Social Incrimination: How North American Courts are Embracing Social Network Evidence in Criminal and Civil Trials

DAN G R I C E * A N D D R. B R Y A N S C H W A R T Z **

I. INTRODUCTION

After the 2011 Stanley Cup finals in Vancouver, infuriated citizens turned en masse to Facebook to search for culprits responsible for vandalizing cars and looting downtown stores. After a bank robbery in Texas, police arrested two bank tellers, the boyfriend of one and the brother of another, after being informed that one of the four posted, "IM RICH" on Facebook.¹ In New Brunswick, a defendant in a person injury lawsuit persuaded the judge to force the plaintiff to archive her Facebook account after photos of her zip-lining appeared to demonstrate that her injuries were not as serious as she claimed.²

Interesting stories like this surface almost every day. Incriminating statements made on a social network may end up opening the door to more substantial investigations. Sometimes investigators discover the evidence, although often it is an individual's own online “friends”. This is

* B.A. (UBC), J.D. (Manitoba). Winnipeg. Articling student-at-law at Baker Newby LLP in Chilliwack. The views expressed herein are his own and do not necessarily reflect the views or opinions of Baker Newby LLP.

** LL.B. (Queen's), LL.M. (Yale), J.S.D. (Yale). Asper Professor of International Business and Trade Law, University of Manitoba.


² Sparks v Dubé, 2011 NBQB 40, 374 NBR (2d) 26 [Sparks].
an era where mobile phones equipped with cameras are common and internet usage has become widespread, presenting investigators and litigators with potential treasure troves of information. A modern obsession with sharing personal thoughts and photographs with online acquaintances has led to incriminating statements and embarrassing photographs proving probative or undermining the credibility of witnesses and litigants in a wide range of cases. As a result, courts across North America are revising and reinterpreting their evidentiary rules to handle evidence gathered from social networking websites.

This paper takes a comprehensive look at a wide variety of evidentiary issues, procedural rules and examples of social networking evidence used in criminal and civil cases in both Canada and the United States. Part II briefly introduces the major social networks and examines their use by courts. Part III addresses some of the general statutes which deal with investigators’ and courts’ access to social networking evidence. Part IV examines the acquisition and use of social networking evidence in the criminal context, including the importance and difficulties of authenticating evidence and the various ways in which courts have reviewed evidence to prevent prejudice. Part V examines the implications of social networking evidence in civil cases, particularly how litigants use court processes to discover information about their adversaries. This can range from uncovering unknown online defamers, to forcing the revelation of pictures or posts from a private section of a social network account. Lastly, we look at how civil courts deal with balancing privacy concerns with the broader obligation to disclose relevant material.

II. Social Networks: An Overview

Social networks are a part of daily life for a large number of Canadians and others across the globe. Websites such as Facebook, MySpace, YouTube, Twitter and LinkedIn let users share statuses, personal pictures, and create personal profiles for themselves, their music bands, or social groups. There are estimated to be over 17 million user accounts in Canada

---

3 Charles Foster, “Social Networks are a Treasure Trove of Information” Claims Canada (October 2008), online:<http://www.claimscanada.ca/issues/article.aspx?aid=1000224989>.
on Facebook alone. These websites facilitate individuals sharing aspects of their lives with friends, acquaintances, or the public at large, depending on the privacy settings of the account. Photos, videos and personal statuses can be added to the website from home computers or from smartphones.

Primarily physically located in California, social networks utilize large data storage facilities and rely on proprietary systems to control the upload of files and privacy settings used. The scale and complexity of these systems means that litigants or investigators must rely upon the companies’ retrieval processes, and have very little ability to retrieve data deleted from the server. Unlike a personal computer where a single drive can be forensically scanned for deleted emails or files, lawyers seeking to use evidence from social networks must often pre-emptively capture the files themselves, obtain the cooperation of the opposing party, or (in criminal investigations) request that the hosting company preserve a user’s account.

Each social networking website has its own unique format and appeals to its own niche. In order to appreciate the potential uses of social networking evidence, it is important to understand the various companies. Several of the most prominent are discussed below.

A. MySpace

MySpace, one of the earliest popular social networks, originally gained in popularity by allowing anonymous profiles and by catering to music fans with its ability to upload music and to customize the look of a profile. From its founding in 2003 up until early 2009, it was the predominant social network in North America. Cases involving MySpace often involve obtaining evidence against sexual predators, proving gang affiliation for those who relied on its partial anonymity to brag about their exploits, and more recently, providing evidence in civil cases. The main legal issue that arises is authentication, because users may create accounts under any pseudonym. Generally, profiles were public and available to anyone so,

---

4 Facebook provides estimates for its advertisers: see online: Facebook, <http://www.facebook.com/ads/manage/adscreator/> (Login required).
5 The number of users grows every month. One source estimated that by the middle of 2011, the company had over 750 million monthly user. Jason Kinkaid, “Facebook Now Has 750 Million Users” (23 June 2011) online: <http://techcrunch.com/2011/06/23/ facebook-750-million-users>.
unlike other social networks’ evidence, most jurisprudence involved proving authorship of potentially damaging posts rather than trying to uncover the posts themselves. MySpace is referenced more in American case law than in Canadian case law.

B. Facebook

Launched in 2004, Facebook allows the creation of user profiles and discourages anonymous posts. Originally confined to college campuses, it has surpassed MySpace in popularity.6 The initial terms of service (which required users to have an academic email account, use a real name and have an actual photograph) have been relaxed to allow anyone with an email address to create a profile. However, Facebook still reserves the right to disallow fake names. Facebook’s most popular feature has been users’ “walls”, more recently changed to “timelines”, where users are encouraged to share personal updates, videos and photographs. As users need to approve their “friends” and can control who accesses their profiles, there is a sense of privacy. Perhaps as a result there is a greater predisposition for users to reveal things they might not otherwise share publicly.

Consequently, evidence from Facebook is becoming increasingly important in both criminal and civil trials. In the criminal context, users have been convicted of uttering threats, uploading incriminating pictures linking them to crime scenes, or posting comments undermining their credibility. In family courts, evidence retrieved from Facebook is being used to challenge the parenting ability of partners in custody disputes. In civil trials and injury lawsuits, defendants are increasingly using discovery motions against plaintiffs to uncover Facebook photographs that may undermine the extent of plaintiff claims.

C. Nexopia

The largest social network run by a Canadian company is Nexopia, based in Alberta, and its user base is mainly teenagers. The primary references in Canadian courts to this particular social network site refer to sexual predators targeting its younger user base and generally, evidence is

obtained as part of a larger criminal investigation.⁷ Because Nexopia is Canadian-based, American laws that limit voluntarily disclosure by hosts of user information to law enforcement do not apply.⁸ As a result, when users sign up they agree to terms that allow the company to screen for potentially illegal posts and to disclose them if necessary.

D. Twitter

Twitter is a website which allows individuals to post brief “tweets” and share them with a broad public audience rather than with a subset of online friends. It appears infrequently in Canadian case law and has not contributed significant evidence in either Canada or the US. Although a very popular site, it does not provide native picture-hosting capabilities and restricts posts to 140 characters in length, providing a limited opportunity to express oneself or share potentially incriminating evidence.

Legal discussions have arisen about the unlawful sharing of Canadian election results,⁹ and controversy arose in the US from attempts to uncover the identities of Wikileaks supporters who may have been responsible for obtaining stolen government documents.¹⁰ While little case law exists in regards to defamation, Twitter’s counsel recently told a forum that this area is very common for litigation and its general policy is to notify users before handing over their information.¹¹ For the most part, most Twitter accounts are completely public, so any discovery would involve attempting to identify the account owner and the author of posts rather than uncovering information.

---

⁸ US, The Stored Wire and Electronic Communications and Transactional Records Access Act, 18 USC § 2701-§ 2712 (2012) [SCA] generally limits ISPs from disclosing information without a warrant and is discussed later. However, exceptions are made in the US to case involving harm to children.
⁹ Canadian Broadcasting Corp v Canada (Attorney General), 2011 ONSC 2281, 105 OR (3d) 679.
¹⁰ In re 2703(d), Order; 787 F Supp (2d) 430 (ED Va 2011) [Re 2703(d)].
E. LinkedIn

LinkedIn caters to professionals who wish to display their work history and other work-related and professional information. As a business-oriented social network, LinkedIn is rarely referenced in Canadian jurisprudence. Some courts have even purposely denied discovery of LinkedIn while granting discovery of other networks.\(^2\) In the US, LinkedIn postings have played a role in a small number of commercial cases. Evidentiary uses have included attempts to show that a party breached non-competition agreements by contacting former clients,\(^3\) to establish the geographic location of witnesses with a view to establishing the proper forum for litigation,\(^4\) to demonstrate work history,\(^5\) or that a party engaged in misrepresentation.\(^6\)

F. YouTube

YouTube, now owned by Google, is a popular website for sharing videos. It is one of the primary Internet video-hosting platforms and the source of many cases involving video copyright infringement. For lawyers concerned with copyright infringement, a whole series of case law in the US involves application of the US Digital Millennium Copyright Act to Youtube.\(^7\) Additionally, YouTube has been brought up in the courts regarding evidence of threats,\(^8\) association with gang members in rap videos,\(^9\) human rights violations involving statements about sexual orientation,\(^10\) and even some personal injury videos.\(^11\) While YouTube does allow private videos, most videos are public and courts have not generally had to deal with civil discovery motions to uncover content. However, in instances where the author of the video is not readily apparent, investigators may be required to contact YouTube for evidence regarding

---

12 Sparks, supra note 2.
15 Blyde v Harrah’s Entertainment, Inc, 2010 WL 5387486 (WD Tenn).
16 Nationwide Payment Solutions, LLC v Plunkett, 2011 WL 446077 (D Me).
18 R v B(R), 2011 ONCJ 118 (available on WL Can) [R v B(R)].
19 R v Sinclair, 2010 ONSC 7254 (available on WL Can) [Sinclair].
20 Pardy v Earle, 2011 BCHRT 101 (available on WL Can).
21 Tyrell v Bruce, 2010 ONSC 6680, 92 CCLI (4th) 248 [Tyrell].
authorship. While YouTube is the most common video sharing site, other emerging video sharing sites, such as Ustream and BlogTV, that are devoted to real-time streaming video, may eventually also find their way into court.

III. EVIDENTIAL LIMITATIONS

Lawyers and courts wanting to use social networking evidence must consider issues involving the rules of evidence. Many precedents and statutes that courts contemplate in social networking cases were established in the context of a world based on paper and ink documents, rather than data created, stored and presented electronically. The challenge for courts is to remain faithful to established principles, while interpreting and applying them in a manner that is sensitive to the practical realities of new technologies.

A. General Evidentiary Rules of Procedure

Generally, both Canadian and American evidentiary laws require the authentication of evidence; this applies to both criminal and civil trials. US rules on admissibility tend not to differentiate between electronic evidence and traditional evidence, often admitting electronic evidence as “writing”. For instance a California court, in dealing with a photograph from a social networking site, utilized laws surrounding writing. In addition to American federal laws that limit how social networks can release private content, a variety of evidentiary rules at both the federal and state level will apply, depending on the nature of the proceeding.

In Canada, the federal rules of evidence that regulate criminal trials recognize electronic evidence as part of the recommendation of the Uniform Law Conference of Canada. The Personal Information Protection and Electronic Documents Act modernized the Canada Evidence Act.

---

22 People v Beckley, 185 Cal App 4th 509 at 2 (Cal App 2 Dist 2010) [Beckley].
24 SC 2000, c 5, s 56 [PIPEDA].
25 Canada Evidence Act, RSC 1985, c C-5 [Canada Evidence Act].
specifically addresses electronic documents, including general guidelines for their admission:

31.1 Any person seeking to admit an electronic document as evidence has the burden of proving its authenticity by evidence capable of supporting a finding that the electronic document is that which it is purported to be.
31.5 For the purpose of determining under any rule of law whether an electronic document is admissible, evidence may be presented in respect of any standard, procedure, usage or practice concerning the manner in which electronic documents are to be recorded or stored, having regard to the type of business, enterprise or endeavour that used, recorded or stored the electronic document and the nature and purpose of the electronic document.\(^26\)

Provincial evidentiary rules, used in civil trials across Canada, have also adopted the Uniform Law Conference recommendations and have similar recognition for the admissibility of electronic documents.\(^27\)

B. Jurisdiction

Unlike traditional evidence, social networking evidence often exists only as a digital record in a data center located in a jurisdiction far removed from the scene of the alleged crime or tort. In many cases, users directly upload photographs and statements to their social networking accounts, and thus the evidence may only be available through one of these websites. Most social networking companies are located in the US. The major ones such as Facebook, MySpace and YouTube are headquartered in California and store information there. Any attempt by a Canadian litigant to compel the release of information from a social network requires the application of American state and federal laws.

While most social networks are located in the US, American courts will generally limit their involvement in Canadian court cases to essential elements, such as domesticating production orders. While servers hosting the content may be located in California, it typically does not create a substantial enough connection to that jurisdiction to give a local court any authority to hear the matter. In other cases, a court might hold that while it does have the authority to hear a matter, it should refrain from exercising jurisdiction but rather leave the matter to be resolved in a more

\(^26\) PIPEDA, supra note 24. (PIPEDA also allowed companies to release private information without consent in accordance with a valid search warrant or subpoena under s 7(3)(c)).

\(^27\) See e.g. Manitoba Evidence Act, RSM 1987, c E150, CCSM c E150, 51.1-51.8.
convenient forum. In *Elmo Shropshire v Canning*, a California court rejected an attempt to sue a Canadian man in their courts for copyright infringement after posting a video with an unlicensed song on YouTube, noting the proper venue would be a Canadian court.\(^{28}\) Courts will also reject claims that there is a sufficient connection simply because a page was viewable in the jurisdiction. A Wisconsin court refused to consider a trademark infringement case involving a California company who used the same trademark, finding that without active solicitation in a region there was insufficient jurisdiction.\(^{29}\) However, where social networking behaviour is purposely directed at an individual or company in another jurisdiction, they may be liable to suit in that location. A Florida court found that an out-of-state company that purposively directed defamation at a Florida company on a website hosted elsewhere had established "minimum contact" and thus the court had sufficient jurisdiction.\(^{30}\)

C. Individual Rights

Various individual rights assigned by statute, the common law, or by constitutional documents or conventions can also impact the evidentiary process as it relates to social network evidence.

1. *The Stored Communications Act*

   The *Stored Communications Act* (SCA)\(^{31}\) is pervasively important in obtaining evidence from social network companies based in the US. Enacted by the US Congress in 1986 prior to the popularization of the Internet, the SCA was initially designed to regulate telecommunications carriers and protect their subscribers from unauthorized access to private communications. Essentially, it prevents companies that offer "electronic communication services" or "remote computing services" from voluntarily handing over personal communications and content, including photographs, statements, chat messages, or profiles to third parties without the subscriber's consent. A limited number of exceptions are made under section 2702, in which law enforcement can obtain the

\(^{28}\) *Elmo Shropshire v Canning*, 2010 Corp L Dec P 30024, (ND Cal).

\(^{29}\) *Trek Bicycle Corp v Trek Winery, LLC*, 2010 WL 744252 (WD Wis).

\(^{30}\) *Spectra Chrome, LLC v Happy Jack's Reflections in Chrome, Inc*, 2011 WL 1337508 (MD Fla).

\(^{31}\) SCA, *supra* note 8, §2701-2712.
contents of transmissions in an emergency involving danger of death or serious physical injury, or with a valid search warrant issued based on reasonable grounds.32 Exceptions are made to non-content based requests such as subscriber information, which may be voluntarily released.33

In Crispin v Christian Audiger, California court confirmed that the SCA applies to all pictures, posts, messages and communications on Facebook and other social networks when privacy settings are available.34 The court quashed a subpoena duces tecum issued by the defendant to Facebook and MySpace to hand over private information or messages from the plaintiff’s account. This decision also means that an accused in a criminal trial will also have no access to obtain private social networking material from potential witnesses, as the exceptions listed in the SCA are only available to government authorities.

The only information that a social network may hand over to a non-governmental authority without consent is basic subscriber details. This includes, for example, what email an account was registered under, when a user started their account, and what internet protocol (IP) address was used to create an account.35 Basic subscriber information may be released by a social network to a third party with a valid subpoena domesticated wherever the social network is located and issued to the company’s registered agents. While the SCA does not affect publicly posted content, which litigators or investigators can capture on their own, it means that any private content required for a civil trial will have to be produced by the party who has access to it.

2. The Canadian Charter of Rights and Freedoms36

As a practical matter in social networking cases, there will rarely be legal significance in applying Canadian standards, including the Charter, to gathering evidence in the US. The Charter does not ordinarily apply to law

32 Ibid § 2702.
33 Ibid § 2701.
35 An IP address is a 12 digit identifying number that is assigned by an internet service provider (ISP) such as a telephone or cable company to a computer when it accesses the internet and can be traced back to find the physical location where a computer accessed the internet.
enforcement activities undertaken abroad by foreign officials, including investigations conducted by Canadian officials while in other jurisdictions. The admissibility of evidence in Canadian proceedings can take into account all the circumstances under which it was originally gathered abroad, and so conscripted evidence obtained abroad in a fashion contrary to Canadian standards might, for example, be excluded because its admission would breach the Charter right to a fair trial.

However, as evidence from social networking websites is gained with the cooperation of the US, Charter issues relating to admissibility rarely arise. In the US, both state and federal Bills of Rights provide protection against unreasonable search and seizure, and statutory and common law protections for users of social networks against release of personal information usually exist. This generally satisfies the rights owed to Canadians under the Charter.

3. Unauthorized access

In the US, any attempt to obtain access to private information on a social network without the authorization of a valid search warrant, emergency exemption, or the consent of the account owner renders an individual liable to tort action. There are two possible torts: a civil tort under the SCA itself or an independent tort of computer trespass. In Canada, however, there has been a case where a court admitted unauthorized content accessed by a spouse who knew her ex-husband’s password without any reprimand from the court.

IV. CRIMINAL PROCEEDINGS

A. Obtaining Social Network Evidence

Obtaining social network evidence in a criminal proceeding has become standardized for law enforcement agents. Larger social networks,

37 R v Hape, 2007 SCC 26, 2 SCR 292 [Hape]. An exception may be made if there is a violation of a binding international human rights obligation: see Canada (Justice) v Khadr, 2008 SCC 28, 2 SCR 125.
38 Hape, supra note 37.
39 US Const amend IV.
40 See SCA, supra note 8 at § 2701; Miller v Meyers, 766 F Supp (2d) 919 (WD Ark 2011).
41 S(MN) v S(JT), 2009 BCSC 661 (available on WL Can).
such as Facebook and MySpace, have internal departments dedicated to handling law enforcement requests and have handbooks available to law enforcement with sample forms and dedicated contact lines. Social networks and internet companies are obliged under American law to release profile information directly to law enforcement once a court order is obtained. With proper authorization, social networks in the US may be compelled to provide law enforcement with subscriber information or with the contents of a user’s account. They may also be mandated to preserve or back up a users’ account when presented with a subpoena or search warrant. Unlike the US, Canada does not require that website operators located in Canada preserve material (when requested) before issuing a search warrant. \(^{42}\) As most social networks are located in the US, law enforcement may send a request to a social network to hold information while they request a search warrant.

**B. Production Orders**

Law enforcement is not granted unlimited access to a subscriber’s account. They are prevented from receiving content information without a valid search order under the US’ SCA and then only if:

the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. \(^{43}\)

Social networks will recognize a foreign subpoena, discussed below, for basic subscriber information, but require foreign officials to directly seek an American issued search warrant.

Access to subscriber records in the US, including the name of the account owner, the account owner’s email address, date of creation, and the IP address used to access the account, requires a court order or an administrative subpoena under section 2703 of the SCA. A production order issued in Canada under section 487.012 of the *Criminal Code* \(^{44}\)

---

42 The Department of Justice has circulated a discussion paper that considers whether preservation orders should be introduced into the Canadian criminal code. Online: <http://www.justice.gc.ca/eng/cons/l-a1/d.html>.

43 *SCA,* supra note 8 at § 2703 (d).

44 *Criminal Code,* RS C 1985, c C-46, s 487.012 [*Criminal Code*].
should suffice for the purpose of the American requirement. When requesting material, a law enforcement agency should be clear on what data they seek and provide the user account number.

The bar for obtaining an order is fairly low in both the US and Canada. For example, regarding the release of confidential government documents by WikiLeaks, a request by Twitter and three of its subscribers to require a higher standard of proof before allowing release of this basic information was denied. A Virginia court found that law enforcement or a government entity must show that the record sought without consent is “relevant and material” to a criminal case and that the “requirement of a higher probable cause standard for non-content information voluntarily released to a third party would needlessly hamper an investigation.”

In the US, a court has found evidence obtained via an emergency request admissible, as subscriber information does not have a high expectation of privacy. Under the SCA there is a provision in the event of an emergency where an individual’s safety may be at stake permitting social networking companies to release information without a court order. The standard in Canada for obtaining a production order is that there are reasonable grounds to believe an offence has been, or is suspected to have been, committed, and that the document will contain evidence respecting the commission of an offence.

Any attempt to find useful information from subscriber records regarding a social networking site will likely require more than one production order to prove an account was created or accessed by an individual. Social networking sites will generally only require an email address to create an account and store an IP address. A second production order will be required from an ISP to match the IP address with a physical address. For instance, in *R v Weavers*, police investigating online threats sent a production order to MySpace to obtain an IP address, and from this IP address they tracked the account to Bell Canada, from whom they

---

45 "MySpace’s International Law Enforcement Guide" (8 July 2008) acknowledges they will accept international subpoenas. This guide is not publicly published, but is available upon request from MySpace.com.

46 *Re 2703(d)*, *supra* note 10.

47 *Sparks*, *supra* note 2 at 4.

48 *US v Beckett*, 2010 WL 776049 (Fla CA 11).

49 *SCA*, *supra* note 8 at § 2702 c (4).

50 *R v Weavers*, 2009 ONCJ 437 (available on WL Can) [*Weavers*].
obtained a physical location. Any attempt to obtain an IP address should note the exact time a user was suspected to log in, as often they are issued temporarily and may be reassigned to other subscribers. Often this information may be used to obtain a physical search warrant for the location.

C. Search Warrants

Content from an American based social network may only be accessed with a valid search warrant based on probable cause and reasonable grounds. Requirements under section 487 of the Criminal Code to issue a search warrant in Canada are similar to those of the US.\(^{51}\) With the exception of good-faith emergency requests, Canadian law enforcement require an enforceable American search warrant. Processing a search warrant is handled by the Canada Mutual Legal Assistance on Criminal Matters Treaty with the United States.\(^{52}\) An investigative request with reasonable grounds and sufficient detail should be provided to the International Assistance Group in the Canadian Department of Justice, the assigned contact for cross-border searches. The International Assistance Group, in turn, works with its US counterpart to obtain the appropriate warrant.\(^{53}\)

Companies such as Facebook have dedicated resources to handle search warrants, and may provide a large amount of personal information, photos, private messages or other information from a user’s account, following a proper request by investigators. Although not a common occurrence, there have been cases where representatives from a social networking company have testified at trial as to the contents of a social networking account.\(^{54}\)

In criminal cases, the ability to access information for the investigative process is limited to law enforcement and the prosecution. The SCA

---

\(^{51}\) Criminal Code, supra note 44.


\(^{54}\) State v Wiley, 68 So (3d) 583 (La App 5 Cir 2011). A MySpace representative appeared on behalf of the prosecution to authenticate an account.
prevents social networking companies from disclosing any content or personal posts or photos to non-governmental entities. American courts appear to reject attempts by defendants to subpoena information directly from a social network. While not binding, a California appellate court in People v Yaqoob denied a subpoena request upon MySpace by the defendant in an attempted rape case on the basis that such a request would violate US federal law.55

Canada’s privacy legislation, PIPEDA, is not as stringent as the SCA, and section 7(3)(c.1) allows companies based in Canada (including internet service providers) to voluntarily release subscriber information or content to a government authority without a search warrant in a police investigation.56 If a company chooses to cooperate, any record may be handed over without the knowledge or consent of the owner.

A defendant in Canada could attempt to compel a witness to provide a copy of their Facebook account under a court-ordered subpoena under section 700(1) of the Criminal Code.57 Although there has been no case law on whether this has been tried, there have been cases where police have obtained records through the consent of a witness. For example, in R v Spackman,58 police obtained chat transcripts from Facebook through the consent of a witness in a murder case, although the court later excluded the chats due to suspicions that the witness was not truthful.

D. Admitting Social Networking Evidence at Trial

While a production order or a search warrant may provide potential evidence, a large body of case law surrounds when social network evidence is admissible. The main considerations are whether the evidence can be authenticated, how it can be used, and whether the evidence proves to be more probative than prejudicial.

55 People v Yaqoob, 2011 WL 264717 (Cal App 4 Dist).
56 PIPEDA, supra note 24. Provision 7(3)(c.1) provides immunity to companies who release information to law enforcement or a government agency to administer or enforce any provincial or national law, as well as if the information relates to national defence or international affairs. The SCA, supra note 8, only permits this in an emergency (see section 2703).
57 Criminal Code, supra note 44, s 700(1). (A witness may be compelled to bring in their own documents).
1. Authentication

In both Canada and the US, evidence such as photographs or documents must be authenticated before they can be admitted. The person introducing evidence must demonstrate to the court that the evidence is the untampered product of the particular person to which the party wishes to attribute authorship. When evidence allegedly comes from a social network and exists electronically, the need to authenticate increases as it becomes easier to manipulate.

Assumptions about who created an account can open the door to defence lawyers and lead to an acquittal. There have been cases where individuals have created fake accounts, or broken into a home network in an attempt to frame their neighbours. In People v Heeter, a woman was convicted of trying to submit a false document to court after she created an account under her partner’s ex-wife’s name and sent fake emails in an attempt to make it look like the woman was harassing her. Most social networking sites are accessed freely and do not require verification that a person creating an account is doing so under their own name.

Even if a social networking site captures an IP address of the user or creator of an account, this information may not be conclusive. For instance, in US v Ardolf, a man was convicted of hacking into his neighbour’s wireless signal in order to send fake threats to politicians and emails that contained child porn. The defendant had used software available online that allowed him to break the password encryption on the router. This was only discovered when the neighbour, a lawyer, had his company’s security expert install a special piece of hardware which allowed him to monitor all computers that accessed his network. Most home network security features are rudimentary and can be bypassed or hacked with some technical knowledge.

In Canada, because the broad language of admissibility provided by the Canada Evidence Act allows authentication by “respect of any standard”, judicial decisions regarding admissibility are not based on rigid traditional rules. In the past, courts relied heavily on the “best evidence rule”, however with modern technology this rule has been rendered obsolete and the question is more about the weight courts should put on

59 People v Heeter, 2010 WL 2992070 (Cal App 2 Dist).
60 US v Ardolf, 2010 WL 3604099 (D Minn).
the evidence.\footnote{John Sopinka, Sidney Lederman & Alan Bryant, \emph{The Law of Evidence in Canada} 3d ed (Markham, ON: LexisNexis Canada Inc. 2009) at 1225. This rule prioritized original copies or works over replications. With electronically stored information, the only way to transfer documents may be to replicate them.} For instance, in \emph{R v Harris},\footnote{\emph{R v Harris}, 2010 PESC 32 (available on WL Can).} a 23-year-old man was convicted of attempting to lure a 14-year-old into having sexual intercourse. The court looked at the totality of evidence to prove that sexually inviting messages were sent from an account operated by the accused. The prosecution presented evidence that the account had the name of accused on it and a picture of his dog. The brother of the accused testified as to the ownership of the account. Some of the messages contained personal details only known to the accused and the victim. Forensic software was run on the accused’s computer to reveal some of the chat transcripts. The defence raised questions about whether someone else may have had access to the computer, but the court found the evidence was sufficient to prove the accused’s own authorship.

Canadian jurisprudence has not discussed in detail whether a minimum level of authentication should exist before social networking evidence is admissible, nor has it analyzed at length the meaning of “any standard”. A number of American decisions however, have provided a clearer picture. These cases are useful in determining how courts in both countries should approach authentication and outline important considerations that should take place before social networking evidence is admitted in a trial.

2. **Expert testimony**

The first consideration when handling social network evidence is to have an expert available who understands how a social networking account is created, or who can testify to the likelihood that a picture has been manipulated. This may be a police officer trained in social networking, or an independent IT consultant. In \emph{People v Beckley},\footnote{\emph{Beckley}, supra note 22 at 2.} a California court, discussing a photograph taken from MySpace and used in a murder trial, emphasized the importance of having an expert able to authenticate the subject matter of a photo if there is not an independent witness to testify to its accuracy. The court also underscored that in the age of computers,
"it does not always take skill, experience, or even cognizance to alter a digital photo." Widely available computer applications such as Adobe Photoshop allow users to manipulate photographs, combine images and remove potentially important details in a way that may be unnoticeable to the average eye.

3. Corroborative evidence

The second consideration is the danger of making assumptions about the author of an email or creator of an account without adequate evidence. It may be unsafe, for example, to rely on the mere fact that an individual owns an account, or that their name or password has been used. In Commonwealth v Purdy the court stated:

Evidence that the defendant's name is written as the author of an e-mail or that the electronic communication originates from an e-mail or a social networking Web site such as Facebook or MySpace that bears the defendant's name is not sufficient alone to authenticate the electronic communication as having been authored or sent by the defendant.

There must be a certain threshold created by a separate "confirming circumstance." This confirmation could be made by way of physical evidence showing the account or files on an individual's computer, or through the manner in which the defendant characterized him or herself. The confirming circumstances can be described in two ways. The first is physical authentication and the second is content-based authentication.

Wherever possible, physical authentication that a suspect created an account should be sought. This may require a physical warrant to search the suspect's computer and may require using some form of software to forensically scan the computer as was done in R v Weavers or Commonwealth v Purdy. Often, a web browser such as Internet Explorer will leave logs on the computer containing remnants of chats or messages. To ensure a conviction, investigators have even gone as far as to make an

64 Ibid.
65 Com v Purdy, 945 NE (2d) 372 at 381 (Mass 2011) [Com].
66 Ibid at 449.
67 Weavers, supra note 50.
68 Com, supra note 65.
arrest when they knew the accused was logged into the account while at work.\textsuperscript{69}

Content-based authentication relies on the specific content of an account or message for personal details or language that may be distinct to a suspect. This can be a highly subjective process and should be used with care. Morris J of a Texas appeal court discussed it in \textit{Tienda v State:}

The inherent nature of social networking websites encourages members who choose to use pseudonyms to identify themselves by posting profile pictures or descriptions of their physical appearances, personal backgrounds, and lifestyles. This type of individualization is significant in authenticating a particular profile page as having been created by the person depicted in it. The more particular and individualized the information, the greater the support for a reasonable juror’s finding that the person depicted supplied the information.\textsuperscript{70}

The court found that references to events surrounding a murder and posts describing the accused being put on an electronic monitoring program provided sufficient information for a jury to decide whether the account belonged to the accused.

The presence of information that could be known only to the accused or victim may be sufficient to at least provide authentication of evidence for the purpose of admissibility. The trier of fact will still need to decide whether this is conclusive. A number of opinions demonstrate how courts have admitted evidence based on distinctive circumstantial details. In \textit{People v Fielding},\textsuperscript{71} the court found that chat transcripts containing information the accused and victim discussed in person provided sufficient proximity to allow the transcripts to be introduced. Any alleged discrepancies were to go to the weight, or importance, placed on them. In \textit{People v Goins},\textsuperscript{72} the appeals court found the trial judge wrongly excluded a MySpace page that could only have been known to the victim and accused. The defendant had wished to introduce it and the appeals court recognized that it contained “descriptive details of the assault that fit within what a reasonable person would consider to be distinctive content.”\textsuperscript{73}

\begin{footnotesize}
\textsuperscript{69} R v McCall, 2011 BCPC 7 at 13 (available on WL Can).
\textsuperscript{70} Tienda v State, 2010 WL 5129722 (Tex App-Dallas) at 5.
\textsuperscript{71} People v Fielding, 2010 WL 2473344 (Cal App 3 Dist).
\textsuperscript{72} People v Goins, 2010 WL 199602 (Mich App).
\textsuperscript{73} Ibid at 2.
\end{footnotesize}
4. Importance of proper authentication

The importance of corroborative evidence and proper authentication should not be understated. Basic content such as a photograph of an accused or a basic profile are insufficient; they leave the door open for reasonable doubt. In the US, a number of cases have been overturned because of the role speculation played.

In Griffin v State, the Maryland Court of Appeal overturned a murder conviction because a trial court allowed a MySpace account to be admitted without authenticating it.\(^4\) The lead investigator printed out a copy of the profile that they assumed belonged to the girlfriend of the suspect and tried to use the photo of the girlfriend and her birth date as authentication. The court ruled that the police should have attempted to introduce more confirming evidence such as cookies or physical authentication.

Shared computers can also raise problems. In R v Johnson,\(^5\) the Ontario Superior Court found the accused not guilty of sexual trafficking in part because there were questions about whether it was the accused or his girlfriend who was accessing and posting to a Facebook account. In any case where key evidence exists as a result of online activities, law enforcement will need to collect sufficient evidence to infer that the accused was in fact the user of the computer. Many web browsers save passwords on a computer so that anyone with physical access to a computer may log onto an account and make posts without the consent of the user. This is particularly problematic in offices, where a computer may be in an unsecure environment, or in a residence, where parents, roommates or children may have access to the same computer.

Where possible, enough confirming evidence should be gathered to ensure the judge or jury can infer that there is no reasonable doubt or alternative explanation as to who created or used a particular social networking account.

5. Determining admissibility

When a criminal court is dealing with social networking evidence, they are primarily dealing with either incriminating statements or with photographs that reveal some insight into the crime. With the

\(^4\) Griffin v State, 19 A (3d) 415 (Md App 2011).

\(^5\) R v Johnson, 2011 ONSC 195 (available on WL Can).
prosecution, the court will usually undertake the weighing exercise from R v Seaboyer\textsuperscript{76} as to whether the evidence is more probative than prejudicial (which serves to prevent inflammatory statements or embarrassing photographs from distracting the court). When the defence attempts to bring in social networking evidence, the main issue is whether the evidence is relevant and probative and whether there are any rules barring the particular nature of the questioning related to the evidence.

6. Challenging the credibility of witnesses

Attempts by the defence to introduce social networking evidence occur most often in cases involving sexual assault, to speak to the credibility of the complainant. It also occasionally arises in cases where the accused claims self-defence.

In sexual assault cases, courts in Canada are constrained by Section 277 of the Criminal Code that limits "evidence of sexual reputation, whether general or specific" concerning the complainant.\textsuperscript{77} Similar rules requiring the exclusion of any evidence of past sexual conduct exist in the US. For example, in the unreported decision People v Greenspan,\textsuperscript{78} the court denied a request by the defence to introduce Facebook photos of the complainant posing in a sexually suggestive manner. In State v Corwin,\textsuperscript{79} the court prevented the defence from introducing Facebook posts by the complainant in which she bragged about getting drunk and waking up with bruises.

Similar limitations may occur in general assault cases. In R v Jilg,\textsuperscript{80} the British Columbia Supreme Court did not allow the defendant to introduce photographs from the complainant’s Facebook page to challenge her testimony as to the extent of her injuries from his assault at his sentence appeal. The defendant had wished to use Facebook posts from after the incident to minimize the severity of the injuries. The court found the evidence was not probative of the danger the accused presented to society. In State v Makue,\textsuperscript{81} a Hawaiian court found that a MySpace

\textsuperscript{76} [1991] 2 SCR 577, 83 DLR (4th) 193.
\textsuperscript{77} Criminal Code, supra 44, s 277.
\textsuperscript{78} People v Greenspan, 2011 WL 809552 (Cal App 4 Dist).
\textsuperscript{79} State v Corwin, 295 SW (3d) 572 (Mo App SD 2009).
\textsuperscript{80} R v Jilg, 2010 BCSC 1476 (available on WL Can).
\textsuperscript{81} State v Makue, 2011 WL 988560 (Hawaii App).
photo of a victim holding a beer had no relevance to whether the complainant was credible when he testified he was not drinking on the day. There was no evidence that the photograph was taken on the day of the assault. In a murder case, People v Mills, 82 the court prevented the defence from introducing MySpace photos of the victim holding a firearm in making its case for self-defence, since there was no evidence that the defendant was aware of the photograph.

Courts have allowed the defence to introduce Facebook profile evidence where there is particular relevance to the credibility of a witness or to the defendant's perception of the events. In R v Garaway, 83 the defence was permitted to introduce evidence that a 13-year-old complainant in a sexual interference case had lied about her age by listing it as 18 on her Facebook profile. An Ontario court acquitted the defendant, finding a reasonable doubt as to whether the accused ought to have known the girl's age. Similarly, an appellate court in the US overturned a conviction for statutory rape of a youth under 14. The trial judge did not permit the jury to consider applying a lesser charge after the complainant listed her age as 15 on her MySpace account. 84

As with all evidence, any attempt to challenge the credibility of a witness or a complainant using social networking photographs or statements should be done while the witness is on the stand. 85 In R v Gardiner, 86 a New Brunswick trial judge refused to allow the defence to introduce a witness to testify that the complainant admitted to perjuring herself in phone conversation and corroborating Facebook messages because they did not fully raise the issue while the complainant was testifying. Fortunately for the accused, the Court of Appeal overturned the case on the basis that Mr. Gardiner was ineffectively defended.

It is common for the prosecution to challenge the credibility of a defendant who chooses to testify by using their social networking profile. As with all character evidence, this should not be used on its own, but

---

82 People v Mills, 2011 WL 1086559 (Mich App). (At 13, the court notes that if the accused had been aware of the photograph, it would have been admissible to establish a reasonable apprehension of harm).
83 R v Garaway, 2010 ONCJ 642 (available on WL Can).
84 State v Berry, 238 Or App 277 (Or App 2010).
85 The rule in Broune v Dunn (1893) 6 R 67 HL.
used to rebut the credibility of an accused if they choose to testify.\textsuperscript{87} For example, in \textit{R v Telford},\textsuperscript{88} an accused man’s Facebook message to his girlfriend, “I bet you don’t want me to see you again,” was used to challenge the credibility of his version of events in which he denied assaulting her. Furthermore, some courts in the US have allowed evidence that is highly prejudicial, and otherwise inadmissible, when a defendant testifies about their own character. In \textit{Hall v State},\textsuperscript{89} the court allowed the prosecution to question a woman charged with obstructing justice about her Facebook profile. She claimed she was an unwilling participant in disposing a body and the prosecution pointed out that she listed a number of horror movies and novels amongst her interests and that her summer plans included, “I should really be more of a horrific person. It’s in the works.”[sic]\textsuperscript{90} Likewise, a court in Indiana allowed the prosecution to question a father who was accused of murdering his child on statements made on his MySpace profile.\textsuperscript{91} In those statements, he claimed to be an outlaw who was able to “do it and get away”. The father, who admitted to violently assaulting his daughter, attempted to claim on the stand that he was reckless and should be tried with manslaughter instead of murder. The court found that since the father made his character a central issue by testifying, evidence of his past statements on his profile were admissible, whereas evidence of past criminal actions would not have been.

7. **Probative value versus prejudicial effect**

For courts determining whether to admit potentially incriminating social network evidence, one of the central concerns is ensuring that inflammatory material with little relation to the matter at hand is not considered. The judge must decide whether material genuinely is probative, and whether it will potentially introduce prejudice. Fairness and integrity of the legal system require that sufficient proof be presented and necessitates that immature statements or inappropriate pictures do not create any preconceptions of guilt. Even in a case tried without a jury, the

\begin{itemize}
  \item Paul Atkinson, \textit{Proof: Canadian Rules of Evidence} (Markham, Ont: LexisNexis, 2007) at 64.
  \item \textit{R v Telford}, 2009 ONCJ 174 (available on WL Can).
  \item \textit{Hall v State}, 283 SW (3d) 137 (Tex App-Austin 2009).
  \item \textit{Ibid} at 149.
  \item \textit{Clark v State}, 915 NE (2d) 126 (Ind SC 2009).
\end{itemize}
judge should avoid any misleading character evidence unless it is deemed essential to the facts of the case. This is important based on the nature of social networking.

Users of Facebook or MySpace often engage in behaviour that may be considered ridiculous by traditional societal standards: posting lewd pictures, bragging about how intoxicated an individual has become, making generally impulsive statements, or even making false or highly exaggerated claims regarding their behaviour. However, with the exception of some family law cases where one’s behaviour may be applicable to their ability to raise children, it is generally not the court or jury’s role to become the judge of appropriate taste.

When admitting social networking profiles and pages, a judge may determine that to maintain fairness, some or all posts or photos should be excluded and that potential evidence must be shown in a particular way. In *R v Sinclair*, the accused in an Ontario murder trial wanted to demonstrate that one of the prosecution’s witnesses and the accused were in a gang by showing a rap video downloaded from YouTube.92 O’Marra J ruled that the violent music and lyrics would be overly prejudicial, but allowed the admissibility of still photos captured from the video to challenge the whether the witness was in a gang with the deceased:

The YouTube tribute video is not evidence of reputation or proof of previous acts of violence. There is no probative value to it to prove a disposition for violence on the part of the deceased capable of supporting the probability that the deceased was the aggressor. However, the defendant should not be prevented from making use of the above described photographs depicted in the video in cross-examination.93

Similarly, a Texas Court admitted a MySpace video in a murder trial of the accused brandishing a firearm because it found the video probative, but did not permit the audio.94 An appeal court reviewing the decision found that while a video showing a suspect with a firearm sometime before a crime may be prejudicial and inadmissible on its own, it had probative value because a witness testified the defendant used the same handgun used in the shooting and it demonstrated that the defendant had access to the specific firearm. In contrast, a Georgia court found that a YouTube

---

92 *Sinclair*, *supra* note 19.
93 *Ibid* at para 82.
video with violent lyrics about gang lifestyle written by an acquaintance of a suspect was not admissible as it was both hearsay and unfairly prejudicial.\textsuperscript{95}

Courts have been reluctant to admit photographs from a suspect's social networking profile unless they have a highly probative value. Generally, they are considered inadmissible character evidence. In US \textit{v} Phaknikone,\textsuperscript{96} an appeals court found that photographs from a MySpace profile under the user name "trigga" of an accused brandishing a firearm was highly prejudicial and not probative of whether an accused robbed a bank. It was not relevant to any detail from the robbery and thus wrongfully admitted. The appeal court also outlined the evidentiary test for admissibility of evidence in a US federal court:

First, the evidence must be relevant to an issue other than the defendant's character. Second, as part of the relevance analysis, there must be sufficient proof so that a jury could find that the defendant committed the extrinsic act. Third, the probative value of the evidence must not be "substantially outweighed by its undue prejudice."\textsuperscript{97}

Prejudicial evidence may be admissible in certain circumstances. In US \textit{v} Drummond,\textsuperscript{98} a court did not allow the prosecution to admit photographs from MySpace of an accused drug dealer posing with large amounts of cash and a gun. This was despite the accused having no job or legal income source. The court found that it would be prejudicial for a jury to convict him because he looked like a drug dealer. However, the court stated that if the prosecution could find witnesses to testify that the accused had large amounts of cash and the defendant denied this, then "it is possible that the relevance of the photos could outweigh any unfair prejudice."\textsuperscript{99} The probative value of evidence increases when the defendant takes the stand and provides contradictory testimony.

On the other hand, social networking photographs or profiles can be highly probative. In R \textit{v} S(MC), Facebook pictures played a strong role in an attempted murder conviction.\textsuperscript{100} The youth, who had a troubled past,

\begin{footnotes}
\item[95] US \textit{v} Gamory, 635 F (3d) 480 (CA 11 Ga 2011).
\item[96] US \textit{v} Phaknikone, 605 F (3d) 1099 (CA 11 Ga 2010).
\item[97] Ibid at 1107.
\item[98] US \textit{v} Drummond, 2010 WL 1329059 (MD Pa).
\item[99] Ibid at 2.
\item[100] R \textit{v} S(MC), 2010 NSPC 26 (available on WL Can) [S(MC)].
\end{footnotes}
depicted himself on his Facebook as "SoulJa" and his chosen profile picture depicted him wearing a hat and with a bandana over his face. Judge Campbell found this to be very relevant:

The person who shot Michael Patriquen was a black male wearing a camouflage bandana covering his face and a dark baseball cap pulled down to his eyes. That description bears a striking similarity to the pictures of M.C.S. posted on Facebook, where he is described as S.\(^{101}\)

The profile picture complemented other circumstantial evidence from Facebook. The suspect's nickname on Facebook matched messages found on a cell phone in a stolen vehicle recovered nearby (which belonged to the suspect's grandfather). Other Facebook evidence showed that a jacket worn in the shooting and found in the vehicle was the same as one the defendant wore in other pictures he uploaded to Facebook. The judge's statements demonstrate that even a prejudicial photograph may sometimes be sufficiently probative to justify admission.

Even highly prejudicial or inflammatory photos may occasionally have a legitimate purpose. In *Williamson v State*, an appeal court affirmed the admission of photographs of the accused in an assault and robbery case committed by a gang of youths, finding the photos relevant in showing the girls acted in concert with each other.\(^{102}\) Although the court recognized that even relevant photographs should be excluded if they are overly prejudicial, the court held that:

> The mere fact that a photograph is inflammatory or cumulative is not, standing alone, sufficient reason to exclude it. [...] Even the most gruesome photographs may be admissible if they assist the trier of fact by shedding light on some issue, proving a necessary element of the case, enabling a witness to testify more effectively, corroborating testimony, or enabling jurors to better understand the testimony.\(^{103}\)

8. **Determining weight and context of evidence**

While it is up to the judge to determine whether evidence can be admitted or not in a criminal proceeding, it is up to the trier of fact to assess the weight or believability of the evidence. Courts should acknowledge that statements individuals make on an online chat forum or when posting to a social network have a greater likelihood of being

---

\(^{101}\) *Ibid* at para 87.
\(^{103}\) *Ibid* at 15.
exaggerated or untrue. Anonymous individuals may post things that they would not say in person, or they may be attempting to brag to their online friends. Furthermore, a post, image, video or message may be unclear, reveal only part of a story, or be taken out of context.

Nevertheless, some Canadian courts have assumed that incriminating statements made online are truthful. In *R v Tscherkassow*, a man’s conviction of assault at a gay bar was secured through an eyewitness account and with the accused’s own self-incriminating statement on Facebook.104 A prosecution witness testified that the accused bragged about “supermanning a fag or a fairy”105 in one of his status updates. The judge rejected the accused’s claim that he lied, determining that “[c]ommon sense and reasonableness suggest that one would not post such a statement for those reasons where the statement is untrue.”106

Similarly, in a tax dispute case, a court rejected a salon worker’s contention that his employment history contained inaccurate information:

Mr. Hall described himself on Facebook as a self-employed hair colour specialist. Everything else about him on his Facebook info page he says is true. This is his own description of his work status made voluntarily, describing his work during the period he worked at the appellant’s salon. It was made in a setting where nothing seemed to turn on it. Though he now says it alone was untrue and dishonest, he cannot explain why this would be the one thing he would choose to lie about on Facebook regarding his personal information.107

Other courts have approached incriminating social networking statements with a more skeptical approach, realizing that there is a need to evaluate the context of a post. This has surfaced in cases where individuals are accused of making threats and contend they were blowing off anger and frustration. In *R v Lee*,108 the defendant was acquitted of making death threats. The judge was unsure of the context of certain statements and remarked that the format of Facebook “diminishes the seriousness that can be attached to the words.”109 In *R v Sather*, the judge recognized an expert witness who testified:

104  *R v Tscherkassow*, 2010 ABPC 324 (available on WL Can).
105  Ibid at para 67.
106  Ibid at para 136.
107  Shonn’s Makeovers & Spa v Minister of National Revenue, 2010 TCC 542 at para 27 (available on WL Can).
108  *R v Lee*, 2010 ONCJ 291 (available on WL Can) [Lee].
109  Ibid at para 9.
...people who profile themselves embellish their character. They deliberately say provocative things to elicit a response from their Facebook "friends". In a sense they construct an alternate persona.\textsuperscript{110}

Even if an individual's posts are genuine and serious, courts should be cautious when it comes to understanding the context of videos, photographs, posts, and messages.

In \textit{R v Huber},\textsuperscript{111} a judge downplayed a video posted on YouTube because of its limited context. This case became notorious after the video of a black man fending off three white attackers in a small British Columbia community became widespread. The judge warned of the limited weight that often should be put on videos posted online:

But the YouTube segment is misleading. To view it out of context is akin to walking into the middle of a movie. At that stage, characters have already formed, the storyline established, and the plot well along. So it is in the case at Bar.\textsuperscript{112}

Statements themselves or messages must also ensure they are put in an appropriate context. Text messages or private communications can be challenging. In \textit{R v P(N)},\textsuperscript{113} a judge dealing with a sexual interference case between a female care giver and an underage male, acknowledged the difficulty of applying a strict legal framework to personal communications:

Having done so I conclude that drawing inferences from any of this material, for or against the positions of the Crown or the defence in this case would ultimately involve me in a process of interpretive speculation. I elect not to go there. I attach no weight to this material apart from supplying interesting context.\textsuperscript{114}

Particularly in a criminal trial, it is important that speculation be avoided and appropriate weight be placed on communications. In \textit{R v Anderson},\textsuperscript{115} a Prince Edward Island appeal court overturned a criminal conviction of a female soccer coach who was accused of sexually exploiting a former player. The trial judge concluded that messages between the coach and the player were evidence of an inappropriate relationship. However, the appeal court found that the judge overlooked evidence that

\begin{thebibliography}{9}
\bibitem{sather} \textit{R v Sather}, 2008 ONCJ 98 at para 9 (available on WL Can) [Sather].
\bibitem{huber} \textit{R v Huber}, 2010 BCPC 347 (available on WL Can).
\bibitem{ibid} \textit{Ibid} at para 4.
\bibitem{pn} \textit{R v P(N)}, 2010 ONSC 3184 (available on WL Can).
\bibitem{ibid2} \textit{Ibid} at para 63.
\bibitem{anderson} \textit{R v Anderson}, 2009 PECA 4 (available on WL Can).
\end{thebibliography}
showed that communications between the complainant and other coaches and players contained similar language and that "the messages were nothing more than adolescent chatter."\textsuperscript{116}

E. Use of Social Networking Evidence

1. \textit{General incriminating evidence}

Often, as discussed above in S(MC),\textsuperscript{117} photographs from Facebook may be used to connect an individual to clothing worn at a crime. In a case yet to go to trial, investigators identified an alleged bank robber after matching clothing worn in the robbery to clothing the suspect wore on his Facebook account.\textsuperscript{118} Occasionally, a Facebook profile picture may even serve to raise suspicion about ongoing illicit activities. In \textit{R v Huxford},\textsuperscript{119} an Ontario detective noticed a convicted felon who was not registered to own a firearm had posted a profile picture of himself holding a handgun. The detective sent a friend request, arranged to sell the felon a firearm and proceeded to arrest him when they met.

Facebook evidence has been used in gaining authorization for search warrants. In \textit{US v McNamara-Harvey},\textsuperscript{120} a Pennsylvania court authorized searching the laptop of a man suspected of domestic terrorism, based in part on anti-Israel comments he made along with threats about starting a riot. In one Canadian case,\textsuperscript{121} evidence was excluded after police reported a suspect in a robbery was wearing the same bandana in a Facebook photo as was worn during a robbery in order to obtain a warrant. On review, the witnesses' descriptions of the colour and the Facebook photo were inconsistent.

In both Canada and the US, social networking photographs have been used in civil seizures related to criminal activity. For example, in Nova Scotia a court ordered a house suspected of being used for drug trafficking

\textsuperscript{116} \textit{Ibid} at para 84.
\textsuperscript{117} S(MC), supra note 100.
\textsuperscript{119} \textit{R v Huxford}, 2010 ONCJ 33 (available on WL Can).
\textsuperscript{120} \textit{US v McNamara-Harvey}, 2010 WL 3928529 (ED Pa).
\textsuperscript{121} \textit{R v Morgan}, 2010 ONSC 4258 (available on WL Can).
closed. Pictures of the owner posing with gang symbols and Facebook posts referring to a local gang were admitted as evidence that the house was posing a threat to community safety. A New York Court ordered a car belonging to the father of a convicted drug dealer seized after extensive photos of the son driving the car were admitted from the son's Facebook account and the court concluded that the car belonged to the father in title only.

Savvy investigators may choose to go onto a social network such as Facebook or Twitter and search for posts with incriminating words. Some websites like Twitter allow users to extensively search all posts, many of which are public. An investigator may also use social networks to track down potential associates of a known individual by viewing their 'friends list'. Individuals on the lam have been caught after posting photographs taken from the locations where they were staying. They can be apprehended after checking their Facebook account after a production order had been issued to release the IP address where the account was last logged on. Those with privacy settings enabled may be safe from amateur sleuths, but they will not be safe from their own 'friends' or from a valid and enforceable search order.

2. Alibis and alternative explanations

Defendants have used photographs to create an alibi or raise reasonable doubt by introducing social networking evidence to their advantage. In R v Lorette, a defendant accused of inappropriately touching a random woman in a bank was acquitted of sexual assault. He successfully argued that he had mistaken the woman for a former girlfriend after introducing Facebook photographs of a woman who resembled the complainant. In R v E(SR) a man convicted of robbery mitigated his sentence slightly by using pictures from his Facebook account to show that some of the allegedly stolen jewelry was in his possession prior to the theft.

---

122 Nova Scotia (Director of Public Safety) v Dixon, 2011 NSSC 5, 297 NSR (2d) 337.
124 R v Lorette, 2010 ONCJ 259 (available on WL Can).
125 R v E (SR), 2010 SKPC 145 (available on WL Can).
3. **Incriminating association**

Frequently, photographs or videos of individuals making gang hand-signs or posing with other gang members have been introduced to complement other evidence. In *US v Cole*,\(^{126}\) a Texas court admitted the defendant's MySpace profile which showed him wearing gang colours and listing 'drug wars' as an interest. This was used to demonstrate that he was aware of a drug conspiracy rather than being an outside contractor working as a security guard like he claimed. In *US v Sirianni-Navarro*,\(^{127}\) a court ordered a wife of a suspected drug dealer to be detained on the basis that she had photos of her husband with large amounts of cash on her Facebook page and thus likely was a knowing participant in his trafficking. In *Lawrence v State*,\(^{128}\) photographs of the defendant from his MySpace account showing him with gang tattoos and appearing with other members of a gang were raised as an aggravating factor in sentencing. In an attempted murder conviction, a California court admitted a video from the accused's MySpace page in which the man rapped about his rivalry with another gang who he was accused of attacking. This was used to corroborate a witness's account.\(^{129}\) In a robbery conviction, an Ohio court admitted MySpace posts in which the defendant bragged about being in a gang.\(^{130}\) Since being a member of a street gang is illegal in some states, courts have blurred the lines around character evidence admitting otherwise prejudicial videos from YouTube and MySpace to demonstrate gang affiliation.

4. **Incriminating messages**

While some self-incriminating evidence is derived from the desire to share photographs or profile information, social networks are also becoming a ubiquitous means of communication. As a result, such communications are increasingly being used in criminal trials. In *R v Todorovic*,\(^{131}\) Facebook messages in which a teenage girl expressed to her boyfriend that she wanted another girl killed were used to convict her of

---

\(^{129}\) *Ibarra v McDonald*, 2011 WL 1585559 (ND Cal).
\(^{130}\) *State v Cole*, 2010 Ohio 1840 (Ohio App 5 Dist).
\(^{131}\) *R v Todorovic*, 2009 CarswellOnt 9949 (WL Can).
being a party to the murder. In sentencing, the judge noted that the messages were strong evidence:

What would, in another age, have shown up in personal notes exchanged between intimates, nowadays finds itself digitally recorded in cyberspace. The words, and their impact, are no less real, however.\textsuperscript{132}

Even apologies made over a social network may be used as evidence. In \textit{R v F (KR)},\textsuperscript{133} the court determined an apology found in a message from a 17 year old to a 10-year-old girl was indicative of guilt in a sexual assault case. Similarly, in \textit{R v G (R)},\textsuperscript{134} the court found a father’s Facebook chat message asking if he should “go away, forever” and his failure to deny his daughter’s allegation of molestation was evidence of guilt.

\textbf{5. Threats and harassment}

Courts increasingly have to deal with threats and harassment committed on social networking sites. The challenge is determining what is criminal as opposed to what may simply be disturbing or inappropriate. As discussed above, the courts in \textit{Sather}\textsuperscript{135} and \textit{Lee}\textsuperscript{136} acquitted two men whose rants were made on their own Facebook accounts. In \textit{Lee}, the accused did not direct his comments towards any individual, while with \textit{Sather} there was reasonable doubt about the seriousness of the threats and whether they met the legal test: the accused “must intend the words to instil fear or intimidate.”\textsuperscript{137} Sather had made comments referring to a “tactical strike” when discussing the Children’s Aid Society preventing him from having custody of his child. Despite this, the court found that he never intended to communicate them with any of the staff and thus did not mean to intimidate.

Courts consider evidence differently if posted on an open social network or video-sharing site such as YouTube. In \textit{R v B(R)},\textsuperscript{138} two youths in Ontario were convicted of public mischief after posting a video threatening the President of the United States as a prank. They were

\begin{itemize}
\item \textsuperscript{132} \textit{Ibid} at para 25.
\item \textsuperscript{133} \textit{R v F(KR)}, 2011 NLCA 2, 304 Nfld & PEIR 171.
\item \textsuperscript{134} \textit{R v G(R)}, 2010 ONSC 2157 (available on WL Can).
\item \textsuperscript{135} \textit{Sather, supra}, note 110.
\item \textsuperscript{136} \textit{Lee, supra} note 108.
\item \textsuperscript{137} \textit{Sather, supra}, note 110 at para 8.
\item \textsuperscript{138} \textit{R v B(R), supra} note 18.
\end{itemize}
fortunate in that the judge gave them a conditional discharge with community service and a limited internet ban. In the US, courts have been far less lenient, particularly where the subject has a criminal record or appears with firearms. An American court sentenced a convicted felon to 79 months in jail after he recorded a drunken video depicting him with automatic firearms making threats against law enforcement officials and posted it to his MySpace account.\(^{139}\)

In addition, American courts appear more likely to convict individuals if they make an attempt to communicate a threatening post in an email or draw attention to it by providing a link. In *US v Jeffries*,\(^{140}\) a man was convicted of making threats after recording a song in which he sang about killing a judge and posting it on YouTube and Facebook. In referencing the public nature of the post, the judge remarked:

...it is reasonably foreseeable that some persons would be concerned by the content of the Defendant’s song and statements and the serious and angry way in which he delivered them and would report the matter to some authority, law enforcement entity, or court official, such as actually happened in this case. If the Defendant shouted his message to a crowd of people who had knowledge about the circumstances of his custody dispute, like his sister and potentially her friends on Facebook, the likelihood that someone would report the threat only increases.\(^{141}\)

In *People v Costales*,\(^{142}\) Costales argued that threats towards an entertainer on Costales’ MySpace account were never intended to be communicated. The court rejected this argument; Costales had sent emails to the singer with links to the webpage where the threats were made.

In addition to direct threats, online harassment on social networks is becoming increasingly common. In *Placanica v State*,\(^{143}\) a Georgia court found a man guilty of harassment after attempting to repeatedly contact a sixteen-year old girl after she had ended their relationship. Online threats and harassment made by those with underlying mental illnesses are also becoming a problem. The Ontario Consent and Capacity Board routinely hospitalizes individuals with clear mental disorders who post death

---

140 *US v Jeffries*, 2011 WL 613354 (ED Tenn) [Jeffries].
141 *Ibid* at 10.
142 *People v Costales*, 2010 WL 2044637 (Cal App 2 Dist).
143 *Placanica v State*, 693 SE (2d) 571 (Ga App 2010).
threats or send threatening emails. Another common form of harassment is creating fake accounts for the purpose of impersonation, although courts do draw a line between creating a website for satire or mockery and actions intended to cause real harm. In *Clear v Superior Court*, a Californian court found a man guilty of false personation after he created a fake MySpace account for a pastor and made lewd statements. The court found that while it was not illegal to make a fake account, doing so for the purpose of sending embarrassing messages to get the pastor fired was a felony. A similar case in Canada, involving a group of unknown individuals creating a fake account under a juvenile’s name to discuss her sexual activities, will be discussed further below.

6. *Sentencing*

A court may consider social networking evidence in determining sentencing. At this stage of the criminal process, the concern becomes evaluating a person’s character to determine the likelihood of reoffending and necessary deterrents. In *Smith*, the judge found the ‘arrogantly sinister gangster’ image a youth presented on his Facebook account a factor in his decision to give that youth an adult sentence.

Social networking and online conduct may directly relate to the crime. In *R v Desilva*, a judge found a man’s decision to upload a sex video of his partner onto Facebook was an aggravating factor necessitating a more severe sentence. Although the court recognized that the man quickly removed the video when contacted by police, Judge Robertson remarked:

In addition to the deterrence to the accused, this offence is one where general deterrence plays an enhanced role. With the proliferation of social networking sites, the opportunity to misuse such sites is significant and with devastating results to the victims; many of the impacts are significant and long lasting. This is

---

144 *Re F(J)*, 2010 CarswellOnt 8100; *Re F(K)*, 2010 CarswellOnt 7835 (WL Can) (ON CCB).

145 *Re F(K)*, *ibid*; *Re F(J)*, *ibid*; *Re H(T)*, 2010 CarswellOnt 9036 (WL Can) (ON CCB).

146 *Clear v Superior Court*, 2010 WL 2029016 (Cal App 4 Dist).

147 *AB v Bragg Communications Inc*, 2010 NSSC 215, 293 NSR (2d) 222 [AB]. See section V(0)(1) of this paper, infra.

148 *S(MC)*, supra note 100.

149 *R v Desilva*, 2011 ONCJ 133 (available on WL Can).
one of those rare cases where general deterrence may actually play an enhanced and meaningful role in sentencing. 150

In sexual solicitation cases, the courts have been equally ready to condemn deviant social networking behaviour. In R v H (II), 151 the judge harshly scolded a 23-year-old man whose Facebook conversation with his 14-year-old foster sister indicated an intention to meet for sexual intercourse. While the accused contended he was not planning to follow through on their illicit chats, the sentencing judge remarked that, "While J.J.H. was not trolling the net, he utilized the net like a dog with a bone once the opportunity presented itself." 152

Social networking evidence can play a role in determining whether a convict is obeying the terms of their probation. One of the primary roles of sentencing is to assist in rehabilitating the offender. For instance, ordering a sex offender not to access the internet or to refrain from using social networks are often mandatory conditions of their release. A probation officer may choose to monitor Facebook or other social networks to ensure their clients are not violating their conditions. 153 This may involve looking at known associates' friend lists in case a parolee creates an account under a different last name or an alias.

Of course, not all criminals are that savvy. In Hawkins v State, 154 a man convicted of indecency with a child was placed on deferred adjudication for eight years in which he was forbidden from using the internet. He was caught breaching his conditions and his probation was revoked after he contacted his probation supervisor on Facebook.

Individuals with alcohol bans and driving prohibitions who maintain a social networking account put themselves at risk if they post incriminating pictures of themselves online. In revoking probation for a woman convicted of killing a passenger in a drunk driving accident, a Connecticut court reviewed evidence taken from her social networking account. While her initial parole violation was driving without a license,

150 Ibid at para 52.
151 R v H (II), 2011 PESC 8, 308 Nfld & PEIR 252.
152 Ibid at 35.
153 See e.g. In re Ronald A, 2010 WL 445468 (Ariz App Div I) where a probationary officer discovered the creation of a Facebook page contrary to probationary orders.
the court allowed the prosecution to admit photographs of the woman drinking and attending parties to demonstrate that:

the beneficial aspects of probation were not being served because the defendant was engaging in many of the same activities post-incarceration as she engaged in before being incarcerated.\(^{155}\)

In another case, a man’s parole was revoked when Facebook pictures of him drinking and smoking marijuana were used to demonstrate that he broke the strict terms of his vehicular manslaughter probation.\(^{156}\) The court found that while a high evidentiary standard may still be needed to prove a breach of conditions, once a breach has been proven the state only needed to show "some indicia of reliability to support its claims."\(^{157}\)

When composing sentences or no-contact orders, courts should be mindful of the exact terms of the order. While it is common for a court to order a person convicted of a crime to avoid contact with the victim, a court may also need to determine whether it is necessary to broaden the scope of the order. In *People v Wente*,\(^{158}\) a court found that a man contacting his ex-wife’s friends through Facebook did not breach his “no contact” order, as the terms were not specific. The court recognized the need to be very clear when drafting orders in the age of social networks: “Changes in technology, including the way people communicate, continue to present unique challenges to the courts.”\(^{159}\)

F. Social Networking and Juries

Ensuring a fair and balanced trial requires the screening of evidence for possible prejudice before its presentation to the jury. However, it is equally important that jury members themselves do not use social networks in a way that creates a perception of unfairness. In Canada, the courts have found the presence of social networks on their own does not necessarily infer a jury will be prejudicial. In *R v Maguire*,\(^{160}\) Coughlan J rejected the defence’s request to have a first-degree murder trial conducted

\(^{155}\) *State v Altajir*, 2 A (3d) 1024at 684 (Conn App 2010); aff’d by 33 A (3d) 193 (Conn 2012) [Altajir].

\(^{156}\) *People v Gittens*, 2010 WL 3246177 (Cal App 2 Dist) (unpublished).

\(^{157}\) Altajir, supra note 155 at 689.

\(^{158}\) *People v Welte*, 920 NYS (2d) 627 (NY Just Cr 2011).

\(^{159}\) Ibid at 629.

\(^{160}\) *R v Maguire*, 2010 NSSC 200, 293 NSR (2d) 33.
by judge alone based solely on fears of jury prejudice because of the proliferation of online discussion. Even though there were a number of Facebook groups and online forums set up to discuss the alleged murder, the judge found that the presence of social networking groups "[did] not show a general prejudicial attitude in the community as a whole so as to justify a change in venue."\footnote{Ibid at para 31.} However, the judge did recognize that it was a potential issue to address during the jury selection process.\footnote{Ibid at para 28.}

Additionally, there have been cases where jurors have been caught abusing social networks. Whether the breach is serious depends on the circumstance. A West Virginia police officer accused of financial improprieties had his conviction overturned when it became known that a juror had added him as a friend.\footnote{State v Dellinger, 225 WVa 736, 696 SE (2d) 38, 2010 WL 2243511 (W Va).} A civil trial verdict was overturned when it was discovered that the head juror’s Facebook account mentioned that he was a relative of a former employee of one of the parties.\footnote{AG Equipment Co v AIG Life, 2011 WL 888266 (N DA).} However, in \textit{People v Rios}, a judge refused to order a mistrial based solely on a juror sending a friend request to a witness, particularly since the witness did not accept the request.\footnote{People v Rios, 26 Misc (3d) 1225(A) (NY Sup 2010).} Another court rejected an appeal of a murder conviction which was based on a juror mentioning online that they had been selected for jury duty without discussing the case.\footnote{State v White, 2011-Ohio-2364, 2011 WL 1988324 (Ohio App. 10 Dist 2011).}

\section*{V. Civil Proceedings}

The focus in civil proceedings is on understanding the consequence of relationships between individuals or entities, rather than expressly proving wrongdoing. Courts often have to resolve conflicts regarding what information should be disclosed and what should remain private. Once both sides have the evidence, the court then determines whether an injury occurred and what the appropriate damages should be. Consequently, in civil trials, issues regarding social networking evidence usually involve determining relevancy and discoverability.
The relevance of social networking evidence in the context of a civil proceeding depends on the issues in dispute. In cases of defamation, the challenge with social media is often uncovering anonymous individuals hiding behind fake profiles. In personal injury cases, courts ensure a plaintiff has provided the defendant with photographs or posts that may demonstrate the seriousness of their injuries or validity of their claims. In family law, participants may not have the same need to uncover incriminating hidden social network evidence as in litigation, but social networking content surfaces particularly in child custody cases, as online activity may relate to a parent’s ability to raise children. In bankruptcy proceedings or disputes over income, photographs may have relevance in the ability to finance a lifestyle and may work adversely to claims of financial hardship. Additionally, courts are increasingly conducting administrative reviews to determine whether social networking content posted outside of school or work is grounds for censure.

For the most part, traditional civil laws of discovery apply and social networking profiles and other electronic evidence are treated like any other document:

The pages of a social networking site, including a Facebook page, is a document for the purpose of discovery and should be listed in a party's affidavit of documents, if relevant ("relating to any matter in issue").\[167\]

Legislative or statutory frameworks that apply to social networking can affect what evidence is discoverable in civil trials. How various courts have applied each province’s discovery rules to social networking evidence will be discussed below.

A. Legislative Frameworks

Generally, there is a statutory requirement of voluntary disclosure of any document relevant to the proceedings. There is often a great deal of judicial discretion when voluntary compliance is not forthcoming, or where there are disputes over relevancy. Most provinces have broad discovery obligations. For example, Manitoba’s Court of Queen’s Bench Rules\[168\] require:

\[167\] Ottenhof v Ross, 2011 ONSC 1430 at para 3 (available on WL Can) [Ottenhoff].

\[168\] Manitoba, Court of Queen’s Bench Rules, Man Reg 553/88[MBQB Rules].
30.02(1) Every relevant document in an action that is or has been in the possession, control or power of a party to the action shall be disclosed as provided in this Rule, whether or not privilege is claimed in respect of the document.

It provides a broad remedy if a party fails to disclose a potentially detrimental document:

30.08(1) b. if the document is not favourable to the party’s case, the court may make such order as is just.

Under certain circumstances, courts could also resort to interim preservation order rules that authorize individuals to enter property to obtain evidence.\textsuperscript{169}

Ontario has a similar statutory requirement in the \textit{Rules of Civil Procedure},\textsuperscript{170} which do not differentiate between regular discovery procedures and those related to social media. There are separate rules, however, for other types of electronic discovery. Rule 29.1.03(4)\textsuperscript{171} does require certain parties to consult with the \textit{“Sedona Canada Principle Addressing Electronic Discovery”} before preparing a discovery plan.\textsuperscript{172} However, these guidelines are more appropriate to commercial litigation where one party may be disclosing thousands of pages of documents, and do not provide guidance to the evidentiary considerations relevant to social networks. Some have argued that by applying traditional electronic discovery rules (such as those in commercial litigation), the courts have ignored the strong privacy implications of social network evidence.\textsuperscript{173}

\textsuperscript{169} Schuster v Royal & Sun Alliance Insurance Co of Canada (2009), 78 CCLI (4th) 216, 83 CPC (6th) 365 at para 39. (ON Sup Ct J) [Schuster]. Price J discusses the use of courts authorizing entry to social networking accounts, although he rejects it as requiring a higher degree of proof.


\textsuperscript{171} \textit{Ibid}, s 29.1.03(4). Manitoba has also referred to them in their practice directive. See “Guidelines Regarding Discovery of Electronic Evidence” (June 2011) online: <http://www.manitobacourts.mb.ca/pdf/qb_disc_of_edocuments.pdf>.

\textsuperscript{172} Sedona Canada, “The Sedona Canada Principles: Addressing Electronic Discovery” (The Sedona Conference, 2008), online: http://www.thesedonaconference.org/dltForm?did=canada_pincpls_FINAL_108.pdf. The \textit{Sedona Canada Principle} is a framework for managing costs and timeframes in larger electronic discovery, especially for dealing with large discovery requests beyond the scope of those handled in a typical case involving social network evidence.

British Columbia's statutes similarly require a broad disclosure of documents in its Supreme Court Civil Rules,\(^{174}\) although it did not significantly change the rules for electronically stored information when it updated its civil rules in 2010. The court has released a general practice direction to deal with electronic documents geared for larger corporate suits.\(^{175}\) The rule for electronically stored information provides a broad disclosure requirement, while providing the court with the ability to screen any contentious documents for privilege:

Rule 7-1 (20) If, on an application for production of a document, production is objected to on the grounds of privilege, the court may inspect the document for the purpose of deciding the validity of the objection.

BC's rules also provide a broad judicial discretion to order documents, which would include social networking materials, to be available for copying for the opposing party:

Rule 7-1 (17) The court may order the production of a document for inspection and copying by any party or by the court at a time and place and in the manner it considers appropriate.

Nova Scotia, on the other hand, has completely rewritten their civil procedure rules, extensively codifying electronic discovery under Rule 16.\(^{176}\) These rules cover in depth the need to preserve relevant evidence including externally hosted database systems that would be applicable to social networking:

Rule 16.02 (2) A party who becomes aware that a proceeding is to be defended or contested, must take measures to preserve relevant electronic information that is of one of the following kinds:

(a) it is readily identifiable in a computer, or on a storage medium, the party actually possesses;

(b) it is accessible by the party to the exclusion of another party, such as information in a database the party accesses by password on a computer the party does not actually possess.

---


Nova Scotia’s civil rules also provide judges with guidance on how to deal with a party’s failure to disclose documents and enumerate situations where judges may subsequently order disclosure:

Rule 14.13(3) - A judge who orders a person to provide access to an original source of relevant electronic information may include in the order terms under which the access is to be exercised, including terms on any of the following:
(a) a requirement that a person assist the party in obtaining temporary access to the source;
(b) permission for a person to take temporary control of a computer, part of a computer, or a storage medium;
(c) appointment of an independent person to exercise the access;
(d) appointment of a lawyer to advise the independent person and supervise the access;
(e) payment of the independent person and the person’s lawyer;
(f) protection of privileged information that may be found when the access is exercised;
(g) protection of the privacy of irrelevant information that may be found when the access is exercised;
(h) identification and disclosure of relevant information, or information that could lead to relevant information;
(i) reporting to the other party on relevant electronic information found during the access.

Although the changes do not necessarily provide greater access to social networking information, they provide clarity for courts in issuing orders and recognize the unique challenges of social networks and other electronic evidence. Of particular importance is the reference to using independent third parties to supervise access and taking appropriate steps to protect the privacy of irrelevant information.

Most of the cases discussed below focus on the nature of discoverable evidence. Courts have generally ruled that the truth seeking process subverts privacy and the expectation of privacy. Additionally, as social network evidence becomes more common in court, formalized court rules provide greater certainty for litigants (particularly in non-commercial litigation) about what they may expect in the discovery process.

B. Relevance and Discoverability

In a contract dispute, a party may be under an obligation to disclose emails between internal sources leading to the formation of a contract. In an employment dispute, social networking material is generally only relevant if it materially affects an individual’s ability to perform their job. In many types of disputes, such as family law or employment law, only
publicly available social networking material may be relevant, and an extensive discovery process may not be required. However, where litigation surrounds a physical injury or a claim relating to emotional well-being, material that may be somewhat private, such as photographs or status updates, may become relevant and come under a statutory duty of disclosure. For instance, the court in Sparks v Dubé, considered photographs on a zip-line relevant because the plaintiff claimed she suffered ongoing “serious impairment”.177

Although there is a general duty to disclose the existence of a wide range of potential material, a party only needs to produce photographs or posts that are relevant to a trial rather than their entire account. Typically, this requires one side to declare what they believe to be potentially relevant material. At an early stage, there may be disagreements between the sides over disclosure. For example, in Anderson v 45859 Ontario Ltd, the court ordered a plaintiff, injured after being kicked by a horse, to provide a list of all photographs on her Facebook site along with the names of people who appeared in her pictures to determine potential relevancy.178 She claimed that she posted only baby pictures on her private site, not relevant to her injuries.

The leading authority on what is discoverable in Canada, referenced both in Canadian and American cases, is Leduc v Roman.179 The plaintiff had been injured in a car accident and claimed his enjoyment of life was lessened and that he faced severe limitations on his personal life. The defendant requested access to the private areas of the plaintiff’s Facebook account, believing that relevant pictures demonstrating the true extent of the plaintiff’s injuries would be uncovered. The court made some key findings. First, any material on a social networking account is potentially discoverable as they are documents within the control of the plaintiff.180 Secondly, the plaintiff has “an obligation to produce all relevant documents in his possession, including any information posted on his

177 Sparks, supra note 2 at para 3.
178 Anderson v 45859 Ontario Ltd., 2010 ONSC 6585.
179 Leduc v Roman, 308 DLR (4th) 353, 2009 CarswellOnt 843 (available on WL Can) (Ont CA) [Leduc].
180 Ibid at para 8.
private Facebook profile demonstrating activities and enjoyment of life, even if it is contrary to his interests in this action.\textsuperscript{181}

Notably, \textit{Leduc} opened information on a social network to potential discovery regardless of privacy settings. The court adopted the view that there is no reasonable expectation of privacy, unlike a private diary, when one posts to a website whose purpose is to share photographs and status updates. While Facebook and many social networks allow individuals to hide content from the general public, the court refused to designate user chosen privacy settings as equivalent to legal privilege:

\begin{quote}
To permit a party claiming very substantial damages for loss of enjoyment of life to hide behind self-set privacy controls on a website, the primary purpose of which is to enable people to share information about how they lead their social lives, risks depriving the opposite party of access to material that may be relevant to ensuring a fair trial.\textsuperscript{182}
\end{quote}

A difficulty in many cases is that the sides may not agree on what material is relevant to a particular claim. Social networks such as Facebook allow users to post information in a private area because users have legitimate reasons to restrict who can view what information. While \textit{Leduc} made it clear that there is no absolute right to privacy in regards to social networking content, there is also no obligation for a party to turn over intimate photographs or embarrassing personal messages to opposing counsel if they are not relevant to the suit.\textsuperscript{183}

In \textit{Carter v Connors},\textsuperscript{184} Ferguson J conducted a broad survey of general evidentiary rules regarding relevancy. The court concluded that all evidence that could be logically relevant to a fact would be admissible unless it was precluded, either by an existing rule or because it was far too prejudicial. Applying this to social networks, the court concluded that the threshold was low and that:

\begin{quote}
...the success of an application to retrieve an individual's electronic computer data principally depends upon the degree of intrusion into the private lifestyle choices and electronic activity of the Internet user as well as the probative values of the information sought.\textsuperscript{185}
\end{quote}

\begin{flushleft}
\textsuperscript{181} \textit{Ibid} at para 15.
\textsuperscript{182} \textit{Ibid} at para 35.
\textsuperscript{183} \textit{Ibid} at para 32.
\textsuperscript{184} \textit{Carter v Connors}, 2009 NBQB 317, 355 NBR (2d) 235.
\textsuperscript{185} \textit{Ibid} at para 36.
\end{flushleft}
An item is relevant at the discovery stage even if on its own it is not particularly conclusive, but it has a semblance of relevance that could possibly lead to a further inquiry or "the answer may lead to the discovery of admissible evidence." The court found exceptions might exist for material that involves third party privacy (such as chat messages received), or material that may reveal "intimate details of the lifestyle and personal choices of the individual" and has otherwise limited relevance to key issues. Plaintiffs are much more vulnerable to broad discovery obligations. Carter found that by initiating a lawsuit, the plaintiff "implicitly accepted certain intrusions into what otherwise might be private information the disclosure of which would ordinarily be left to her own personal judgment." While the plaintiff may accept certain intrusions, these must be predicated by evidence. Furthermore, the court retains a degree of discretion. In Bishop, the court found it could reject overly broad requests with unknown relevance or requests where there was little probative value and which raised confidentiality issues.

As in Leduc, where physical injuries have occurred and a plaintiff claims they are unable to enjoy life or work, photographs on a social network may have a high degree of relevance. The broader the claim for damages, the more likely the material will be considered relevant. In Murphy v Perger, the plaintiff claimed that she was not able to engage in sports and could no longer enjoy life. The court found that photographs in a private area of Facebook could be relevant not only for assessing the credibility of the claim but also in determining damages. In Leduc, the court likewise found that photographs found in a private area would likely be relevant to the plaintiff's claims of loss of enjoyment of life, as they would demonstrate how he lived his life since the accident.

American courts have taken a similar approach. A New York court in Romano v Steelcase, an action concerning injuries that occurred when a

186 Ibid at para 25.
187 Ibid at para 37. Contra Frangione, infra note 198 which felt that even third parties to a suit sacrificed their expectation of privacy on a social network.
188 Ibid at para 38.
189 Ibid at para 41.
190 Bishop v Minichiello, 2009 BCSC 358 at para 47, 8 WWR 307 [Bishop].
191 Murphy v Perger, 67 CPC (6th) 245 (available on WL Can).
192 Leduc, supra note 179.
193 Romano v Steelcase Inc, 907 NYS (2d) 650 (NY Sup 2010) [Romano].
woman fell out of an office chair, found that photos on her MySpace and Facebook accounts could be relevant to her claims that she suffered permanent injuries and was confined to her bed. The court allowed extensive discovery, in particular because her Facebook profile appeared to show her smiling outside her house and mentioned that she had travelled out of state. The court found “[p]laintiffs who place their physical condition in controversy, may not shield from disclosure material which is necessary to the defence of the action.”

Where a plaintiff claims severe emotional distress or post-traumatic stress, American courts have been willing to allow the defence access to private communications and posts on social networks, as they may be relevant to the plaintiff’s emotional state. In *EEOC v Simply Storage Management,* two plaintiffs sued a former employer for emotional pain and suffering and loss of enjoyment of life after alleged sexual harassment by a supervisor. The court ordered the plaintiff to turn over information relevant to their emotional claims as well as possible alternative explanations for their suffering. This included any posts, pictures, groups joined, or applications “that reveal, refer, or relate to any emotion, feeling, or mental state, as well as communications that reveal, refer, or relate to events that could reasonably be expected to produce a significant emotion, feeling, or mental state.” The court limited disclosure of communications with third parties to those necessary to provide context to issues of emotion, and did not require disclosure of pictures posted by others. The court limited the precedent set by stating that such discovery obligations were only relevant to claims that went beyond “garden variety emotional distress”.

When a plaintiff claims that they permanently cannot work or have some form of brain injury from an accident, a court may hold that their entire account, including private communications, may be relevant to the validity of the claim and their capacity to communicate. In *Wice v Dominion of Canada General Insurance Co,* the court determined that any

---

194 *Ibid* at 5.
195 *EEOC v Simply Storage Management* 270 FRD 430 (SD Ind 2010).
197 *Ibid* at 12.
198 Wice v Dominion of Canada General Insurance Co, 75 CCLI (4th) 265 (available on WL Can).
social networking material could be relevant to whether the plaintiff needed the services of a personal assistant due to alleged brain damage and ordered the plaintiff to preserve everything in his account. In Frangione, the plaintiff's claim of a catastrophic brain injury resulted in the master ordering the plaintiff's entire profile, including private messages, to be disclosed. The messages were determined relevant in showing how the plaintiff, who claimed he could only focus for a few minutes at a time, had lived his life since the accident. However, the master did not distinguish between personal communications such as messages, and private posts shared to a larger circle of friends when rejecting the plaintiff's concerns over privacy. Other courts, such as Carter and Bishop have taken a different approach. Instead of turning over personal communications to determine usage, they ordered production of either computer logs or those logs maintained by the internet service provider.

C. Court-Ordered Disclosure

As discussed earlier, American federal law prevents social networks from releasing user's content to non-governmental entities without the consent of the account holder. In a civil action, the burden falls upon the parties to an action to uphold various duties to preserve their social networking accounts, to disclose documents and other evidence, and to permit the other party to inspect relevant material. In the age of social media, at least one court has made it clear that lawyers are legally obliged to alert their clients to the admissibility of evidence: "[it is] incumbent on a party's counsel to explain to the client, in appropriate cases, that documents posted on the party's Facebook profile may be relevant to allegations made in the pleadings." Ideally, the parties will voluntarily deliver all potentially relevant material including pictures and posts from their social networking accounts. However, concerns over privacy and relevancy as well as animosity between the parties often make court-mandated disclosure necessary.

In Leduc, the court acknowledged that it was the plaintiff's obligation to disclose information. However, the defendant could request court

199 Frangione v Vandongen, 2010 ONSC 2823 (available on WL Can) [Frangione].
200 Carter, supra note 184 at 38.
201 Bishop, supra note 190.
202 Leduc, supra note 179 at para 28.
oversight if they did not feel the disclosure was forthright or contained all relevant material.\textsuperscript{203} The judge found two possible ways to infer whether hidden material may exist. First, the court could consider account specific information such as public profile pictures and privacy settings.\textsuperscript{204} Additionally, the court could:

\begin{quote}
infer from the social networking purpose of Facebook, and the applications it offers to users such as the posting of photographs, that users intend to take advantage of Facebook's applications to make personal information available to others.\textsuperscript{205}
\end{quote}

Not all claims result in the same inferences. In \textit{Schuster v Royal & Sun Alliance},\textsuperscript{206} the court declined a discovery request based on the mere existence of a plaintiff's Facebook account because no relevant material existed on the publicly listed profile.

In both Canada and the US, courts have exercised their discretion in a variety of ways. In some cases, the judge has sanctioned failure to disclose relevant material by forcing unfettered production of an entire account. In \textit{Bass v Miss Porter's School},\textsuperscript{207} a Connecticut court presided over a case in which the plaintiff claimed intentional infliction of emotional distress after being expelled from school. After the defendant complained that the plaintiff was not disclosing all posts related to their emotional state of mind following the expulsion, the judge undertook a sample comparison between the plaintiff's entire Facebook account and what information had been disclosed. The court ordered the plaintiffs to hand over the entire contents of their account to the defendants after finding their voluntary disclosure to be insufficient. In \textit{Frangione v Vandongen},\textsuperscript{208} an Ontario master ordered a plaintiff who claimed he could only sit for 20 minutes at a time to turn over private communications such as messages and chat transcripts in addition to photographs and posts.

Some states have extremely broad disclosure rules that require almost all material, even if only peripherally related to the case, be disclosed.\textsuperscript{209} In

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{203} \textit{Ibid} at para 13.
\item \textsuperscript{204} \textit{Ibid} at para 21.
\item \textsuperscript{205} \textit{Ibid} at para 31.
\item \textsuperscript{206} \textit{Schuster, supra} note 169 at para 39.
\item \textsuperscript{207} \textit{Bass ex rel Bass v Miss Porter's School}, 2009 WL 3724968 (D Conn).
\item \textsuperscript{208} \textit{Frangione, supra} note 198.
\item \textsuperscript{209} See \textit{Pennsylvania, Pennsylvania Rules of Civil Procedure}, Pa RCP No at r 4003.1. This
\end{itemize}
\end{footnotesize}
McMillen v Hummingbird Speedway, Inc, a Pennsylvania court rejected any notion of privacy or confidentiality concluding that, since Facebook and MySpace’s privacy policies indicate that a site operator might require access to a person’s account, there was never a reasonable expectation of privacy. In Romano v Stelcase, a New York court ordered the plaintiff to sign a consent form authorizing MySpace and Facebook to release personal information from the plaintiff’s social networking account. Conversely, in Canada, the judge in Ottenhof v Ross recognized that a request for a password and intensive access to an account would likely be “overly intrusive unless the party is claiming as part of his or her damages claim a level of disability that inhibits his or her computer time.”

In some cases, courts have sought methods outside of the traditional scope of discovery to verify disclosure. In Barnes v CUS Nashville LLC, frustrated with the parties’ inability to determine relevant material voluntarily, the judge offered to “friend” the plaintiff and review posts and pictures. In Lodge v Fitzgibbon, a New Brunswick court ordered the plaintiff’s attorney in a medical malpractice suit to let the defendant’s attorney view the plaintiff’s Facebook account at the plaintiff’s counsel’s office to screen for potentially relevant material. Furthermore, some American courts have taken a ‘hand-over-the-keys’ approach. They have ordered one side to turn over passwords to their accounts or sign a consent form authorizing a social network such as Facebook or MySpace to provide as much information as possible. Usually this is a last resort after it becomes apparent that a plaintiff may be exaggerating a claim or injury.

Lastly, computer logs may be requested where the fundamental issue in a case requires information on a party’s computer usage. In Bishop v Minichello, the plaintiff claimed he was suffering from fatigue because of

---

rule allows discovery of material related to peripheral materials such as potential witnesses.


211 Romano, supra note 193.

212 Ottenhof, supra note 167 at para 3.

213 Barnes v CUS Nashville, LLC, 2010 WL 2265668 (MD Tenn).

214 Lodge v Fitzgibbon, 2009 NBQB 332, 352 NBR (2d) 225.

215 Bishop, supra note 190.
an accident. The defendant claimed the plaintiff's fatigue was a result of late night usage of Facebook, rather than lingering effects from the accident. The court ordered the plaintiff to turn over his hard drive to a third party expert who would produce logs indicating how long and at what times the plaintiff used his computer. The court found that the logs could provide the relevant information without disclosing the content of message or posts.

D. Preserving and Producing Social Networking Evidence

Each party in litigation has a duty to preserve and disclose relevant material once there is a reasonable prospect that there will be legal proceedings. Unless a litigant has a reason to suspect their adversary is failing to disclose all of the relevant material or is not preserving evidence, then the discovery process can proceed with minimal court oversight. Commencement of litigation triggers the duty to preserve potentially relevant material, including a social networking account. In Ottenhof v Ross, the court made it clear that the plaintiff was required to preserve his Facebook page "in the same way that any litigant is required to preserve potentially relevant documentation",\(^\text{216}\) and outlined the proper way to conduct disclosure:

> The pages at a social networking site or internet site including a Facebook page is a document for the purpose of discovery and should be listed in a party's affidavit of documents, if relevant ("relating to any matter in issue"). The mere existence of a Facebook account is insufficient to require its production on discovery. Whether it is listed in the affidavit of documents or not, the responding party is entitled to cross-examine on the affidavit of documents to determine firstly if it exists, secondly the relevance of the contents, and finally production of the relevant portions for which privilege is not claimed.\(^\text{217}\)

It may not be necessary to hand over the entire account to the opposing party; archiving an account and providing an itemized list of photos and potentially relevant messages or statuses may be sufficient. To facilitate this process, sides may choose to agree in advance on a period of updates or photographs potentially relevant to the process. Lawyers seeking to assist their clients in preserving material, or who wish to capture material from an adversary's account, can manually review relevant

\(^{216}\) Ottenhof, supra note 167 at para 3.

\(^{217}\) Ibid.
material or use preservation tools, both freely and commercially available.\textsuperscript{218} While some courts may admit screenshots or even printouts, it is far more reliable to capture original sources or generate a time stamped archive.

Furthermore, changes in technology may provide an alternative to the "hand over the keys" approach when a court wishes to order full production of information. In the fall of 2010, Facebook introduced a feature that allows any user to archive and export their entire account into a handy backup in which all photographs, posts, and messages are saved.\textsuperscript{219} An order to export such an archive would in many cases be a more direct and efficient approach than one requiring a party to hand over passwords and account information to the court or opposing party.

E. \textit{Ex Parte} Motions and Adverse Inferences

Courts are recognizing the challenge of preserving social networking evidence, since accounts are easily closed and photographs or statuses permanently deleted. As a result, they are beginning to grant motions designed to preserve information or impose adverse consequences on parties who appear to be deleting relevant information. For example, in \textit{Terry v Mullowney}, the court drew an adverse inference against a plaintiff in a personal injury lawsuit after he shut down his Facebook account mid-litigation, concluding he had likely posted incriminating evidence undermining his claim before deleting the account.\textsuperscript{220}

The trend moving forward in e-discovery may be the use of \textit{ex parte} motions prior to discovery. While parties have a general obligation to

\textsuperscript{218} There are a variety of ways that both social networking sites and the private sector provide solutions to discovery requirements. For example, Facebook has an archive function that allows a user to download a copy of their entire profile. Companies such as Hanzo Archives <http://www.hanzoarchives.com/products/social_media_archiving>, have software capable of backing up Facebook, Twitter, Linked and YouTube media. They also have useful tools for companies to integrate with enterprise backup solutions for automating preservation of content. There are other tools that exist for those looking to capture posts by other users. Some browsers, such as Apple's Safari, allow users to save a webpage as a template and similar add-ons are available for Mozilla's Firefox.

\textsuperscript{219} Craig Ball, "Facebook Feature Could Ease Cloud-Based EDD" (23 February 2011), online: Law Technology News <http://www.law.com/jsp/article.jsp?id=1202482852070>.

\textsuperscript{220} \textit{Terry v Mullowney}, 2009 NLTDC 56, 285 Nfld & PEIR 19.
preserve relevant documents once litigation has begun, an ex-parte motion may pre-empt a party’s deletion of damaging information. In *Sparks v Dubé*, the defendant became aware that the plaintiff had a Facebook account. On the account were publicly accessible photographs of her participating in a zip-line course, shopping, and relaxing on a beach, appearing to contradict her claims that she was seriously injured. The court noted that it was very simple and quick for a party to delete relevant material once the plaintiff became aware of its potential impact on their claim, and that this fear had played out in the past:

Weighing in favour of the hearing being held ex parte is the real and legitimate concern that any data that might be deleted from her Profile in violation of a Preservation Order made if both parties were present for this motion, would very likely be impossible to resurrect after the fact.

The court attempted to set a balance between privacy and the need to preserve evidence. The court allowed the ex parte motion to supervise discovery of the Facebook account because public photographs posted after the accident were relevant to determining the plaintiff’s injuries and it was likely that more material was available in hidden areas. However, the court denied the ex-parte order for access to the plaintiff’s YouTube, Twitter and LinkedIn accounts, as there was no evidence they contained relevant material.

In granting the motion, the court engaged in a multi-step process. First, the moving party was required to show the social networking account sought is under the other side’s control and the content passes a “semblance of relevance” test. Second, the court allowed the defendants to deliver an order to the plaintiff’s attorneys requiring them to appoint either another lawyer from their firm, or an independent agent to oversee the process. Additionally, the court issued a temporary interlocutory injunction restraining the plaintiff from deleting material. Next, the plaintiff downloaded and preserved the material in the presence of the third party, who would supervise the process, record the times and verify

---

221 Usually only granted in cases where advance notice might cause irreversible harm, in an ex-parte motion one side requests a court order without alerting the other side.
222 *Sparks, supra* note 2.
223 *Ibid* at para 32.
224 *Ibid* at para 51.
that the entire material was saved.225 Last, confident that a backup of the material had been made, the court ordered the plaintiff to ensure all photographs or potentially relevant material were disclosed on her list of documents for future inspection.226

Nevertheless, despite this decision, not all hearings may permit discovery requests to uncover hidden content. While essentially all jurisdictions have civil rules allowing discovery in litigation, some provinces have statutory arbitration hearings to reduce litigation costs in certain proceedings such as automobile claims. In Prete v State Farm Mutual Automobile Co,227 the Financial Services Commission of Ontario rejected a request by an insurance company to force a claimant to disclose information from his social network.

As well, the nature of social networking forums make the requirement to disclose images on such forums procedurally burdensome in the context of an administrative law tribunal. Active participants in these sites post and remove images frequently. The images do not necessarily have the date upon which they were created. It is not uncommon for adults to post their baby pictures. This practice exemplifies the reality that an image may be posted on a date relevant to the claim but was not created at a relevant time. It would be a procedural quagmire to set guidelines for the preservation and production of these images in a manner that would render them reliable evidence in a process that is required to provide a speedy, accessible and fair process for dealing with disputes relating to the Schedule.228

F. Denial of Discovery Requests

Any attempt to request discovery of information from a social networking profile should begin with a factual basis. The party requesting the information should clearly explain how the evidence requested would be relevant to the case. Requests for discovery of social networking material may be denied if done at a late stage in a trial, or if a party cannot demonstrate the relevance of the material sought.229 While courts may be open to inference, an ex-parte application requires “evidence of irreparable harm must be clear and not speculative.”230 American Courts have

---

225 Ibid at para 82.
226 Ibid at para 83.
227 Prete v State Farm Mutual Automobile Co, 2011 CarswellOnt 1019 (WL Can) (FSCO).
228 Ibid at para 17.
229 See e.g. Schuster, supra note 169.
230 Ibid at para 27.
followed a similar test, denying discovery requests where a party has failed to establish a "factual predicate with respect to the relevancy of the evidence." 231

The timing of discovery requests for social networking must generally happen early enough in the process to provide both sides ample time to gather evidence. A defendant cannot delay a discovery request in the hope that a plaintiff will continue to post incriminating social networking evidence. Unless a litigant can show that the evidence obtained demonstrates substantial or unexpected change in circumstances, courts are likely to deny late requests to access private material. As well, parties have an ongoing duty to disclose any relevant material they post after initial discovery that shows a change in circumstance. 232 Even where material may be otherwise admissible, the courts are most likely to limit discovery if it risks delaying the trial, especially if there is a failure at an initial discovery meeting to inquire about photographs or social networking material.

In Kent v Laverdiere, the defendant had failed to ask the plaintiff about the existence of possible photographs. 233 Concerned that reopening discovery would risk delaying the trial, the master declined the request. However, the master did note that had the request come earlier, she would have likely allowed discovery for claims of loss of enjoyment of life as some pictures appeared to show the plaintiff smiling, which would have met the threshold for the semblance of relevance. Conversely, it would have denied discovery for claims such as loss of comfort, care or guidance made by the parents of the plaintiff since these could not be determined from the plaintiff's Facebook account.

G. Costs

In civil cases, where a party seeks material with limited relevancy or fails to disclose relevant material they may also be liable for costs. In Schuster, the court warned the defendant that, "the party who has failed to comply with its obligations or who has asserted without justification that

231 McCann v Harleysville Ins Co of New York, 78 AD (3d) 1524 (NY AD 4 Dept 2010) at 1525.
232 Kent v Laverdiere, 2009 CarswellOnt 1986 (WL Can) (Ont Master).
233 Ibid at para 34.
the other has failed to do so, will be accountable for the costs it has caused."

H. Authentication, Context, and Prejudice

Social networking evidence in civil trials is far less likely to face a rigid admissibility test or the same evidentiary burdens that occur in a criminal trial. Prejudicial evidence may be more relevant to damages or the relationship between the parties than in a criminal context. Furthermore, there is less concern over authentication and the quality of evidence. Pictures or videos taken from a social networking site may be admitted, even if they are grainy or of poor quality. A federal court admitting YouTube videos in a royalty dispute commented: "The Court has viewed the videotapes and while not likely to win any award for cinematography, they may be no worse, for example, than the quality of some surveillance videos used in trials."  

This does not mean that authentication and contextualization are unnecessary. Where one party attempts to introduce evidence they claim to have received from a social network, the courts may require them to disclose how they obtained the evidence and explain its relevance. In *Knight v Barrett*, a New Brunswick court asked the party attempting to present evidence to annotate a Facebook printout and provide details on how they came to possess the printouts. A Kentucky court noted that in a civil trial, a photograph taken from Facebook did not require a high level of authentication as testimony describing the subject matter of the photo would suffice. The court acknowledged that while photos can be faked or altered, it is up to the litigants themselves to challenge the evidence and put forward those allegations for consideration.

Social networking evidence may be denied admittance if the only purpose is to challenge the credibility of a claimant or to put the litigant in an unflattering light and it is highly prejudicial. While this is a general evidentiary rule, it is especially important in social networking cases where profiles may contain highly embarrassing information that may be

---

236 Knight v Barrett, 2008 NBQB 8 at para 8, 331 NBR (2d) 199.
237 Lalonde v Lalonde, 2011 WL 832465 (Ky App).
unconnected to the litigation. In *Kinlock v Edmonds*, a female youth sued a police officer who tethered her while in police custody. The court denied attempts to admit photos of the plaintiff using drugs obtained from her Facebook page, recognizing the defendant’s strategy of trying to portray the plaintiff in an unflattering light. On the other hand, had the case been a child custody dispute, drug use by one of the parties might have been highly relevant to their parenting ability.

Courts should be careful when dealing with printouts or testimony from a social network. Material posted by a litigant must be differentiated from material that may be posted by an acquaintance or automatically generated by the system. While a photograph posted by a friend featuring a plaintiff or a defendant may have relevancy, most social networking sites allow friends to comment or leave posts on an individual’s page without approval. For example, in an employment law case, an Alberta court overturned an employee’s dismissal for allegedly making harassing comments. The court concluded that another individual without approval likely made the comments, and the mere presence of statements on the employee’s Facebook wall had no relevance to the employee’s ability to perform their job.

At least one recent decision appears to show a judge misinterpreting how social networks function. In a child custody dispute, an Ontario judge criticized a father for uploading a video of his daughter to YouTube and juxtaposing it next to an unsavory video. While the father’s decision to upload a video may have been questionable and relevant, many social networks such as YouTube or Facebook dynamically generate advertisements or related content, often based on the computer settings or search terms of the person viewing the pages. Courts should ensure that only pictures, video or posts are admitted as evidence and not peripheral advertising or related links.

I. Use of Social Networking Evidence

Social networking evidence has uses in a variety of different suits.

---

238 *Kinlock (Guardian ad litem of) v Edmonds*, 2008 BCSC 1684 (available on WL Can).
240 *Bekeschus v Doherty*, 2011 ONCJ 232 at para 23 (available on WL Can) [*Bekeschus*].
1. **Uncovering the Unknown Defendant: Defamation**

In most civil actions, the parties are known at the onset of an action; a plaintiff will know the identity of another driver in a collision or an ex-spouse in a family dispute. However, as the internet allows individuals to create a social networking account under a false name, it is easier for a person to post libellous content anonymously. In cases where a statement or post is clearly defamatory or a profile is clearly false, users may report the content and the company may voluntarily remove a post or block an account. In the US, social networks are protected from being held liable for content by the *Common Decency Act*,\(^\text{241}\) which limits their duty to monitor content.

When an individual decides that defamation made on a social network is sufficiently harmful to warrant litigation and the identity of the person uploading libel is not readily apparent, an individual may need to rely on a discovery process. The plaintiff would need to start an action and request a court order to obtain subscriber information and IP address from a social networking company. A second court order might then be required from a Canadian Internet Service in order for them to pair the IP address with a physical address. Handling cross border defamation cases can be costly, and will generally require legal resources in both jurisdictions to obtain the identity of an alleged defamer. In Canada and the US, the legal tests needed to uncloak an anonymous individual are similar; both set a high evidentiary threshold to prove that defamation has occurred.

On the Canadian side, social networking companies and internet providers will generally require a production order before they will release any information. In *AB v Bragg Communications*,\(^\text{242}\) a Nova Scotia court considered a defamation case in which a phony Facebook profile was created by an unknown perpetrator for the sole purpose of embarrassing the plaintiff. The court ruled that a production order would be issued only if there were no other means by which the plaintiff could obtain the information. The fact that the Facebook page was anonymous satisfied

---

\(^{241}\) US, *Communications Decency Act of 1996*, 47 USC § 230. Section 230(c)(1) provides immunity to providers of interactive computer services from materials posted by users of their site.

\(^{242}\) *AB*, *supra note* 147.
that requirement, the court held that there is no general public interest in cloaking a defendant in anonymity for the purpose of libelling or destroying the reputation of another.

To obtain the account information from Facebook or other social networks, a litigant will need to get their Canadian subpoena domesticated by an American court in the jurisdiction where the social network is located. A social network, upon receiving a subpoena, will notify a user of the request for their subscriber information. If a user wishes to quash the subpoena, they have the ability to challenge the production order. The court looks at whether a prima facie libel was established, and then considers whether the merits of potential public interest reasons for allowing a user to remain anonymous: "Requiring at least that much ensures that the plaintiff is not merely seeking to harass or embarrass the speaker or stifle legitimate criticism." The court may also look at whether an alleged defamation was likely to have caused harm, and whether there was actual libel. In Krinsky v Doe 6, the court quashed a subpoena when it did not find the comment to be truly defamatory.

When it comes to social networking, courts are most likely to look at the entire context of a discussion to differentiate between crude comments and posts that may genuinely damage a reputation. In Finkel v Dauber, a court rejected a defamation suit in which outrageous statements were made about the plaintiff.

While the posts display an utter lack of taste and propriety, they do not constitute statements of fact. An ordinary reader would not take them literally to conclude that any of these teenagers are having sex with wild or domestic animals or with male prostitutes dressed as firemen. The entire context and tone of the posts constitute evidence of adolescent insecurities and indulgences, and a vulgar attempt at humor. What they do not contain are statements of fact.

Online defamation cases are growing, and the courts are probably wise to maintain a high threshold related to discovery and vicarious liability so as to avoid entangling themselves in petty disputes where the costs of litigating would be disproportionate to the actual damages of defamation.

243 Ibid at para 19.
244 Ibid at para 20 (Referencing Warman v Wilkins-Fournier, 2010 ONSC 2126, 100 OR (3d) 648).
246 Ibid at 1180.
247 Finkel v Dauber, 906 NYS (2d) 697 at 703 (NY Sup 2010).
2. **Personal Injury**

The most common use of social networking evidence in personal injury claims is the determination of damages, particularly the extent of injury and the amount of damages. Some cases involve plaintiffs seeking claims beyond statutory maximums or standardized insurance company payouts for general damages. The evidence may not eliminate all damages, as the courts are likely to issue general damages for pain and suffering, but may be used to demonstrate that a plaintiff's ongoing claim is exaggerated.

For example, a British Columbia court reduced the claim for future earnings loss of a 22-year-old who suffered a back injury, after discovering Facebook photos that showed her white water rafting, playing soccer and climbing.\(^{248}\) Another court minimized damages to an accident victim who claimed she could no longer engage in activities after Facebook photographs appeared of her hiking and riding a bike, raising doubts about whether the injuries affected anything other than her ability to run long distances.\(^{249}\) A court refused to issues further damages for a boy injured in three separate accidents after Facebook photos showed him playing football and other sports indicating his knee injuries had healed.\(^{250}\)

An Ontario Court in *Kourtesis v Joris*\(^{251}\) found that Facebook photos of the plaintiff celebrating and in social poses indicated that she still enjoyed life, and therefore was not eligible for increased benefits beyond those authorized under the province's no-fault insurance scheme. Similarly, an Ontario judge limited damages to a girl who received a scar across her face in a car accident. The court found the injuries were not seriously interfering with her life as "she socializes, dates and has even gone to the extent of providing her picture on the computer program Facebook."\(^{252}\) In *Tyrell v Bruce*,\(^{253}\) an Ontario judge rejected the plaintiff's entire belated claim for severe injuries after the defendant uncovered evidence of the plaintiff dancing in a rap video.

\(^{248}\) Skusek *v* Horning, 2009 BCSC 893 (available on WL Can).
\(^{249}\) Bagasbas *v* Atwal, 2009 BCSC 512 at para 5 (available on WL Can).
\(^{250}\) MacIntyre (Litigation Guardian of) *v* Pitt Meadows Secondary School, 2010 BCSC 256 (available on WL Can).
\(^{251}\) Kourtesis *v* Joris, 2007 CarswellOnt 4343 (WL Can) (ON Sup Cr J).
\(^{252}\) Goodridge (Litigation Guardian of) *v* King (2007), 161 ACWS (3d) 984 at para 128 (available on WL Can) (Ont Sup Cr J).
\(^{253}\) Tyrell, *supra* note 21.
While there have been cases where social networking evidence undermines a plaintiff’s case, courts have recognized that they must be placed within the context of medical reports and other testimony. In *Mayenburg v Lu*, the court put little weight on the defence’s admission of photographs of the plaintiff hiking, dancing, and bending, noting that the plaintiff’s claimed not that she could not do these things, but that she would “feel the consequences afterwards”\(^{254}\). The court warned the defence against trying to create a “straw person who ... cannot enjoy life at all.”\(^{255}\) In *Raun v Suran*, the court held, despite admitting a video from Facebook that showed the plaintiff capable of athletic moves including jumping out of a pool, that the plaintiff still deserved “fair and reasonable amount for his pain and suffering and loss of enjoyment of life.”\(^{256}\)

Furthermore, some courts have recognized that a plaintiff who presents a positive image on a social network may not be putting forward an image that genuinely reflects their suffering or their actual medical condition. In *Cikojevik v Timm*,\(^ {257}\) a BC court found that photographs of the plaintiff smiling and engaging in activities such as running did not contradict doctor’s testimony that she suffered from depression and head injuries. An Alberta court found that Facebook photographs of a man riding a bike were not persuasive compared to medical evidence about the painful foot injuries he suffered after falling through a faulty platform while playing laser tag:

> While Mr. DeWaard’s Facebook profile is not completely consistent with his evidence at trial, I am prepared to accept that Facebook profiles may contain an overly positive perspective regarding one's abilities and interests or a certain amount of puffery.\(^ {258}\)

Social networking evidence is unlikely to drastically affect reasonable claims, but those who wish to exaggerate their injuries will face far more scrutiny. In many cases, the threat of having to divulge personal materials may be more of a tactical maneuver, in order to acquire a settlement prior to trial. For example in *Sparks v Dubé*, where the court ordered the

---

\(^{254}\) *Mayenburg v Lu*, 2009 BCSC 1308 at para 40 (available on WL Can).

\(^{255}\) *Ibid* at para 41.

\(^{256}\) *Raun v Suran*, 2010 BCSC 793 at para 25 (available on WL Can).

\(^{257}\) *Cikojevic v Timm*, 2010 BCSC 800 at para 124 (available on WL Can).

\(^{258}\) *DeWaard v Capture the Flag Indoor Ltd*, 2010 ABQB 571 at para 41 (available on WL Can).
supervised download of a plaintiff’s Facebook profile, the case was settled out of court shortly after the ex-parte ruling was issued.\footnote{Facebook photo seizure settlement reached” CBC News (1 March 2011), online: CBC News <http://www.cbc.ca/news/canada/new-brunswick/story/2011/03/01/nb-facebook-personal-injury-lawsuit-523.html>.

3. \textit{Income Assessment}

In cases where the income of a party or their ability to work becomes an issue (including bankruptcy suits, spousal support, or access to social service benefits), social networks and particularly photographs may provide probative and relevant information into the lifestyle an individual lives and their access to financial resources. Vacation photographs or participation in expensive activities may provide reasonable grounds for a court to doubt the credibility of claims related to poverty, financial hardship and inability to work.

For example, a BC court refused to discharge a man from bankruptcy and debts to a former girlfriend after his creditors introduced photographs from his Facebook account showing him at an expensive social club on numerous occasions.\footnote{Jabs, Re, 2010 BCSC 1325 (available on WL Can).} A judge rejected a father’s attempts to reduce his child support obligations, finding that Facebook photographs depicting him on a motorcycle and his girlfriend skydiving contradicted his claims of financial hardship.\footnote{Kolodziejczyk \textit{v} Kozanski, 2011 ONCJ 6 (available on WL Can).} In \textit{Cikojevic \textit{v} Timm}, the Master rejected an earlier motion by the plaintiff to get an advance on damages after the admission of numerous photographs from her Facebook account demonstrated her ability to afford activities such as snowboarding and golf.\footnote{2008 BCSC 74 at para 47 (available on WL Can).} An Ontario court, on the other hand, rejected a former husband’s attempt to end spousal support because he felt his wife could afford to vacation in Paris and Cancun.\footnote{Vacaru \textit{v} Vacaru, 2010 ONSC 7020 (available on WL Can). The wife had clicked a ‘like’ button on Facebook that indicated she wanted to visit those destinations despite her relative financial inabilities. This is very different from uploading photographs of her actually vacationing.}

In addition, social networking evidence has been used to challenge an individual’s credibility regarding their ability to work. A court rejected a father’s contention that he was not capable of working due to medical
issues after reviewing submissions from his Facebook account and finding statements that he was self-employed and evidence that he regularly biked and engaged in off-road motor sports.\textsuperscript{264}

Courts in the US have denied social security benefits or increased support payments for individuals whose social networking profiles appear to contradict their medical health concerns. An Arkansas court refused to overturn an administrative decision denying a woman’s application for a permanent disability pension because of her alleged mental incapacity, noting she spent all day on Facebook and had little difficulty engaging in activities when she wanted to.\textsuperscript{265} A New Jersey appellant court took judicial notice of a Facebook photograph of a woman smoking in a review of whether she was fairly denied permanent disability benefits, noting that such evidence appeared to contradict her claims that she was unable to work on account of severe asthma.\textsuperscript{266} A New York court determining spousal support amounts found that Facebook entries about a woman belly dancing were relevant to the effect an alleged accident had on her life and whether she was unable to leave the house to find employment.\textsuperscript{267}

4. \textit{Family Law}

While most civil trials limit the ability to introduce prejudicial character evidence, in family law almost any picture, status update or link shared may be relevant to the capacity of a parent to raise a child. Often, the character of the individuals is the central issue, and the only legal issue for a court to determine is the weight to be given to social networking evidence once admitted.

Increasingly, profiles and posts of parents and former spouses have tended to lead to adverse rulings against one of the parties. It may be that former spouses are still connected as ‘friends’ through a social network, or a mutual friend may be willing to pass on material from another’s account, or the information may appear through the discovery process. In some cases, online activity is relevant to the decision. Social networks will often reveal photographs or statements indicative of lifestyle choices that may reflect badly on a parent in a court case.

\textsuperscript{264} R(CM) v R(OD), 2008 NBQB 253, 337 NBR (2d) 90.
\textsuperscript{265} Conners v Astrue, 2010 WL 903416 (ED Ark).
\textsuperscript{266} Purvis v Commissioner of Social Sec, 2011 WL 741234 (DNJ).
\textsuperscript{267} BM v DM, 927 NYS (2d) 814 (NY Sup 2011).
For example, a father whose Facebook profile contained inappropriate language and homophobic jokes was denied access to his children.\textsuperscript{268} Another father was denied joint parenting control after the court reviewed his Facebook account, noticing crude and obscene references to porn stars, links to a page referring to his former spouse as crazy and other derogatory material alongside photos of his child.\textsuperscript{269} A young mother who uploaded photographs of herself smoking marijuana, drinking and dancing to Facebook was denied custody of her child and unsupervised overnight visits.\textsuperscript{270} In another case, a wife won sole custody after her husband made repeated negative comments about her and appeared to stalk her by posting photographs of her car parked at a friend’s house on his Facebook account.\textsuperscript{271}

However, not all social networking material impacts negatively on a decision. One judge rejected as immaterial that a mother used to work as a stripper and had salacious photos on her Facebook account, stating, “[c]onduct, save as it bears upon the care of the children, is irrelevant to my determination of temporary custody and access.”\textsuperscript{272} A BC judge rejected a mother’s contention that a disheveled photograph taken of a father with his daughter likely showed him on drugs, noting the alternative explanation that it was a sleepy morning photo taken while camping.\textsuperscript{273}

5. Education Law

Educational institutes are also coming to terms with social networking usage by students. Unlike private law cases involving employers, universities and schools are more limited in how they can use comments on a social network; many are “government actors” and thus their students may be protected by either Section 2(b) of the Canadian Charter of Rights and Freedoms\textsuperscript{274} or by the First Amendment in the US.\textsuperscript{275} In Pridgen v

\begin{footnotesize}
\textsuperscript{268} Westhaver v Howard, 2007 NSSC 357, 260 NSR (2d) 117.
\textsuperscript{269} M(MJ) v D(A), 2008 ABPC 379 at para 52 (available on WL Can).
\textsuperscript{270} W(JWA) v B(A), 2008 NBQB 157 (available on WL Can).
\textsuperscript{271} Byram v Byram, 2011 NBQB 80, 376 NBR (2d) 241.
\textsuperscript{272} Dearden v Dearden, 2009 ONCJ 90 at para 11 (available on WL Can).
\textsuperscript{273} D(K) v S(J), 2010 BCSC 1160 (available on WL Can).
\textsuperscript{274} Charter, supra note 36, s 2b.
\textsuperscript{275} US Const amend I.
\end{footnotesize}
University of Calgary, a student successfully appealed a University decision to reprimand him for comments made in a Facebook group regarding a professor’s teaching style. The Court rejected the University’s assertion that “expression in the form of criticism of one’s professor must be restricted in order to accomplish the objective of maintaining an appropriate learning environment.”

While courts have found that students may criticize teachers, educational institutes do have the ability to discipline students for comments that violate the law or risk disrupting classes. An Ontario court upheld the decision to expel a law student who, after being warned, continued to post comments that his fellow students were “subhuman” and which made reference to killing sprees. The court rejected the student’s contention that the comments were made out of school and agreed that the comments could create fear and apprehension amongst classmates. It also differentiated between acceptable social networking statements and that which could be held against a student:

This court is mindful of the historical importance of encouraging free speech on university campuses, and rigorously defending the right of students to debate difficult and often highly unpopular issues with passion. However, free speech has its limits, including the making of threats and defamation of character.

Courts in the US have taken a similar approach finding that online postings can be grounds for dismissal if they are likely to disrupt class. In JC ex rel RC v Beverly Hills Unified School District, the court agreed with a school’s decision to suspend a student who created YouTube videos mocking another student. It found that statements or posts made on the internet could be grounds for removal if it is “foreseeably likely to cause a substantial disruption of school activities” and a “sufficient nexus exists where it is “reasonably foreseeable” that the speech would reach campus.” The court also noted that it is reasonable foreseeable that material posted on the internet would reach the school.

---

276  *Pridgen v University of Calgary*, 2010 ABQB 644, 325 DLR (4th) 441.
277  *Ibid* at para 82.
278  *Zhang v University of Western Ontario*, 2010 ONSC 6489 at para 27, 328 DLR (4th) 289.
279  *Ibid* at para 35.
281  *Ibid* at 1107.
suspensions have been upheld where threatening social networking videos have been produced in jest if they "materially and substantially disrupt the work and discipline of the school."\textsuperscript{282}

\textbf{VI. CONCLUSION}

This paper examined the legal issues related to discovering and utilizing evidence from social networks and looked at the ways courts have dealt with it in terms of both criminal and civil law. In criminal proceedings, investigators have tools to obtain evidence directly from the social networks when reasonable grounds exist. They must then proceed to prove the authenticity of the material as well as ensure that the probative value outweighs potential prejudice. In Canada, local investigations can be assisted by the Department of Justice to obtain the necessary court orders in the US. Defence lawyers faced with social networking evidence should be aware of issues regarding authentication, context and potential prejudice.

In civil proceedings, parties are obligated to produce any evidence that is relevant to an issue which depends on the nature of the claim or the dispute. In litigation particularly, it is incumbent on counsel to advise their clients on the risks of using social networks, as well as their obligation to preserve relevant material even if it is adverse to their case. Anyone involved in a dispute should be aware that procedural fairness and the truth seeking process will generally outweigh personal privacy concerns, and courts have the power to compel individuals to uncover their digital lives to assist in dispute resolutions.

Social networks have only been around a few years and the law in these areas will continue to grow. Some of the cases covered spring from misunderstandings of the private nature of a social network. Others are the result of a compulsion to seek attention despite the consequences.

In large part, the use of social networking has resulted in traditional means of communicating inner secrets and private thoughts being displaced with keyboard strokes and chat transcripts. This paper is not intended to dissuade individuals from using social networks. From connecting long lost friends to helping overthrow dictators, the benefits of

\textsuperscript{282} OZ v Board of Trustees of Long Beach Unified School Dist, 2008 WL 4396895 (CD Cal).
new forms of communication are numerous. However, any form of social incrimination, public or private, may find itself admissible in a court.