69; *Durocher, supra* note 84 at para 92.

[112] See *CB, supra* note 17 at para 77.

[113] *CEA, supra* note 37, s 31.2.

[114] Paciocco, *supra* note 4 at 200; *GB, supra* note 62 at para 73;

[115] *R. v. J.V.*, 2015 ONCJ 837, 2015 CarswellOnt 21031 (Ont. C.J.) at para. 21 [*JV*]; Nader Hasan, "No Progress Without Proof: Authenticating Electronic Evidence in the Digital Age" (2020) 40:3 For the Defence: The Criminal Lawyers' Association Newsletter.

[116] *CEA, supra* note 37, s 31.3.

contextually consistent conversations involving that device at the relevant time can constitute evidence capable of supporting a finding that a device was working properly at all material times.[118] In *R. v. Moon*, for example, the best evidence rule was satisfied when the complainant testified that the phone on which she received messages was working normally, she had purchased the phone herself, and she had received the messages in question in the normal fashion as she usually did.[119] If a novel program is used or if a presumption is disputed, evidence beyond the testimony of the complainant, such as an affidavit or testimony from the technology company itself, may be required to explain how the technology works.[120] If there is any doubt that the program being used to capture the digital evidence is not a well-known program, the Crown will want to consider what evidence will be needed to explain the functionality of the technology beyond the basic knowledge of the complainant.

The Supreme Court of Canada in *Martin* recently characterized the admissibility requirements under the *CEA* as serving as a "generous gateway for a common form of communication in our current society" while also serving to "provide some degree of quality control."[121] As noted by Dufraimont, the low threshold for admissibility under the *CEA* means that trial judges are safer to err on the side of admission, and leave the resolution of any doubts regarding the content of electronic evidence to an assessment of weight at the end of trial.[122] This may be true even if there is evidence providing an air of reality to claims of tampering or impersonation in relation to the document.[123] Thus claims by defence counsel that someone else could have authored an electronic document will generally be insufficient to prevent threshold authentication under the *CEA*. Those arguments are to be addressed at a later stage in the admissibility process or at trial by the triers of fact in determining weight.[124]

Dufraimont notes that the *CEA* authentication and best evidence requirements will seemingly be met "whenever police receive from an anonymous source a coherent document that looks like a Facebook post labelled with the accused's name and/or photo."[125] Some have argued that the threshold for admissibility under the *CEA* has been interpreted as being so low

---

[117] Lisa Dufraimont, "*R v. Martin,* 2021 N.L.C.A. 1 Case Comment", 69 CR (7th) 301 [Dufraimont, "Case Comment"], citing *Martin, supra* note 17 at para 71.

[118] *R. v. S.H.*, 2019 ONCA 669, 2019 CarswellOnt 14110 (Ont. C.A.) at 10,[[author please check: Unsure if this is pinpoint cite or not, flagged it for your review.]] affirmed 2020 SCC 3, 2020 CarswellOnt 2380, 2020 CarswellOnt 2381 (S.C.C.) [*SH*]

[119] *Moon, supra* note 61.

[120] *R. v. Nardi*, 2012 BCPC 318, 2012 CarswellBC 2801 (B.C. Prov. Ct.).

[121] *Martin, supra* note 17 at para 4, citing *Donaldson, supra* note 78.

[122] Dufraimont, "Case Comment", *supra* note 117. See also Paciocco, *supra* note 4 at 197.

[123] *CB, supra* note 17 at paras 71-72.

[124] Dufraimont, "Case Comment" *supra* note 117; *CB, ibid* at para 72; *R. v. Sandham*, 2009 CarswellOnt 6608, [2009] O.J. No. 4527 (Ont. S.C.J.) at para. 16.

[125] Dufraimont, "Case Comment" *supra* note 117.

that in order to preserve trial fairness, it may need to be adjusted or buttressed by other factors, such as through the engagement of the trier of fact's gatekeeping function. Judges have the discretion to exclude technically relevant evidence where the prejudicial effect of a piece of evidence outweighs its probative value.[126] Silver argues that, to ensure trial fairness, there should be stronger considerations regarding the accuracy of digital evidence at the authentication stage and a more robust use of the trier of fact's discretionary gatekeeper role when deciding whether to include or exclude digital evidence.[127] Her concerns stem from the fact that social media is dynamic and can be manipulated in ways that are different from other forms of evidence. Engaging the gatekeeper function of the judge to address reliability issues and balance the potential prejudicial effect of admission with the evidence's probative value could help mitigate any concerns about admitting questionable electronic evidence.

Ultimately, recent appellate jurisprudence appears to indicate that authorship and authentication are distinct issues, and that the *CEA*'s authentication and best evidence requirements represent a very low bar to admissibility. That being said, the conflation of authorship and authenticity in many cases makes it difficult to predict what types of digital evidence will be admitted in a given trial setting. Indeed, the recent Ontario Court of Appeal decision *R. v. Aslami*,[128] discussed further below, indicates that expert evidence regarding the functionality of digital messaging applications will be necessary in some cases, but it does not explicitly state whether such evidence is necessary for threshold admissibility, proof of identity, or both. As the standard for admissibility under the *CEA* appears to be contested and developing, Crown counsel should not assume that a copy of a digital message and the complainant's testimony that they received it on a functioning digital device will always be sufficient to have that evidence admitted.

Once the *CEA* requirements of authenticity and the best evidence rule are met, ultimate admissibility still requires that a document be legally relevant (involving a consideration of the purpose for which the evidence is being tendered) and consideration of any related general evidence rules.[129] Once a document is admitted, the final determination of authorship and the weight given to digital evidence will be determined by the trier of fact. The next two sections outline the approach being taken by criminal courts to authorship in relation to having electronic documents admitted as exceptions to the rule against hearsay, and to establishing identity at trial.

---

[126] Paciocco, Paciocco & Stuesser, *supra* note 14 at 47-53; Paciocco, *supra* note 4 at 219.

[127] Silver, *supra* note 1.

[128] *Aslami* 2021, *supra* note 79.

[129] *Ball, supra* note 15 at para 68; Paciocco, *supra* note 4 at 193.

(ii) Admissibility as Hearsay

When an electronic document meets the requirements of authenticity and the best evidence rule under the *CEA,* this means that this evidence may be admitted, not that it will ultimately be admitted.[130] As discussed by Nader Hasan, it is important to remember that authenticity does not equal admissibility.[131] Standard evidentiary rules still apply, and the contents of the document may raise admissibility issues.[132] Courts must consider the application of exclusionary rules and any relevant exceptions to those rules, as well as the exercise of the judge's exclusionary discretion.[133]

In the cases we examined, questions of admissibility frequently arose in relation to digital evidence that purportedly included statements by the accused, as such out-of-court statements constitute hearsay if the messages are being admitted for the truth of their contents.[134] While hearsay evidence is presumptively inadmissible, it may be admitted if it falls within a traditional exception to hearsay.[135] An accused's digital communications can be admitted pursuant to the "admission exception" to the rule against hearsay if the Crown can prove on a balance of probabilities that the accused authored the message.[136] Additionally, it can be admitted pursuant to the "principled approach," provided it meets the requirements of necessity and reliability.[137]

In order to be admissible as an exception to the rule against hearsay, the Crown must establish on a balance of probabilities that the statement is attributable to the accused. The balance of probabilities standard can be met in relation to authorship on evidence such as "the source of the information, access to the relevant email or social media address, the disclosure of details known to the purported author, and the nature of the exchanges between the parties, particularly where the exchanges relate to matters shared between the parties."[138] As with evidence admitted pursuant to the *CEA*, once the admission is accepted as evidence, the trier of fact must still determine whether the Crown has

---

[130] Hasan, *supra* note 115; Paciocco, *supra* note 4 at 193.

[131] Hasan, *supra* note 115.

[132] *SH, supra* note 118.

[133] Paciocco, *supra* note 4 at 219-220; Paciocco, Paciocco & Stuesser, *supra* note 14 at 47-53.

[134] Paciocco, Paciocco & Stuesser, *supra* note 14 at 135. There is some debate about whether admissions are an exception to the hearsay rule, or are simply admissible evidence because the accused is available to be a witness at the trial and has the opportunity to take the stand to contest this evidence (See *Durocher, supra* note 84 at para 63-64).

[135] Paciocco, Paciocco & Stuesser, *supra* note 14 at 151-232.

[136] *R. v. Evans*, 1993 CarswellAlta 111, 1993 CarswellAlta 567, [1993] 3 S.C.R. 653 (S.C.C.) at para. 32; Paciocco, Paciocco & Stuesser, *ibid.* at 193.

[137] *R. v. Khan*, 1990 CarswellOnt 108, 1990 CarswellOnt 1001, [1990] 2 S.C.R. 531 (S.C.C.); *R. v. Starr*, 2000 SCC 40, 2000 CarswellMan 449, 2000 CarswellMan 450 (S.C.C.) [*Starr*]; *R. v. Khelawon*, 2006 SCC 57, 2006 CarswellOnt 7825, 2006 CarswellOnt 7826 (S.C.C.); Paciocco, Paciocco & Stuesser, *supra* note 14 at 151-173.

[138] *JV, supra* note 115 at para 3

proven guilt beyond a reasonable doubt, which may include a determination that the accused did in fact author the admissions.[139]

In four sexual assault cases we examined, the Crown sought to admit electronic conversations between the accused and the complainant as evidence containing admissions by the accused.[140] In these cases, the Crown was able to establish on a balance of probabilities that the accused authored the messages, and evidence related to the content of the messages and the history of communication between the accused and the complainant was useful in proving authorship. Information linking the phone number to the accused was also helpful in two of these cases.[141]

In *R. c. Soh*, the contested messages were allegedly exchanged between the complainant and the accused on Facebook, and the defence highlighted that the Crown had not led any evidence from Facebook regarding the details of the account, such as the username or IP address, or linked any such information to the accused.[142] The judge noted that while the IP address linking a Facebook page to a particular individual would have be useful evidence, obtaining that information would require an order that the provider disclose this information, which is not absolutely necessary to prove the user's identity in every case.[143] In *Soh*, circumstantial evidence, including the accused's use of a nickname that only he called the complainant and discussions of details of the alleged sexual assault only he could know, were sufficient to establish authorship on a balance of probabilities in order for the evidence to be admitted as an exception to the rule against hearsay.

In *Moon,* the complainant and accused also knew each other personally and had a long history of text and phone communication through the telephone number associated with the alleged admissions. Despite the defence arguing the accused's wife could have authored the messages because she also had access to his phone, the timing and details of the texts led the judge to conclude on a balance of probabilities that the accused authored the texts about the alleged sexual assault.[144] Likewise in *R. v. Phagura*, a record of ongoing communication between the accused and complainant on WhatsApp helped associate the admissions with the accused.[145] In that case, the only evidence relied on by the judge in determining the accused was the author of the messages was the fact that the complainant identified the messages as coming from WhatsApp, where she

---

[139] *R. v. Teerhuis-Moar*, 2009 MBQB 22, 2009 CarswellMan 28 (Man. Q.B.); *Soh, supra* note 106 at para 40.

[140] *Moon, supra* note 61; *Phagura, supra* note 105; *Soh, supra* note 106; *Macdonald, supra* note 61.

[141] *Moon, supra* note 61 at paras 72-81; *Phagura, supra* note 105 at para 27.

[142] *Soh, supra* note 106.

[143] *Ibid.* at para 36.

[144] *Moon, supra* note 61 at paras 72-81.

[145] *Phagura, supra* note 105 at para 27.

had saved the accused as a contact, and subsequently received messages from that contact.[146]

In *R. v. MacDonald,* the defence suggested that incriminating Facebook messages could have been sent to the 15-year-old complainant by another individual impersonating the accused; however, the judge found it was speculative to suggest another person would gain unauthorized access to the accused's account days after the event to apologize and inquire about further sexual activity. The messages came quickly and regularly from the sender's account, suggesting it was not an imposter unfamiliar with the incident, and contained details about the encounter that would not be easily known by anyone beyond the accused and the complainant.[147]

The cases described above indicate that witness testimony and circumstantial evidence can be sufficient to establish authorship on a balance of probabilities in relation to digital hearsay evidence. A previous history of communications between the complainant and accused may be relevant in establishing authorship, but a lengthy correspondence is not required. In *Phagura,* only two days of messages were entered into evidence (it is unclear if this was the extent of the accused and complainant's correspondence), while in *MacDonald* the accused and complainant only began exchanging messages after the alleged assault. A longer messaging history may be even more useful, as it may include personal details about the parties that indicate the accused is in fact the sender. Further, while evidence linking an accused to the account from which the messages originated (rather than linking an accused to the content of the messages) may be helpful, such evidence was not always required. Thus, in order for digital communications purportedly authored by the accused to be admitted under the *CEA* and as an exception to the hearsay rule, evidence originating from the complainant's testimony has in many cases been sufficient. Whether or not this evidence will be sufficient to establish authorship beyond a reasonable doubt has been the subject of varying interpretations in the case law.

(e) Proving Authorship of Digital Evidence at the Gender-Based Violence Trial

As noted previously, identity is an essential element of any criminal offence and must be proven beyond a reasonable doubt.[148] In accordance with an accused's presumption of innocence, the Crown bears the burden of proving the accused is the guilty party, and the accused is never required to prove their innocence.[149] Unlike other essential elements, identity need not be proved through direct evidence, and circumstantial evidence may be sufficient to

---

[146] *Ibid.* at para 27.

[147] *Macdonald, supra* note 61 at para 25.

[148] *R. v. Grant*, 2015 SCC 9, 2015 CarswellMan 89, 2015 CarswellMan 90 (S.C.C.) at para. 3 [*Grant*].

[149] *Ibid.*

establish identity.[150] Where electronic communications are relied on to establish identity, the Crown must prove the accused authored the messages.[151] In many cases, defence counsel will lead evidence to counter the Crown's theory that the accused was the author of impugned messages. While a number of the cases we reviewed involved only witness testimony and circumstantial evidence sufficient to prove the identity of the author of digital messages beyond a reasonable doubt, recent appellate case law indicates additional evidence will be necessary in some circumstances. Precisely what circumstances will require further evidence is not entirely clear, leading to potential confusion for victims, police, lawyers, and judges.

Witness testimony coupled with circumstantial evidence was held to be sufficient to prove authorship beyond a reasonable doubt in a number of the GBV cases we reviewed. This evidence was similar to that relied on to establish threshold admissibility and in the hearsay cases discussed above and included the accused's name being associated with an online account,[152] the timing of the messages,[153] possible motives of the accused,[154] images of the accused or of things associated with him (*i.e.*, his children, animals, vehicles),[155] similarity in user names between messages or with information relating to the accused,[156] personal information about the parties in the content of the messages,[157] and similarities in the language or ways of communicating between disputed and undisputed messages.[158]

While the complainant's testimony and circumstantial evidence alone were sufficient to establish authorship in some cases, in others the circumstantial evidence tendered by the Crown was insufficient to establish authorship beyond a reasonable doubt. In *R. v. Himes*, the accused had been convicted at trial of child luring in relation to two 14-year-old girls.[159] On appeal, the defence successfully argued that the trial judge erred in finding identity had been proved beyond a reasonable doubt in relation to the second complainant. The inculpatory text messages purportedly sent to this complainant had not been

---

[150] *R. v. Eckstein*, 2012 MBCA 96, 2012 CarswellMan 587 (Man. C.A.) at para. 27.

[151] *Harris, supra* note 36.

[152] *Himes, supra* note 105.

[153] *Macdonald, supra* note 61 at para 25; *R. v. Proctor*, 2019 QCCQ 5608, 2019 CarswellQue 8475 (C.Q.) at para. 139 [*Proctor*].

[154] *Lauck, supra* note 62; *R. v. M.R.*, 2017 ONCJ 558, 2017 CarswellOnt 12537 (Ont. C.J.) [*MR*].

[155] *Macdonald, supra* note 61; *Hirsch, supra* note 84 at para 26.

[156] *Colosie, supra* note 94 at para 20; *Proctor, supra* note 153 at para 139.

[157] *Harris, supra* note 36; *Hirsch, supra* note 84 at para 26; *Macdonald, supra* note 61 at para 25.

[158] *Hirsch, supra* note 84 at para 26; *Proctor, supra* note 154 at para 139; *Lauck, supra* note 62 at para 138.

[159] *Himes, supra* note 105.

placed before the court, as her phone had been stolen prior to her reporting the incident to police. This complainant testified that she received texts from an unknown telephone number she believed was linked to the accused, and when neither the Crown nor defence pushed the issue of identity further, the trial judge intervened and asked the complainant how she knew it was the accused's number. She responded that she had asked him his name, and he had told her.[160] The judge on appeal found this to be a leading question on a crucial issue, which constituted a palpable and overriding error.

In *R. v. Pogoryelov,* there was no evidence directly linking the accused to text messages arranging a sexual encounter with a police officer who he believed to be a 14-year-old girl.[161] The judge found that the circumstantial evidence of the accused appearing at the specified hotel room door at the time arranged in the text messages, carrying the agreed-upon amount of cash, and the cellphone that sent the messages being located in a nearby car containing the accused's I.D., were insufficient to establish guilt. The defence did not explicitly raise any theory of who an alternative sender could be; however, the judge relied on the Supreme Court of Canada's decision in *R. v. Villaroman* in acquitting the accused.[162] In *Villaroman,* the Court clarified that when a case turns on circumstantial evidence, judges are required to consider other plausible theories and reasonable possibilities inconsistent with guilt, so long as these are based on logic and experience, rather than speculation.[163] The Crown may be required to negative reasonable possibilities, but it is established law that the Crown does not need to "negative every possible conjecture, no matter how irrational or fanciful, which might be consistent with the innocence of the accused."[164] The judge in *Pogoryelov* found that the evidence as a whole left open reasonable inferences other than guilt that were not purely speculative.[165]

The above outcome can be contrasted to *R. v. Chheda,* in which the accused was convicted of child luring in similar circumstances, after arriving at the agreed-upon hotel room at the prearranged time, holding two hot chocolates and the precise amount of cash the undercover officer had asked him to bring via text-message. While the police searched the accused's car in the parking lot and did not locate the phone used to send the text messages to the undercover officer, they did locate another cell phone in that car. Representatives from Rogers and Freedom Mobile gave testimony regarding the records of the two phones, which demonstrated they travelled to the same locations on the relevant date. This,

---

[160] *Ibid.* at para 55.

[161] *R. v. Pogoryelov*, 2019 ONCJ 701, 2019 CarswellOnt 16386 (Ont. C.J.) [*Pogoryelov*].

[162] *R. v. Villaroman*, 2016 SCC 33, 2016 CarswellAlta 1411, 2016 CarswellAlta 1412 (S.C.C.) [*Villaroman*].

[163] *Ibid.* at para 37.

[164] *R. v. Bagshaw*, 1971 CarswellOnt 159F, 1971 CarswellOnt 159, [1972] S.C.R. 2 (S.C.C.) at 8 [S.C.R.], cited in *ibid* at para 37; *R. v. Paul*, 1975 CarswellQue 42F, 1975 CarswellQue 16, [1977] 1 S.C.R. 181 (S.C.C.) at 191 [S.C.R.].

[165] *Pogoryelov, supra* note 161 at para 20.

combined with the circumstantial evidence of the accused arriving at the prearranged location carrying specific items, was found to prove the accused was the sender of the text messages.[166] Thus, additional forensic evidence regarding the location or account details of a communications device may be necessary to prove identity beyond a reasonable doubt in some cases.

In four cases we reviewed, defence counsel raised the possibility that a third party may have written messages incriminating the accused. In *R. v. Harris,* forensic evidence from the accused's hard drive, as well as circumstantial evidence, was relied on to prove that sexual Facebook messages to an underage complainant who was a personal acquaintance of the accused originated from his account.[167] The judge noted that it defied logic and common sense that another individual would use the accused's account to set up a sexual encounter with the complainant, as the plan would fall apart when she attended the meeting and did not recognize the author.[168] In *R. v. M.R.,* defence counsel put forward a theory that an anonymous hacker may have authored an email containing the complainant's intimate images, a theory which the judge found to be "devoid of any realistic foundation."[169] The judge found the circumstantial evidence left him with no reasonable doubt that the accused distributed the photos, as the accused was the only person to whom complainant had sent the images, he had access to her Facebook account, and the emails were sent to people close to the complainant rather than random individuals or all of the complainant's contacts.[170]

In *R. v. Proctor,* the defence argued that unknown clients of the complainant, who worked as an escort, could have made harassing phone calls and authored anonymous harassing text messages.[171] In rejecting those arguments, the judge noted the accused's consistent use of the term "goof" in his messages to the

---

[166] See also *R. v. Sanchez*, 2012 BCCA 469, 2012 CarswellBC 3643 (B.C. C.A.) at para. 45, in which the accused showing up to the police station at a time arranged over the phone using a certain phone number was considered strong circumstantial evidence that the accused used that same phone number to send text messages and make calls to his ex-wife.

[167] *Harris, supra* note 36.

[168] *Ibid.* at para 29.

[169] *MR, supra* note 154 at paras 146-47. In that case, the accused had gone to the additional work of sending anonymous emails to the complainant's academic advisor indicating that her account had been hacked, as well as informing the complainant her intimate images had been posted on Reddit, in order to lend credibility to the anonymous hacker theory.

[170] *Ibid.* Additional evidence in this case which the judge found to be the "most probative" included a series of text messages sent by the accused after the images were distributed demonstrating "he possessed peculiar information concerning the timing and content of the dissemination of emails" (at para 124). We note however that this did not appear to reveal specialized knowledge outside of what the accused would have discovered as a recipient of the email, if it had in fact been distributed by an anonymous hacker.

[171] *Proctor, supra* note 153.

complainant and in fake profiles used to harass the complainant,[172] as well as consistent spelling errors, expressions, and themes in the messages, to determine the accused authored all of the relevant messages.[173] Finally, in *R. v. Careen,* the defence argued that another person or persons could have authored incriminating text messages allegedly sent by the accused teacher to one of his female students, as the accused's phone was frequently left sitting out in the accused's home and borrowed by other individuals at his workplace. The judge noted the proximity in timing between the messages the accused admitted authoring and those he contested,[174] and he identified the accused's consistent use of exclamation points and the phrase "ha ha" between contested and uncontested messages, which he understood to indicate the accused was the author of the messages.[175] The judge found the inference that someone would take control of the accused's phone at multiple points in time to impersonate his "very distinctive style of text communication" was implausible and lacked a conceivable rational motive.[176]

In five cases we examined, defence counsel raised the possibility that the complainant herself may have authored the incriminating messages in order to frame the accused. In *R. v. G.B.,* the defence argued that the complainant had forged text messages and images of injuries following an alleged sexual assault, but the trial judge did not accept these arguments on the basis there "were and still are too many ways and means to expose such a hoax for that contention to be credible."[177] In *R. v. Lauck,* the defence raised the possibility the complainant may have authored the numerous harassing pseudonymous Facebook messages she received in order to make the accused look bad in a custody dispute over their daughter.[178] Following inconsistent evidence from the accused about his knowledge of and access to digital accounts, and after examining the content of the messages, the judge framed the relevant question not as whether it was possible that someone else sent the impugned messages, but how likely it was that someone else did.[179] The judge did not find it likely that the complainant would use pseudonymous accounts if she wanted to frame the accused, nor would she call herself sexist and degrading names in group chats with mutual acquaintances.[180] Circumstantial evidence including consistency in contents of

---

[172] *Ibid.* at paras 133-35.

[173] *Ibid.* at paras 138-39.

[174] *R. v. Careen*, 2011 BCSC 1833, 2011 CarswellBC 3744 (B.C. S.C.) at paras. 179-181, 224, affirmed 2013 CarswellBC 3723 (B.C. C.A.) [*Careen*].

[175] *Ibid.* at paras 29, 176, 222.

[176] *Ibid.* at paras 167-68.

[177] *GB, supra* note 62 at para 111. The accused was nevertheless acquitted based in part on deficiencies in the electronic evidence.

[178] *Lauck, supra* note 62.

[179] *Ibid.* at para 121.

[180] *Ibid.* at paras 135-41.

the messages with the way the accused spoke, such as the use of particular words and phrases, led the judge to conclude that the only rational inference to be drawn from the evidence was that the accused authored the messages.[181]

In *R. v. Owens*, the defence relied on the complainant's expertise in computers and apparent motivation of obtaining leverage to get the house in separation proceedings from the accused in support of a theory that the complainant manufactured harassing emails she received.[182] The trial judge rejected the defence theory that it was the complainant who wrote these emails, noting a "striking similarity" between an email the accused admitted having sent and the four contested emails was the "unusual use of capital letters," as well as the theme of forgiveness in two of the emails.[183] The judge found this similarity suggested either that the defendant wrote all of the emails or "that the complainant was careful to replicate a theme and grammatical style associated with the defendant in an email sent by him months earlier."[184] The judge found the contents of the emails too subtle, noting that if the complainant had fabricated them to frame the accused, they would have been more explicitly harassing.[185] As in *Lauck,* the judge found the complainant would logically have sent the messages under the accused's name if she were attempting to frame him.[186] Further, in this case there was additional evidence of the emails being sent from IP addresses associated with physical addresses linked to the accused.[187]

While many judges rejected claims the complainant fabricated abusive messages as far-fetched or speculative, these claims were successful in contributing to a reasonable doubt in at least one decision. In *R. v. S.S.,*[188] a case involving allegations of extortion and the non-consensual disclosure of intimate images, there was a wealth of digital evidence before the court, including over 550 pages of online communications ostensibly between the accused and complainant. The defence submitted that in some of the online exchanges the complainant may have authored the accused's side of their conversations by logging into his account, asserting that she had done this to a former boyfriend in the past.[189] Defence counsel further claimed that the complainant or someone acting on her direction likely posted her intimate images online.[190] While the judge concluded that the accused authored most of the electronic conversations

---

[181] *Ibid.* at paras 132-42.

[182] *R. v. Owens*, 2007 ONCJ 151, 2007 CarswellOnt 2088 (Ont. C.J.) [*Owens*] at paras. 22-25.

[183] *Ibid.* at para 43.

[184] *Ibid.*

[185] *Ibid.*

[186] *Ibid.* at para 45.

[187] *Ibid.*

[188] *SS, supra* note 62.

[189] *Ibid.* at paras 52-53, 58.

[190] *Ibid.* at para 75.

tendered as evidence, he found it "plausible" that the complainant was talking to herself at some points.[191] The judge relied on certain characteristics of digital platforms for this finding, noting that the display name of a Skype account can be easily changed at any time and was "in no way dispositive" of the question of whether that message originated from a particular account,[192] that it would have been simple for the complainant to gain access to the accused's Skype account,[193] and that Facebook does not take steps to ensure account holders are who they say they are.[194]

In contrast to *Lauck* and *Owens,* the judge in *SS* rejected arguments that similarities in language and spelling errors between contested and non-contested messages, as well as references to personal information about the accused within those messages, established that they were written by the accused. The judge found that someone attempting to disguise themselves as the accused could have included these references "in an effort to add credibility to a deception," and that the complainant would have had this knowledge of the accused given their past intimate relationship.[195] The judge ultimately found that neither the accused nor complainant were credible witnesses, and that the integrity of the electronic evidence was "at the very low end of the spectrum," such that he was left with a reasonable doubt about what actually occurred.[196]

Finally, in *Aslami*, defence counsel at trial had raised the theory that the accused's ex-wife and a man he considered an enemy might have authored incriminating messages in order to frame him.[197] In that case, the accused's ex-partner had a sexual encounter with the accused's so-called enemy and sent the accused an image of the two of them in bed together. A few hours after that image was sent, the home of the enemy's ex-wife, where she and their three children resided, was set on fire. At trial, the Crown relied on SMS text messages, messages sent through an application called TextNow,[198] and Facebook messages implicating the author in the fire-bombing, arguing these messages had been authored by the accused.

The trial judge detailed reasons for finding the accused had authored the electronic messages, highlighting evidence he found did not depend on the testimony of the complainants and noting the animus between the parties and the

---

[191] *Ibid*. at paras 116-17.

[192] *Ibid*. at paras 120, 125.

[193] *Ibid*. at para 121.

[194] *Ibid*. at para 123.

[195] *Ibid*. at para 130.

[196] *Ibid*. at para 85.

[197] *R. v. Aslami* (December 8, 2017), Doc. Ottawa C66326 (Ont. C.J.) at para. 19 [*Aslami* 2017].

[198] TextNow is a free Canadian-developed application designed for use on computers or cellular phones that allows users to obtain one or more phone numbers and to make calls and send text messages over WiFi. According to its website, the application has fifteen million users (textnow.com).

defence theory of possible fabrication.[199] The judge found the content and timing of the messages aligned with the accused's activities at the relevant time, as confirmed by independent evidence.[200] The judge also found that consistency in "content, specific terms, tone, grammar and spelling" between the messages sent across the various platforms indicated the accused had authored all of them.[201]

The Ontario Court of Appeal found that the trial judge in *Aslami* committed a serious error in failing to "recognize the inherent fallibility" of the digital evidence.[202] At paragraph 11, Nordheimer JA stated:

> This case demonstrates the risks associated with not paying adequate heed to the dangers that are associated with relying on text and other messages, absent expert evidence explaining how various pieces of software, or "apps," can be used to generate these messages, and how reliable the resulting messages are in different respects. Put simply, it is too easy to use various pieces of software to create, or manipulate, messages such that they can appear to be from someone when, in fact, they emanate from an entirely different person. Similarly, the timing of the messages can be altered to suit a particular purpose.

The Court noted the lack of any evidence directly linking the messages to the accused. While accepting that the trial judge could reasonably have concluded that text messages describing the accused's whereabouts were authored by him,[203] the most incriminating messages were sent via the TextNow application, which the Court found to be unreliable. The screenshots tendered by the Crown did not show the exact time each message was sent or received, and no expert evidence was led regarding the functionality or fallibilities of TextNow.[204] Further, nothing in the content of the TextNow messages established the accused as the sender.[205] While the trial judge had found that particular phrases and spelling errors including "Karama is a bitch," "my worst enemie," "u won" or "u win," "Woow," misspelling "else" as "elese," and misspelling "house" as "hous" on multiple occasions indicated the accused authored all the messages,[206] the Court of Appeal criticized the trial judge's reliance on style and tone as a "flawed and unreliable foundation" for that conclusion.[207] The Court noted that grammar and spelling are not unique to an individual person, text messages often use unusual expressions, and spelling errors are common in relation to text

---

[199] *Aslami* 2017, *supra* note 197 at para 19.

[200] *Ibid*. at paras 32-33.

[201] *Ibid*. at para 63.

[202] *Aslami* 2021, *supra* note 79 at para 10.

[203] *Ibid*. at para 23. The Court noted, however, that no cellphone had been found on the accused when he was arrested.

[204] *Ibid*. at para 20.

[205] *Ibid*. at para 24.

[206] *Aslami* 2017, *supra* note 197 at paras 62-74.

[207] *Aslami* 2021, *supra* note 79 at para 26.

messages.[208] The Court found that it was unclear "what the trial judge meant by, or how he could extract, the 'tone' of the text messages," or how such tone would be unique to the appellant.[209] The Court further found that determining that the substantive content indicated the appellant was the author engaged in "somewhat circular reasoning," as it assumed that because the sender knew about the firebombing, it must be the accused who sent the messages.[210] Finally, the Court found the Facebook messages had no evidentiary value, as there was no evidence tying them to the accused other than the recipient's belief they originated from him.[211] The Court warned that trial judges must be cautious in their evaluation of electronic evidence and noted that the prosecution ought to have called expert evidence to address the issues posed by the evidence.[212]

The Ontario Court of Appeal's decision in *Aslami* appears to indicate that expert evidence relating to the functionality and reliability of messaging software and applications will be necessary in some cases where authorship is contested.[213] This, along with the Court's rejection of reliance on similarities in style and tone of contested messages as indicative of authorship, appears to be something of a departure from the previous case law on authorship of digital communications.[214] Judges are being asked to strike a difficult balance between accepting the reality that digital communications can be fabricated with relative ease, while not allowing entirely speculative and far-fetched claims regarding alternative authorship to raise a reasonable doubt in every case involving digital evidence. In the final section of this paper, we outline our recommendations for police, Crown, and judges to ensure that accuseds' right to a fair trial is protected without creating an impossible burden for the Crown and re-traumatizing victims of GBV when authorship is disputed.

(f) Recommendations

The cases examined above indicate that the criminal justice system is in a state of flux regarding the handling of electronic evidence in cases where the authorship of that evidence is contested. This state of uncertainty may cause difficulties for complainants in cases of GBV. Complainants have historically been disbelieved and have borne the brunt of providing evidence, where scant

---

[208] *Ibid*. at para 26.

[209] *Ibid*. at para 27.

[210] *Ibid*. at para 28. This indicates that, while messages containing details of an offence may be helpful in establishing identity where the occurrence of the crime itself is contested, such as in cases of sexual assault (see e.g. *Macdonald, supra* note 61), reliance on such messages to establish identity may be considered "circular" where the prospect of the accused being framed has been raised.

[211] *Ibid*. at para 29.

[212] *Ibid*. at para 30.

[213] *Ibid*. at paras 11, 30.

[214] See e.g. *Lauck, supra* note 62; *Proctor, supra* note 153; *Owens, supra* note 182; *Careen, supra* note 174.

evidence may exist, on which the person who harmed them can be found guilty beyond a reasonable doubt. In this concluding section we briefly outline some recommendations stemming from our examination of the existing case law that may assist victims of GBV, police, and the Crown in providing the courts with sufficient evidence to prove authorship in cases involving crucial digital evidence.

When receiving a complaint of GBV, police must consider whether relevant digital evidence may be available and work quickly to ensure that evidence is located, extracted, and preserved in a timely manner. In order to do this, police must familiarize themselves with various social media and messaging platforms and make timely requests to intermediaries such as cell phone companies, Internet Service Providers, and in some cases social media or software companies to gather relevant information about the source, timing, or location of these communications.[215] When possible, police should consider collecting the metadata associated with this evidence.[216] While metadata was not always necessary to establish authorship in the GBV cases we reviewed, it can assist police, the Crown, and the court in identifying the date, author, recipient, and other relevant details related to the case.[217]

Given the nature of police investigations involving GBV complaints, the majority of digital communications evidence will likely come from complainants' devices. Police should do everything in their power to ensure that this information is extracted quickly, and GBV complainants are not deprived of their digital communications devices for extended periods of time, as complainants will often rely on these devices for their social connections, livelihoods, or ability to access help or support in the wake of a traumatizing violent incident.[218] Wherever possible, police should consider the possibility of extracting this digital evidence elsewhere by obtaining a warrant to search the accused's devices,[219] seizing an accused's devices in cases of allegations of non-consensual distribution, voyeurism, or child pornography,[220] or using their

---

[215] See e.g. *Donaldson, supra* note 78 at 5; *SS, supra* note 62 at paras 104-05, 112; *Aslami* 2021, *supra* note 79 at para 20.

[216] Susan Wortzman & Susan Nickle, "Obtaining Relevant Electronic Evidence" (2009) 36:2 Adv Q 226.

[217] Gordon Scott Campbell, "What Test will be Applied by the Courts with Respect to the Production of Metadata Related to Digital Images" (1 June 2019) Carswell CARS1-MEMO:ONM 9274.

[218] In a case not cited elsewhere in this paper (*R. v. C.R.D.*, 2019 PESC 30, 2019 CarswellPEI 56 (P.E.I. S.C.)), the judge critiqued the police for not seizing the complainant's phone to recover relevant digital evidence. This was not done in part because the complainant did not want to part with her phone for the "couple of weeks to a month" she understood she would need to, and the judge noted that while the complainant claimed she could not do without her phone during that time for school and family reasons, the police "did not pursue that option with any vigour" (at paras 10, 36). See also Nancy E Glass et al, "The Longitudinal Impact of an Internet Safety Decision Aid for Abused Women" (2017) 52:5 Am J Preventative Medicine 606; Chuka Emezue, "Digital or Digitally Delivered Responses to Domestic and Intimate Partner Violence During COVID-19" (2020) 6:13 JMIR Public Health Surveillance 1.

power under the *Criminal Code* to obtain a preservation or production order from an individual or company likely to possess relevant data.[221] The accused may have a reasonable expectation of privacy in their electronic communications even if these are seized from the device of the recipient, something the police must take into account when conducting searches of electronic devices.[222] Whether a reasonable expectation of privacy exists will turn on a case-specific assessment of the totality of the circumstances,[223] and thus section 8 *Charter* considerations must always be kept in mind by investigating officers.

Finally, officers involved in the extraction of relevant digital evidence should be prepared to testify about how this evidence was located and extracted, and about the functionality of the relevant application or platform from which it was obtained. Once again, having familiarity with a wide variety of digital messaging platforms will be necessary in this regard. Officers understanding what these platforms are and how they function will assist in ensuring relevant digital evidence is extracted quickly, properly, and comprehensively, and may limit the necessity of requiring expert evidence at trial, as discussed further below. Alternatively, forensic experts may be used to carry out these searches and be similarly prepared to testify on these issues.

Assuming police have undertaken a comprehensive investigation and located all relevant digital evidence, it is up to Crown counsel to ensure this evidence is presented in a way that establishes as far as possible that the accused authored these messages. Crown counsel should put together as complete a record as possible of communications between the complainant and the account or number associated with the contested messages, as a history of communications between the complainant and that account or number was found to be relevant to establishing authorship in a number of cases.[224] The time and dates stamps of the communications should be included, as well as evidence confirming that the time records on the device accurately represented the time.[225]

Crown counsel should familiarize themselves with the admissibility requirements under the *CEA* and ensure that all electronic evidence, including relevant digital communications, is properly admitted pursuant to those provisions.[226] Crown counsel must ensure that the complainant is properly

---

[219] Coughlan & Currie, *supra* note 22.

[220] *Code, supra* note 55, s 164.1.

[221] See *ibid.,* ss 487.012-487.016; Grice & Schwartz, *supra* note 28.

[222] See *R. v. Mills*, 2019 SCC 22, 2019 CarswellNfld 161, 2019 CarswellNfld 162 (S.C.C.) [*Mills*]; *R. v. Marakah*, 2017 SCC 59, 2017 CarswellOnt 19341, 2017 CarswellOnt 19342 (S.C.C.) [*Marakah*]; *R. v. Ahmad*, 2020 SCC 11, 2020 CarswellOnt 7387, 2020 CarswellOnt 7388 (S.C.C.).

[223] *Marakah, supra* note 222; *Mills, supra* note 222.

[224] *Moon, supra* note 61; *Phagura, supra* note 105; *Soh, supra* note 106; *Macdonald, supra* note 61; *Hirsch, supra* note 84 at para 26; *Proctor, supra* note 153 at para 139; *Lauck, supra* note 62 at para 138.

[225] Hasan, *supra* note 115.

prepared to answer questions about the source and timing of any contested communications, as well as how and why they believe the communications originated from the accused. A failure to do this in *Himes* resulted in the trial judge intervening to ask how the complainant knew the messages originated from the accused, resulting in an acquittal being entered on appeal.[227] Crown counsel must also prepare complainants to answer basic questions regarding the functionality of their devices and accounts from which the digital evidence was extracted. Complainants are unlikely to be familiar with the evidentiary rules behind digital evidence and would benefit from preparation either by the Crown or from outside legal advice. Several provinces, including Ontario, Nova Scotia, and Newfoundland, have introduced state-funded legal representation for sexual assault complainants.[228] Lawyers in these roles have the opportunity to explain the role that digital evidence may play in the trial process and assist complainants in preparing to testify about digital evidence. Frontline victim service organizations would also benefit from funding and training that could help them explain the role of the complainant in presenting digital evidence at trial.[229] However, not all complainants will have access to these services, and Crown counsel must remain vigilant in their role when preparing witnesses for what to expect at trial.

Circumstantial evidence has been sufficient to prove authorship in a number of cases, and Crown counsel must carefully compile and present such evidence in a way that supports an inference that the accused authored the relevant evidence. When attempting to establish authorship in relation to hearsay, or for the purpose of establishing identity at trial, the Crown should call witnesses who were involved in the creation of the electronic evidence, such as the person who took the screenshot. This was not done in two cases we examined. In one of these cases, the judge noted that calling such a witness would have been preferable,[230] and the accused was acquitted in the other.[231] This process of establishing

---

[226] See e.g. *Donaldson, supra* note 78, in which electronic evidence was excluded based on the Crown's failure to tender additional evidence.

[227] *Himes, supra* note 105.

[228] Queen's Printer for Ontario, "Independent Legal Advice for Sexual Assault Victims" (15 July 2021), online: *Ontario.ca* < www.ontario.ca/page/independent-legal-advice-sexual-assault-victims > ; Province of Nova Scotia, "Legal Advice for Sexual Assault Survivors", online: *NovaScotia.ca* < novascotia.ca/sexualassaultlegaladvice/ > ; Government of Newfoundland and Labrador, "Legal Support Now Available to Survivors of Sexual Violence" (19 June 2018), online: *Newfoundland Labrador* < www.gov.nl.ca/releases/2018/exec/0619n02/ > .

[229] The BC Society of Transition Houses is an example of an organization doing excellent work in this area. They have published a comprehensive resource entitled *Technology-Facilitated Violence: Preserving Digital Evidence Toolkit* intended to assist victims in collecting and preserving digital evidence for use in criminal or civil courts: online, bcsth.ca/digitalevidencetoolkit/.

[230] *Hirsch, supra* note 84.

[231] *SS, supra* note 62.

authorship could also include taking statements from witnesses who received or took screenshots of the digital evidence, searching the device from which the original post was made, or obtaining information from a social media website to address issues of authorship.

Whatever the comprehensiveness of the police investigation and preparation of Crown counsel, how digital evidence is interpreted and what conclusions are drawn from it are within the control of the judge and trier of fact. In terms of admissibility, the current state of the law indicates that judges are safer to err on the side of admitting electronic evidence pursuant to the *CEA*, even where questions of authorship are contested or unresolved.[232] Judges must ensure they are familiar with the *CEA* provisions so that their admission and consideration of digital evidence is not left vulnerable to appeal.[233] That being said, the extremely low bar for threshold admissibility under the *CEA* has raised concerns for trial fairness by some commentators.[234] We agree with Silver that judges should consider using their gatekeeper function to exclude electronic evidence that may be unfairly prejudicial.

Crucially, judges should familiarize themselves with the functionality of common digital communications technologies. David Paciocco noted in 2013 that many judges consider information technology to be mysterious, but that fear of this technology, and concern about potential manipulation, cannot result in the rejection of the use of electronic documents and emails at trial.[235] The Canadian Judicial Council released a substantially revised *Ethical Principles for Judges* in June 2021. These principles state that judges "should develop and maintain proficiency with technology relevant to the nature and performance of their judicial duties."[236] We agree with Amy Salyzyn that this obligation should be read as including competence in relation to commonly used technologies that may produce evidence tendered in court.[237] While judges cannot be expected to keep up to date with every available digital messaging service, social media platform, or communications application, some awareness of the workings of widely-used technologies and the general operations of these platforms should be required.

Judicial familiarity with digital communications technologies will help ensure that trials where authorship of digital evidence is contested proceed in an expedient and fair manner. While testimony explaining the operation of certain

---

[232] Dufraimont, "Case Comment", *supra* note 117.

[233] See e.g. *Hirsch, supra* note 84; *Durocher, supra* note 84; *CB, supra* note 17.

[234] Dufraimont, "Case Comment", *supra* note 117; Silver, *supra* note 1.

[235] Paciocco, *supra* note 4 at 181-83.

[236] Canadian Judicial Council, "Ethical Principles for Judges" (2021), Commentary 3.C.5, online (pdf): < cjc-ccm.ca/sites/default/files/documents/2021/CJC_20-301_Ethical-Principles_Bilingual_Final.pdf > .

[237] Amy Salyzyn, "A Taxonomy of Judicial Technology Competence", *Slaw* (24 June 2021), online: < www.slaw.ca/2020/12/18/a-taxonomy-for-lawyer-technological-competence/ > .

electronic devices, applications, or platforms will often be necessary, we believe that expert evidence regarding the functionality of these devices, applications, or platforms should only be required in cases dealing with disputes regarding particularly complex or uncommon technologies or investigatory techniques, or in cases where there is evidence to suggest the digital evidence has been manipulated. While it was not explicitly stated in the decision, we understand the Ontario Court of Appeal's finding in *Aslami* to suggest that expert evidence should be called to explain how messaging software operates in the context of the lesser-known application TextNow. This suggests that expert evidence may be required to explain apps that might not be familiar to the courts, or may more easily be used to misrepresent data. We do not understand this to be a finding that expert evidence will always be necessary in cases involving digital messages where authorship is contested. Expert testimony lengthens the trial process and adds pressure for additional resources from the parties involved and from the courts.[238]

For means of electronic communications that are commonplace and widely-used, such as SMS text messaging, iMessaging, Facebook, Twitter, Gmail, etc., judges should ideally be able to take judicial notice of certain aspects of their functionality.[239] Judicial notice allows judges to accept the existence of a proposition when no reasonable person could dispute the proposition being asserted.[240] In *R. v. Swierkot*, for example, the judge took judicial notice of the functionality of iMessages on the basis that "iPhones have long been among the most commonly used mobile devices on the planet, and that the messaging application is used dozens of times daily by millions of users,"[241] and in *MR* the judge noted that "[a]lmost any sentient person in our society knows in a general sense, that page rank returns on Google are generated by a complicated revenue-driving enterprise, combined with a propriety algorithmic ranking of the interest associated with a particular website."[242]

In the cases we reviewed, everything from the complainant's sole testimony,[243] to non-expert testimony from investigating officers,[244] to evidence from a qualified expert[245] was relied on to establish authenticity and/

---

[238] Coughlan & Currie, *supra* note 22; Paciocco, *supra* note 4.

[239] Paciocco, *supra* note 4 at 188-92; Jeffrey Bellin & Andrew Guthrie Ferguson, "Trial by Google: Judicial Notice in the Information Age" (2014) 108:4 Nw UL Rev 1137.

[240] *R. v. Find*, 2001 SCC 32, 2001 CarswellOnt 1702, 2001 CarswellOnt 1703 (S.C.C.) [*Find*]; *R. v. Spence*, 2005 CarswellOnt 6824, 2005 CarswellOnt 6825, [2005] 3 S.C.R. 458 (S.C.C.) [*Spence*].

[241] *R. v. Swierkot*, 2019 QCCQ 4820, 2019 CarswellQue 7397 (C.Q.) at para. 117.

[242] *MR, supra* note 154 at para 84.

[243] *Colosie, supra* note 94; *Durocher, supra* note 84; *Hirsch, supra* note 84; *Lauck, supra* note 62; *Macdonald, supra* note 61; *Moon, supra* note 61; *MR, supra* note 154; *Phagura, supra* note 105; *Proctor, supra* note 153.

[244] *CB, supra* note 17; *Harris, supra* note 36; *Himes, supra* note 105 (in relation to Facebook messages sent to the first complainant); *Martin, supra* note 17.

or identity. For technologies that are not commonplace, or with regard to aspects of their operation that are not notorious or capable of immediate and accurate demonstration,[246] lay "fact" witnesses with expertise or experience using the technology or platform should provide factual evidence about its operation without requiring qualification as an expert.[247] As noted in *R. v. Durigon,* where the evidence "concerns facts related to the operation of technology, the evidence is properly regarded as simply factual technical information, ultimately incontrovertible, and not open to debate."[248] Paciocco classifies "mundane technologies" as "the day-to-day uses to which information technology is put," and he includes the use of social media and the operation of search engines, computers, tablets, smart phones, applications, and digital recording technologies within this category.[249] In cases where courts require help in understanding these mundane technologies, lay witnesses can be called to describe their functionality.[250] Where there is a debate between the parties as to how the technology operates, where there are legitimate concerns over the manipulation of evidence through technology, or where evidence is required to explain a more technical aspect of the technology's operation, expert opinion may be required.[251]

Our final recommendation relates to the standard that judges should apply in assessing defence theories of fabrication in cases where the evidence is wholly or primarily circumstantial. An accused's right to make full answer and defence entitles them to challenge the Crown's case and lead evidence raising a reasonable doubt as to whether the accused committed the offence.[252] While all relevant evidence put forward by the defence must not be excluded unless its prejudicial effect substantially outweighs its probative value,[253] in order for a judge to put a defence to a jury, the accused "must point to evidence on the

---

[245] *JV, supra* note 115; *Owens, supra* note 182; *Harris, supra* note 36.

[246] *Spence, supra* note 240 at para 53; *Find, supra* note 240.

[247] *R. v. Marquard*, 1993 CarswellOnt 995, 1993 CarswellOnt 127, 85 C.C.C. (3d) 193, [1993] 4 S.C.R. 223 (S.C.C.); *R. v. Durigon*, 2017 ONSC 7075, 2017 CarswellOnt 21796 (Ont. S.C.J.) at paras. 44, 48; *R. v. Hamilton*, 2011 ONCA 399, 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 10920, 2012 CarswellOnt 10921 (S.C.C.), leave to appeal refused 2012 CarswellOnt 10892, 2012 CarswellOnt 10893 (S.C.C.); *R. v. Cyr*, 2012 ONCA 919, 2012 CarswellOnt 16386 (Ont. C.A.); *R. v. Ajise*, 2018 ONCA 494, 2018 CarswellOnt 8628 (Ont. C.A.), affirmed 2018 CarswellOnt 19672, 2018 CarswellOnt 19673 (S.C.C.). See also Paciocco, *supra* note 4 at 185.

[248] *Durigon, supra* note 247 at para 44.

[249] Paciocco, *supra* note 4 at 185.

[250] *Ibid.* at 185-86.

[251] *Ibid.* at 186.

[252] *Grant, supra* note 148 at para 4.

[253] *Ibid.*; *R. v. Seaboyer*, 1991 CarswellOnt 109, 1991 CarswellOnt 1022, [1991] 2 S.C.R. 577 (S.C.C.); *R. v. Shearing*, 2002 SCC 58, 2002 CarswellBC 1661, 2002 CarswellBC 1662

record that gives the defence an air of reality."[254] Further, when assessing circumstantial evidence, inferences consistent with innocence do not have to arise from proven facts.[255] Rather, in assessing circumstantial evidence, what matters is the range of reasonable inferences that can be drawn from this evidence.[256]

As noted above, the Supreme Court of Canada's decision in *Villaroman* clarifies that the Crown is required to respond to, and judges are required to consider, plausible alternative theories other than guilt.[257] The Court in that decision noted that the line between a plausible alternative theory and speculation is not always easy to draw.[258] A theory alternative to guilt will not be speculative simply because it arises from a lack of evidence, rather than evidence on the record; however, it must "be based on logic and experience applied to the evidence or absence of evidence, not on speculation."[259]

In our view, the assessment of whether viewed logically and in light of human experience the evidence is reasonably capable of supporting an inference other than guilt must include some consideration of the reasonable likelihood of a theory involving fabrication or an alternative sender.[260] Alternative inferences must be reasonable, not just possible.[261] In the cases we examined, judges generally dismissed as far-fetched or unrealistic theories that a third party sender authored the incriminating messages,[262] or that the complainant authored them herself.[263] While there will certainly be circumstances in which the possibility of fabrication should be taken seriously and be sufficient to raise a reasonable doubt as to guilt, we argue that there must be some evidence to support the assertion that this could be the case to meet the standard of a plausible alternative theory. While the Court of Appeal ordering a new trial in *Aslami* may have been the only outcome consistent with the accused's right to be presumed innocent, we also note that the Court overturned the trial judge's decision based on a lack of direct evidence establishing the accused as the author of the messages while rejecting types of circumstantial evidence that have assisted in proving authorship in previous cases.[264] The Court also did not engage deeply with the

---

(S.C.C.); *R. v. Arcangioli*, 1994 CarswellOnt 1151, 1994 CarswellOnt 51, [1994] 1 S.C.R. 129 (S.C.C.).

254 *Grant, supra* note 148 at para 20, citing *R. c. Cinous*, 2002 SCC 29, 2002 CarswellQue 261, 2002 CarswellQue 262 (S.C.C.).

255 *Villaroman, supra* note 162 at para 35.

256 *Ibid.*

257 *Ibid.* at para 47.

258 *Ibid.* at para 39.

259 *Ibid.* at para 36.

260 See *Lauck, supra* note 62.

261 *Ibid.* at para 42, citing *R. v. Dipnarine*, 2014 ABCA 328, 2014 CarswellAlta 1776 (Alta. C.A.) at paras. 22, 24-25.

262 *Harris, supra* note 36; *MR, supra* note 154; *Proctor, supra* note 153.

263 *GB, supra* note 62; *Lauck, supra* note 62; *Owens, supra* note 182; *Careen, supra* note 174.

plausibility of the defence theory that the complainants could have authored the messages themselves. For example, as noted by the trial judge, any plan to frame the accused involving the man who was his enemy would have required his so-called enemy to be complicit in fire-bombing a house where his own children lived.[265]

CONCLUSION

Cases of GBV, including sexual assault and intimate partner violence, are uniquely challenging for all criminal justice system actors and participants. In addition to the historical biases, myths, and stereotypes that continue to contribute to GBV victims being disbelieved, having their behaviours unfairly scrutinized, and having their cases insufficiently investigated, the increase in digital evidence in these cases has created new challenges for police, the Crown, and judges. Authorship of digital evidence can be difficult to prove given its fluid, interconnected, and dynamic nature, and questions of who authored relevant digital evidence may be frequently raised and difficult to resolve.

In order to ensure GBV trials proceed fairly, and that complainants do not have their claims dismissed or credibility undermined based on speculative claims regarding contested authorship, justice system participants must ensure they take requirements regarding electronic documents seriously. Victims of gender-based violence are often reluctant to report the crimes against them because of the systemic barriers they have faced and continue to face that make the costs of participating in the justice system outweigh the benefits. Without sufficient investigations and adequate trial strategies involving GBV and digital evidence, victims are at risk of being re-traumatized by the justice system process. Additionally, inadequate investigations may result in trial unfairness for the complainant. Police must ensure the timely and accurate collection of electronic evidence, ideally including evidence indicating the author of digital messages. Crown counsel bear the responsibility of proving identity beyond a reasonable doubt and must ensure any digital evidence supportive of identity is properly admitted and fully explored through direct and cross-examination of witnesses, including expert witnesses where challenges to the veracity of this evidence are likely. Judges must ensure that they familiarize themselves with the evolving law in this area and keep up to date with communications technologies that are in general use, and they must not unduly exclude or give little weight to digital evidence based on the mere possibility of fabrication. The criminal justice system is adjusting to the new reality of digital evidence, and actors within that system must do their best to ensure trial fairness for victims of GBV.

---

[264] *Lauck, supra* note 62; *Owens, supra* note 182; *Proctor, supra* note 153; *Careen, supra* note 174.

[265] *Aslami* 2017, *supra* note 197 at para 97.