

Social Media: The Law Simply Stated

*Steve Coughlan and Robert J. Currie**

INTRODUCTION

It is a challenge to simply state the law about social media, because there is no such thing as “social media law.” Rather, the law bumps up against social media in many ways. In some cases, existing law can be seamlessly applied to new technologies and means of interaction. In other cases, entirely new paradigms will likely need to be adopted to handle new challenges. Many other cases will fall somewhere in between.

Our goal in this Law Simply Stated is to provide some background on the nature of social media themselves, and then to state the basic law in a number of applicable fields. In particular we shall begin with discussion of the definition of “social media,” along with consideration of what we see as an important analytical theme: is this topic a topic? Do the challenges posed by social media have a single solution? Are they matters to which the law can simply adapt, or must new approaches be created? Can the same answer be provided in each context?

Following that we will move to discuss basic principles of law in a variety of areas which are relevant to social media. These are: judicial notice; courtroom management; civil discovery; privacy; admissibility of electronic documents; criminal evidence-gathering; employment law; defamation; and finally, cyber-bullying.

I. WHAT ARE “SOCIAL MEDIA”?

There is no single commonly-accepted definition of “social media” and for purposes of this discussion it is not crucial to settle upon one. It is possible to point to some common characteristics of what we mean by social media, however.

First, social media are internet-based, which means that generally speaking they share the characteristics of much communication on the web: whatever is posted has the potential to reach nearly worldwide and the material is difficult if not impossible to control once posted. Because of the nature of some social media, though, it can be possible to have more control over the extent to which information is released in the first place.

* Steve Coughlan, Associate Director, Law & Technology Institute, Schulich School of Law, Dalhousie University; Robert J. Currie, Director, Law and Technology Institute, Schulich School of Law, Dalhousie University. A version of this article was prepared by the new editors of the Canadian Journal of Law and Technology as the background material for two online courses on social media offered by the National Judicial Institute, one exclusively to Canadian judges, the other to judges from Canada, Australia, and Scotland. It is presented here as a kind of introductory editorial on the subject, setting out an introduction to the many ways in which social media can be relevant to various areas of the law. It is meant to present the questions which must be asked, without attempting to provide answers to all of them.

Second, social media are interactive and in most cases have the capacity for multi-party live communication. An important point to recognise is that social media are not merely a form of communication, though they can be used in that way. Rather, they are a method for people to remain connected, often in real time. A group of people who are using Facebook or Twitter (to name well-known examples) might be experiencing their interaction in much the way they would if they were sitting in the same room having a conversation.

This means that social media might need to be regarded as being different in kind, not merely in degree, from other sorts of media. People have long been able to write letters to the editor taking issue with some article which has appeared in print, or to phone or email a television station in response to a program which has appeared. Now a person can comment on a blog posting, receive a reply from the blogger, post a further response, and continue an exchange essentially live before whatever audience the blog might have. Similarly, viewers of a television program (such as an awards show) are frequently able to tweet to the show while it is in progress and have their tweets appear on screen: this means viewers can effectively become a part of the program as it is occurring and possibly even shape what occurs.

These points are aptly summarized by Antony Mayfield:¹

Social media is best understood as a group of new kinds of online media, which share most or all of the following characteristics:

Participation

social media encourages contributions and feedback from everyone who is interested. It blurs the line between media and audience.

Openness

most social media services are open to feedback and participation. They encourage voting, comments and the sharing of information. There are rarely any barriers to accessing and making use of content — password-protected content is frowned on.

Conversation

whereas traditional media is about “broadcast” (content transmitted or distributed to an audience) social media is better seen as a two-way conversation.

Community

social media allows communities to form quickly and communicate effectively. Communities share common interests, such as a love of photography, a political issue or a favourite TV show.

Connectedness

Most kinds of social media thrive on their connectedness, making use of links to other sites, resources and people.

¹ Antony Mayfield, *What is Social Media?* An e-book from iCrossing.com, download available online at <<http://www.icrossing.co.uk/what-we-think/our-research/a-bluffers-guide-to-social-media/>>.

It is also worth considering some examples of social media, to recognise the various forms they can take.

The image most people have when they think of social media is a social network, which include “personal” sites like Facebook or MySpace and “professional” sites like LinkedIn. The purpose of a social network is to create a method of being in touch with other people, either friends or business contacts. Users create their own personal page, containing information which will vary from user to user and, depending on the purpose of the site, can interact with other users on the site. Facebook, for example, allows other users to write on the “wall” of their friends, and sends a regular report to each user about the updates which have occurred on the pages of their friends. Typically there is some ability to control access, so that a user can determine who will see the information posted. In a social network, users will not normally be anonymous: the whole point is to be in contact with friends or professional contacts, and indeed the terms of service for both Facebook and LinkedIn require the use of one’s real name. Nonetheless the typical user is likely to expect some privacy in some of the material, at a minimum.

Other social media also allow the same kind of long-term interactivity, but not necessarily under one’s own identity. There are many online forums, for example, devoted to the discussion of particular topics or hobbies. Individual users can develop an identity on that forum, become known to others and have a reputation on that site, and reach either a large or small audience, depending on the particular forum — all under the identity generated for that site, which might have little or no correspondence to the person’s “real-life” identity.

Similarly, there are various sites in which the content is generated by users but which are accompanied by forums for comments. YouTube is one example of such a site, and it has the potential to reach an enormous audience, potentially affecting their behaviour. One might also include here sites such as Pinterest, Instagram or Flickr, which are primarily devoted to pictures, but which allow users to “like” particular submissions, to make comments, to follow other users, and so on. Other sites which rely on user participation are sites like Wikipedia, which Mayfield considers to be a social network.

Much of the content of YouTube is meant only for entertainment purposes, and a great many postings will be viewed by relatively few people. On the other hand it is not uncommon for a person to be able to produce short videos on relatively mundane subjects — how to change a flat tire, for example — and receive thousands or even tens of thousands of views. Further, some posters on YouTube have more ambitious goals. The controversial Kony2012 video, for example, was aimed at multinational action to arrest Ugandan rebel leader Joseph Kony. The International Criminal Court had issued an arrest warrant for Kony in 2005 but he was largely unknown outside of central Africa before the YouTube video (which has now been viewed almost 100 million times) was posted. The video quite deliberately aimed at using the networking capacities of the internet and encouraged viewers to “above all share this movie online” — as thousands and thousands did, through things such as Facebook pages. The video ultimately prompted thousands of people to become involved in a poster campaign in cities around the world.

Although YouTube has the ability to connect people on a global basis, it is not clear that YouTube users would consider themselves a community, in the way that

someone would have a group of friends on Facebook.² On the other hand there are news aggregation sites such as Reddit which consist primarily of material reposted from elsewhere on the web, but where the real character of the site is the community which exists in the comments section (similar sites include Digg or StumbleUpon). Reddit users earn “karma” when other users “upvote” their submissions or comments: karma is nothing but a measure of approbation from other users. Many Reddit users think of themselves as part of a community, recognize and follow one another in the comments section, and enter into real world relationships — holding, for example, the largest “secret santa” in the world, or raising money to support other Redditors in need.³ News aggregation sites such as Reddit can also work as a mobilizing force: Barack Obama conducted a live question and answer session on the site in August of 2012, and users on the site have banded together (or sometimes competed against one another) to accumulate donations for various causes. In some cases this simply amounts to using Reddit as a focus for fundraising efforts which would occur in any case, such as aid after the earthquake in Haiti. In other instances however this form of social media has led to action which realistically could not have occurred otherwise. In January 2012, for example, a Reddit user in Kenya posted about the need for a security fence at a local orphanage, hoping to raise \$2,000: by the next day \$80,000 had been donated.⁴

The last form of social media to be discussed here is the blog, though we include within that what is sometimes referred to as “microblogging,” services like Twitter or Tumblr. “Blog” is a short form of “weblog.” Some blogs are well-known and widely read, such as BoingBoing, while most blogs are a labour of love for some individual and will be hosted on a third party site such as WordPress. Blogs typically have a comments section, and so on more popular sites extended debates between readers can take place. The distribution of blog posts is made simpler through features such as Really Simple Syndication, more popularly known as an RSS feed, which allows users to subscribe to a site and receive notice of updates.

In many cases, blogging is more akin to a form of journalism than it is to other social media, which presents challenges of its own. Does privilege ever attach to a blogger/source communication?⁵ Do defences to defamation apply in the same way to traditional journalists and bloggers?⁶ Most bloggers will have few followers but some will be much more widely read than a local newspaper. There are controls other than the choice of the journalist governing whether something appears on radio or television or in a newspaper, such as the judgment of an editor or pub-

² Moreover, YouTube is not entirely “social,” insofar as users can offer their own YouTube “channels” by which they can make money.

³ Frances Bea, “Reddit Readers Donate \$30,000 to Cancer-Stricken Redditor” *Digital Trends* (13 June 2012), online: <<http://www.digitaltrends.com>>.

⁴ “Attack in Kenya Orphanage Yields \$80k in Donations” *The Wall Street Journal* (2 February 2012), online: <<http://online.wsj.com>>.

⁵ *R. v. National Post*, 2010 SCC 16, 2010 CarswellOnt 2776, 2010 CarswellOnt 2777 (S.C.C.).

⁶ *Grant v. Torstar Corp.*, 2009 SCC 61, 2009 CarswellOnt 7956, 2009 CarswellOnt 7957 (S.C.C.).

lisher, but for many bloggers it is just a matter of clicking “post.” There will not always be an easy answer.

The most well-known example of microblogging is Twitter, which permits users to post messages of no more than 140 characters. Individual messages, known as “tweets,” are visible to anyone on the service, though it is possible to specifically follow particular users or to send messages to other users. Conversations among a group of individuals can therefore occur “live” over twitter, including not just text but pictures. Twitter has a reputation of simply being a means for individuals to post the most quotidian details about their lives, and that is not always wrong. However, services like Twitter are capable of more than that.

An important aspect of Twitter (or other sites, such as Instagram) is the “hashtag,” which is interesting not only for what it does but because it is a user-created function of the site rather than a feature built in by the designers.⁷ A hashtag is the pound sign followed by other words: for example “#whatimissmost” is a hashtag designed to be attached to tweets about nostalgia. The hashtag allows twitterers to follow tweets on a particular subject, which has many ramifications. First, this feature allows twitterers to engage in conversation with one another, even with people they did not previously know, since everyone can be following the same set of tweets. Second, it allows Twitter to be tied to other forms of media, so that television shows, for example, can receive live tweets about the content of the programming.

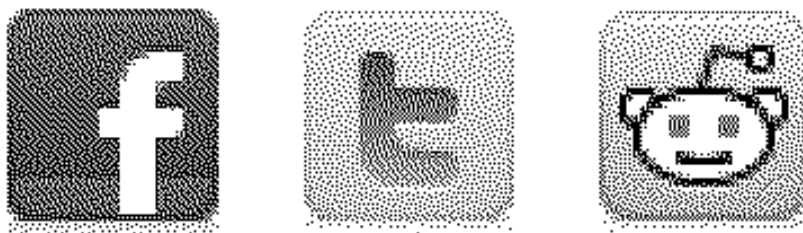
Perhaps most significantly, it allows communities to be mobilized into real world action, not merely conversation. Twitter played a role in the “Arab spring” uprisings in the Middle East in 2011, for example, largely through the use of hashtags such as “Egypt,” “protest,” “Bahrain,” and so on, which allowed participants to coordinate their actions.⁸ Facebook postings were also seen as an important part of this planning process, and in fact, Facebook itself recently installed a hashtag function on its platform for use by all of its users.

Twitterers often use their real names. However, unlike sites such as Facebook or LinkedIn, twitterers can remain anonymous by setting up an account with a pseudonym. Further, although tweets can be far-reaching, unlike a great deal of the web tweets are ephemeral and are not saved in any central location.

Relevant to all social media, of course, is the portability of content between them and the possibility (hope, in many cases) that content will go “viral”: that is, be posted and reposted from site to site and Facebook page to Facebook page, be tweeted and retweeted, and be upvoted to the top spot on a news aggregation website. It is that aim which makes common the hyperlinks to Facebook, Twitter, Reddit and other sites which are found on so many web pages:

⁷ Henry Bailer, “Top Twitter Hashtags of the Last 12 Months” *Yahoo! News* (31 August 2012), online: Yahoo! <<http://news.yahoo.com>>.

⁸ Carol Huang, “Facebook and Twitter Key to Arab Spring Uprisings: Report” *The National* (6 June 2011), online: <<http://www.thenational.ae>>.



II. IS THIS TOPIC A TOPIC?

Social media raise many legal issues in many different areas of law, some of which will be pursued below. The first question to be asked, however, is whether this topic really is a topic.

It was suggested above that some social media differ in kind rather than merely in degree from previous forms of communication and contact. The issue is whether that means entirely new legal approaches to those media are necessary, or whether existing rules can simply be adapted to cover the different situation. The likely answer is that some of each will be required.

Consider, for example, the law of negligence. Its founding principles are quite general, and for the most part it has simply been able to adapt to new factual situations. Sometimes the law has been adjusted (for example occupational health and safety rules or Workers' Compensation schemes) but generally speaking the basic law has adapted to changes in society.

On the other hand copyright law developed at a time when copying of other works was possible but cumbersome. The widespread use of photocopiers or of VCRs created some challenges, but nothing requiring a fundamentally different approach. With the mass digitization of information and the advent of downloading, however, it seems fair to say that a paradigm shift has occurred. It is not simply a question of degree, i.e. that far more people download music than recorded it from the radio onto a cassette tape. Rather, it is that the changed technology has led to a changed attitude. Many downloaders do not realize that they are violating copyright or engaging in theft. More important, though, is that most of those who *do* realize it do not care. Downloading music, videos or other information has become, in many people's eyes, like speeding, or failing to declare the full value of goods brought across the border: it is known to be against the law but there is no stigma attached to violating that particular law. Copyright law was not equipped to deal with the change in kind rather than degree that the technology has wrought, and so its fundamental assumptions and principles are being re-worked.⁹

That same question — do we need new rules or can the old rules simply be adapted — arises in many contexts due to social media.

⁹ Michael Geist, ed, *In the Public Interest: The Future of Canadian Copyright Law* (Toronto: Irwin Law, 2005).

For example, the extent to which a defamatory statement was disseminated is relevant to what damage award might be appropriate: perhaps it is possible simply to take into account that a defamatory statement on the web has a wider reach than one in a small town newspaper, but leave the basic approach unchanged. Alternatively, perhaps the correct approach is to analogize an exchange on a blog to live conversation, and find in that context no defamation at all.¹⁰ Perhaps our understanding of what it means to “publish” a defamatory statement can be adapted to the internet context with no fundamental change in the rules.¹¹ Whatever the answer, the law of defamation can likely be adapted to handle the situation.

But in other areas the nature of social media seems to demand a more fundamental change in the law. We have a ban on reporting federal election results in areas where the polls have not yet closed, for example. At one point that simply amounted to requiring television and radio stations not to begin election coverage in an area until voting had finished there, which was an enforceable law. It was possible, of course, for individuals in the East Coast to phone friends on the West Coast to report results, but to the extent this was a problem it was minor and manageable. As early as 2000, however, it was apparent that the existence of the web posed challenges to that approach.¹² Realistically, the subsequent development of social media sites, through which individuals tweet or place on their wall interesting news, means that individuals across the country are continually in contact with one another, which has made the law functionally unenforceable and purposeless.¹³

We live in a time where news of an earthquake can arrive before the earthquake itself.¹⁴ How this new reality plays out will need to be determined in each separate area of the law.

III. JUDICIAL NOTICE

The doctrine of judicial notice “dispenses with the need for proof of facts that are clearly uncontroversial or beyond reasonable dispute.”¹⁵ It serves a trial efficiency function, since it allows us to avoid consuming valuable court time by proving things which should simply be assumed. It maintains the repute of the administration of justice, since courts should not be seen to allow parties to “game” the legal system by contesting obvious matters nor to run the risk of not accepting as fact what everyone knows to be true.

¹⁰ *Baglow v. Smith*, 2011 ONSC 5131, 2011 CarswellOnt 8852 (Ont. S.C.J.); additional reasons 2011 CarswellOnt 11650 (Ont. S.C.J.); reversed 2012 CarswellOnt 7383 (Ont. C.A.).

¹¹ *Crookes v. Newton*, 2011 SCC 47, 2011 CarswellBC 2627, 2011 CarswellBC 2628 (S.C.C.).

¹² *R. v. Bryan*, 2007 SCC 12, 2007 CarswellBC 533, 2007 CarswellBC 534 (S.C.C.).

¹³ “Tories Plan to Lift Election Results Ban” *MacLeans* (13 January 2012), online: <<http://www2.macleans.ca>>.

¹⁴ Randall Munroe, “Seismic Waves” (webcomic), online: [xkcd <http://xkcd.com>](http://xkcd.com).

¹⁵ *R. v. Spence*, 2005 SCC 71, 2005 CarswellOnt 6824, 2005 CarswellOnt 6825 (S.C.C.), at para. 53, quoting *R. v. Find*, 2001 SCC 32, 2001 CarswellOnt 1702, 2001 CarswellOnt 1703 (S.C.C.).

As Justice Paciocco observes, “[t]he only caveats [to the robust use of judicial notice] are related to the objective that judges are obliged to respect the adversarial system and the need to maintain the appearance of justice.”¹⁶ Accordingly, at its strictest, and as regards *adjudicative facts* (those facts which are directly at play in the litigation), judicial notice may only be taken of that which is:

- (1) so notorious or generally accepted as not to be the subject of debate among reasonable persons; or (2) capable of immediate and accurate demonstration by resort to readily accessible sources of indisputable accuracy.¹⁷

Where the facts sought to be judicially noticed are *legislative facts* (relevant to statutory interpretation or legal reasoning) or *social facts* (which provide necessary background for fact-finding), then the test is whether the fact “would be accepted by reasonable people who have taken the trouble to inform themselves on the topic as not being the subject of reasonable dispute *for the particular purpose for which it is to be used*.”¹⁸ Finally, the level of rigour required is on a sliding scale: the more central the fact is to the dispute between the parties, the closer to “indisputable” or “notorious” the fact must be.¹⁹

The question of when and of what to take judicial notice has always been a vexing one. The challenge of taking judicial notice of technological points has been frequent and sometimes stark, but not unmanageable. It required the courts to change with the times, which of course they can and do — at some point it became unnecessary to call expert evidence to explain the basic workings of a “motorcar” or “aeroplane.” Similarly, courts have become familiar enough with new technology to take judicial notice of it. Judicial notice of e-mail has become completely functional and implicit; no one calls expert evidence of what it is, how it works, what an “attachment” is, etc., even though this might have been required as recently as the late 1990s.

Social media, however, may represent the kind of paradigmatic “rapid technological change” that causes issues. The facts that its rise in use and popularity has been meteoric and that the rate of its change and evolution is practically unprecedented mean that it is difficult to keep track of. This is compounded by the fact that social media use is highest among the younger and more computer-savvy demographic of our population, who tend to be early adopters. The challenge in the courtroom, then, is clear. Large swathes of the population are intimately familiar not just with the specific social media platforms themselves, but with their mechanics and workings, all of which might be relevant at least as background but sometimes as adjudicative facts. Other large swathes have little or no familiarity, and sometimes are proud of that fact. Judges and counsel are more likely to belong to the latter demographic than the former. The result is a disconnect between knowledge of counsel and courts, and that of the public they serve. It is not difficult to imagine a situation where a witness could refer, in testimony, to having observed or done something within the context of a social media platform, and that most or all

¹⁶ Justice David M Paciocco, “Proof and Progress: Coping With the Law of Evidence in a Technological Age,” in this issue.

¹⁷ *Spence*, *supra* note 15 at para. 53.

¹⁸ *Ibid.* at para. 65.

¹⁹ *Ibid.* at paras. 60–62.

of the jurors (and possibly counsel, if they have prepared the witness properly) understood what was being described, but the judge did not. Consider:

COUNSEL: How did you become familiar with Mr. X [a musician]?

WITNESS: I saw a link to his Facebook page on my friend's wall, and I liked his page.

COUNSEL: Did you like his personal page or his musician page?

WITNESS: Uh, musician.

COUNSEL: How did you come to invite your friend, Y, to Mr. X's concert?

WITNESS: X posted about it on his page, and I tweeted his post. Y saw it and retweeted it.

Understanding this exchange requires the listener to know that: a) a "wall" is a running series of posts by Facebook users that can be viewed by other Facebook users who are linked to the first user; b) "liking" someone's Facebook page means hitting a button marked "like," which then links the two Facebook pages and allows users to view each other's content; c) there is a difference between "personal" Facebook pages and commercial pages which operate in a similar way to a website (and are popularly used by musicians); d) "tweeting" something refers to posting it on Twitter, and it is not unusual to post text from one social media platform (here, Facebook) to another (here, Twitter); and e) "retweeting" is a function within Twitter that allows one user to post another user's entries on their own Twitter feed.

It is not as if all of this cannot be explained or proven through evidence, but as the previous paragraph makes obvious it would be time-consuming. Moreover, it is entirely possible that everyone in the courtroom under the age of 50 will have understood the entire exchange without any explanation, which tends to militate towards the taking of judicial notice. The problem for the law of judicial notice, then, is obvious, when one recalls the classic framing of judicial notice as the device by which the court should find as fact what "everybody knows,"²⁰ and Lord Justice Scrutton's wry observation that "It is difficult to know what judges are allowed to know, though they are ridiculed if they pretend not to know."²¹ Because of what is essentially a generational gap, it can be difficult to figure out what "everyone knows."

It is worth reflecting that such a problem was not born with the internet, as illustrated by the following statement of a trial judge in a 1970s case concerning a stripper: "The dance was described to me as a 'go-go dance' which, I understand, is a violent movement of almost all parts of the body, more or less in time to strongly rhythmic music."²² However, it is highly arguable that the potential degree of disruption is greater in cases involving social media.

This is compounded by the problem of where one should go to find evidence of what is reasonably notorious or indisputable regarding social media. They change rapidly enough that the *Encyclopedia Britannica* is unlikely to be of much

²⁰ *Spence, supra* note 15 at para. 49, quoting Thayer, "Judicial Notice and the Law of Evidence" (1889-1890) 3 Harv L Rev 285 at p. 305.

²¹ *Tolley v. Fry* (1929), [1930] 1 K.B. 467 (Eng. C.A.), at p. 475 ; reversed [1931] A.C. 333 (U.K. H.L.).

²² *R. v. Campbell*, 1972 CarswellAlta 125, 21 C.R.N.S. 273 (Alta. Dist. Ct.).

use. Should one consult the background information on the social media platform itself? Bill Gates' blog? Certainly Wikipedia serves a lot of information needs but has reliability concerns that should (but do not always) give courts pause.²³ Need experts be called, or will it be sufficient that the parties agree on the particular matter?

The Supreme Court of Canada's flexible framework in *Spence* certainly provides some useful tools for resolving these problems. But as Aaron Fox remarked in a recent paper, "[t]he challenge of determining what you 'are allowed to know' and avoiding 'ridicule' if you pretend not to know, remains greater than ever."²⁴

IV. COURTROOM MANAGEMENT

Several challenges arise for courtroom management, all related to the "constant connectedness" of social media.

Court proceedings generally are subject to the open court principle, and so in the absence of any direction to the contrary anyone in court will reasonably expect that they are entitled to report the proceedings. Nonetheless there are occasions when a publication ban is granted²⁵ or other restrictions are placed on the media in their reporting.²⁶ One can expect journalists to understand and respect the terms of a publication ban. It is not immediately apparent that every person in a courtroom who might have a smartphone or other electronic device with access to the internet will understand the ban so clearly, or feel so compelled to respect it. The Supreme Court has held, for example, that it is appropriate to ban publication of the name of an underage plaintiff who is suing over sexualized cyber-bullying.²⁷ It is, nonetheless, not at all difficult to imagine circumstances in which some person in court immediately tweets "the judge just banned publication of Susie's name," either maliciously or genuinely unaware that doing so is a violation of the order.

Further, there can be occasions where the need for a publication ban does not become apparent until after particular evidence has been led — just as things are sometimes said in front of the jury before it is apparent the jury should be excused. Where a publication ban is aimed at print media or at journalists planning a later broadcast on radio or television, an after-the-fact ban is possible. But where someone in the court, journalist or not, is tweeting the proceedings or posting about them on Facebook, even a ban imposed only a few minutes later might already be too late.

²³ HB Murray and JC Miller, "Wikipedia in Court: When and How Citing Wikipedia and Other Consensus Websites is Appropriate" (2010) 84 St John's Law Review 633.

²⁴ Aaron A Fox, QC, "Judicial Notice of 'New' Technology" unpublished NJI paper (copy on file with the authors), 9.

²⁵ *R. c. Dufour*, (sub nom. *CBC v. THE QUEEN*) [2011] 1 S.C.R. 65, 2011 CarswellQue 41, 2011 CarswellQue 42 (S.C.C.).

²⁶ *Société Radio-Canada c. Québec (Procureur général)*, (sub nom. *CBC v. Canada (A.G.)*) [2011] 1 S.C.R. 19, 2011 CarswellQue 43, 2011 CarswellQue 44 (S.C.C.).

²⁷ *A.B. (Litigation Guardian of) v. Bragg Communications Inc.*, 2012 SCC 46, 2012 CarswellINS 675, 2012 CarswellINS 676 (S.C.C.).

By way of analogy, consider *Tremblay v. 1168531 Ontario Inc.*²⁸ In that case a settlement had been mediated to a human rights claim by an employee against her employer, which included the payment of money to the employee and a confidentiality agreement concerning the settlement. The employee, however, had been posting to Facebook about the negotiations both during and immediately after the proceedings, and so was found to be in breach of the agreement.

Exactly this same kind of possibility, that proceedings in court might be tweeted or otherwise reported essentially live by people who see themselves as in conversation rather than as “publishing” could have an impact in other areas. In many trials witnesses are excluded so that they will not hear the testimony of prior witnesses and adjust their own testimony accordingly: the possibility of tweeting from the courtroom adds a further dimension to the challenge.

The same issue arises in juror selection where there will be a challenge for cause. Prospective jurors are frequently excluded from the courtroom during the challenge process, and indeed the *Criminal Code* has been amended to provide for the option of a “static triers” approach rather than a “rotating triers” approach, to try to ensure that no member of the jury has been tainted by hearing the questions asked of others.²⁹ Again, of course, conversation by tweet from within the courtroom has the potential to undermine this approach.

Perhaps less challenging but raising the same concerns is the issue of jury sequestration. While deliberating, juries are supposed to be kept from all extrinsic material, which is particularly important because publication bans frequently end when jury deliberations begin. Information about matters intrinsic to the jury’s deliberations must be kept confidential according to the jury secrecy rule, though it is permissible to report on extrinsic matters which affect them.³⁰ At a minimum the relatively simple solution of ensuring jurors take no cell phones with them to the jury room seems in order, but more might be required.

Finally, note that most of these concerns need not arise from deliberate bad faith actions on the part of lay-participants in the system. There is also, of course, the possibility of exactly that sort of misbehavior related to social media. Consider, for example, a New Brunswick juror who belonged to a Facebook group which was explicitly opposed to the accused³¹ or a British juror communicating via Facebook³² with the defendant in a prosecution.

V. DISCOVERY IN CIVIL LITIGATION

Under most provincial civil procedure regimes the traditional test for what documents must be produced in any civil case has been a broad one. The tendency was for the courts, in applying the relevant civil procedure rule, to adhere to the

²⁸ *Tremblay v. 1168531 Ontario Inc.*, 2012 HRTO 1939 (Ont. Human Rights Trib.).

²⁹ See *Criminal Code*, RSC 1985, c C-46, s 640 and the discussion in *R. v. Riley*, 2009 CarswellOnt 2470, 247 C.C.C. (3d) 517 (Ont. S.C.J.).

³⁰ *R. v. Pan*, 2001 SCC 42, 2001 CarswellOnt 2261, 2001 CarswellOnt 2262 (S.C.C.).

³¹ “Murder Case Mistrial over Juror’s Facebook Comments” *CBC News* (18 July 2012), online: Canadian Broadcasting Corporation <<http://cbc.ca/news/>>.

³² Michael Holden, “British Juror Jailed for Facebook Comment” *Reuters* (16 June 2011), online: <<http://www.reuters.com>>.

traditional *Peruvian Guano* standard³³ and require the disclosure of documents which tend to have a “semblance of relevancy”³⁴ or any bearing on any question which is or might be at play between the parties. However, over the last decade or so, the law and practice on discovery of documents in civil matters has been profoundly affected by three concurrent, separate but related trends, and the bar has shifted a great deal.

The first is the move towards “proportionality,” i.e. the idea that the amount of procedure required for a claim should bear some rough parity with the amount involved and the importance of the issues,³⁵ which has led to some jurisdictions raising the test from “semblance of relevancy” to actual or “trial” relevance.³⁶ The second is the advent of electronic discovery, resulting in exponential increase in the amount of data which *can* be produced and a desire to tailor how much *should* be compellable. The third is the increasing sensitivity of the courts to the privacy interests of litigants, and concern about preventing discovery from needlessly interfering with individual privacy, particularly (but not exclusively) in personal injury cases.

All three of these birds have come home to roost in the issue of when data that are contained in social media platforms must be produced, and of how to tailor disclosure when it is required. The typical case is that of a personal injury plaintiff who claims pain, disability, loss of enjoyment of life, etc., but has posted photos or text on a social media platform that might undermine the credibility of the claim. Unguarded MySpace, Facebook or Pinterest pages might have compromising material, leading the defendant’s insurer to demand all such data in case there is anything relevant. In some cases, what is sought is evidence of the amount of time a plaintiff is able to spend using a computer generally and social media specifically, to test claims of both physical and mental impairment stemming from negligence.³⁷

The ubiquitous use of social media has resulted in litigants essentially manufacturing a great deal of evidence which can be used against them, and both motions and appellate courts have wrestled with overbroad discovery requests, on the one hand, and resistance to disclosure on the other. Courts have generally recognised that social media profiles contain a great deal of private information — even when shared with “friends” — and have applied what seasoned civil litigators would recognise as a presumption against fishing expeditions that seek broad discovery rights in situations where the defendant has not presented sufficient facts to

³³ *Compagnie Financiere et Commerciale du Pacifique v. Peruvian Guano Co.* (1882), 11 Q.B.D. 55 (Eng. C.A.).

³⁴ *Eastern Canadian Coal Gas Venture Ltd. v. Cape Breton Development Corp.*, 1995 CarswellNS 436, 141 N.S.R. (2d) 180 (N.S. C.A.).

³⁵ See generally Martin Teplitsky, “Making civil justice work: A new vision” (2008) 27:3 *Advocates Journal* 7.

³⁶ E.g. in Nova Scotia and Ontario.

³⁷ E.g. *Bishop v. Minichiello*, 2009 BCSC 358, 2009 CarswellBC 871 (B.C. S.C.); leave to appeal refused 2009 CarswellBC 3301 (B.C. C.A. [In Chambers]); *Carter v. Connors*, 2009 NBQB 317, 2009 CarswellNB 632 (N.B. Q.B.).

sustain invasive inquiries.³⁸ However, judges do not shy away from sorting out which information is sufficiently relevant to be ordered disclosed while at the same time applying proportionality, based on the issues as raised in the pleadings.³⁹

One issue that has emerged with some clarity in this context is that of litigant destruction of evidence, in this case their own social media data. Despite the quasi-public nature of much social media activity, people nonetheless object vociferously to being told or ordered to produce their posted holiday pictures, status updates, travel and activity information, which seems quintessentially private to them. This can result not just in litigation of discovery demands but spoliation concerns. In one controversial case, a motions judge was hearing a defence *ex parte* motion for disclosure of social media evidence by a personal injury plaintiff. He found on the facts that there was some danger that the plaintiff would destroy data in her Facebook account if she was ordered to disclose it. He ordered an injunction and a preservation order to issue, but coupled this with a requirement that the plaintiff's lawyer engage another lawyer in his firm or an outside lawyer to summon the plaintiff to the lawyer's office without telling her the nature of the order until she arrived there, then supervise the downloading of the Facebook material.⁴⁰

On one view it might be said that this is simply an increase in volume which is driving a need for efficiency, rather than any radical change. Insurers have been monitoring questionable claimants by way of private investigators for years, and the only real shift here is that the investigators have moved indoors and onto computers. It is difficult to tell whether this is simply a case of new wine in old bottles, but the fermentation of the issue continues to bear watching.

VI. ADMISSIBILITY OF ELECTRONIC DOCUMENTS

One important concern with social media in the litigation context is how social media-based data, in whatever form, will be entered into evidence. There will, of course, be the usual kinds of admissibility concerns, e.g. whether statements posted on Twitter are hearsay, what inferences can be drawn from the manner or length of social media use, etc. However, a major issue coming to light is at the authentication stage, concerning whether the electronic data itself is even capable of becoming part of the evidentiary record. The *Canada Evidence Act* and nearly all of the provincial evidence statutes contain provisions dealing with these issues,⁴¹ but

³⁸ For example, see *Dosanji v. Leblanc*, 2011 BCSC 1660, 2011 CarswellBC 3255 (B.C. Master). Though there is division of opinion as to when the appropriate relevance threshold has been reached; compare *Frangione v. Vandongen*, 2010 ONSC 2823, 2010 CarswellOnt 5639 (Ont. Master), with *Schuster v. Royal & Sun Alliance Insurance Co. of Canada*, 2009 CarswellOnt 6586 (Ont. S.C.J.).

³⁹ See *Morabito v. DiLorenzo*, 2011 ONSC 7379, 2011 CarswellOnt 14825 (Ont. S.C.J.); *Fric v. Gershman*, 2012 BCSC 614, 2012 CarswellBC 1177 (B.C. Master).

⁴⁰ *Sparks v. Dubé*, 2011 NBQB 40, 2011 CarswellNB 80 (N.B. Q.B.).

⁴¹ See the *Canada Evidence Act*, RSC 1985, c C-5, ss 31.1–31.8; the *Ontario Evidence Act*, RSO 1990, c E23, s 34.1; and most recently the *Nunavut Evidence Act*, RSNWT (Nu) 1988, c E-8, s 37.1. See the slightly outdated “Status of E-Commerce Legislation in Canada 2004”, online: Uniform Law Conference of Canada <<http://ulcc.ca>> under 2004 Regina SK Annual Meeting, Civil Sector Documents. Only Newfoundland, Brit-

based on the reported cases and informal conversations the authors have had with members of the judiciary, these provisions are not well-known. The provisions are complex and reward sustained attention, and they require a brief review here.

The statutory provisions were the result of work in the late 1990s by the Uniform Law Conference of Canada, which drafted the *Uniform Electronic Evidence Act* in response to concerns that the traditional rules of evidence mapped poorly onto electronic evidence, and that courts were blurring the authentication, best evidence and hearsay rules as a result.⁴² The provisions provide a broad definition of “electronic document,” which includes both data “recorded or stored” on a computer system as well as “a display, print-out or other output of that data.”

In terms of authentication of electronic documents, the provisions codify the common law rule which places the burden on the party adducing the document to provide “evidence capable of supporting a finding that the electronic document is that which it is purported to be” — anticipating that the trier of fact will make the ultimate decision on this point. In the era of social media, this point is even more important than it may appear to be — people often share the sign-in credentials and passwords for their social media accounts or stay logged in while they are away from their computers. This can create issues around proving that particular statements or actions are actually attributable to a specific person; not a new concern, perhaps, but one that is more “live” than it used to be.

The most noteworthy aspect of these provisions is their recognition that electronic documents revive the concerns behind, if not the letter of, the “best evidence rule,” which had otherwise fallen into disuse. The traditional rule required a party to produce the original of a document or demonstrate that the use of a copy was necessary, in order to combat forgery. Electronic data raises similar concerns about its reliability, but often cannot be traced down to something like an “original,” particularly in a networked environment. In addition, the distinction between “original” and “copy” is not of much use, because there is usually in practice no discernible difference between the original and the copy. Thus, the original is not likely to be more clearly reliable than a copy.

The solution set out in the *Uniform Act* provisions was the imposition of a requirement of “system integrity,” allowing the adducing party to meet the best evidence rule by proving that the storage system from which the document emerged was in sufficient working order so that it can be relied upon. Several presumptions are set up to allow efficient proof of integrity, which can be established through: proof that the storage medium was operating properly; proof that the document was recorded or stored, or recorded and stored by an adverse party; or proof that the document was recorded or stored in the ordinary course of business by a party outside the litigation. This integrity can be proven by way of affidavit, though depending on the nature of the technology, expert evidence may be required.

The reported decisions considering these provisions are not numerous, and until recently all concerned the *CEA* version. The August 2012 decision in *Saturley v.*

ish Columbia, and the Northwest Territories have yet to adopt some form of electronic evidence legislation.

⁴² Uniform Law Conference of Canada, *Uniform Electronic Evidence Act* (1998), online: Uniform Law Conference of Canada <<http://www.ulcc.ca>>.

*CIBC World Markets Inc.*⁴³ considered the Nova Scotia *Evidence Act* version of the provisions in dealing with two kinds of electronic data: data entered by individuals into computer databases and data automatically generated by computers. Justice Wood held that the latter kind of data, while it met the definition of “electronic record” in the *Evidence Act*, was not a “document” at all but rather real evidence — meaning that it did not require recourse to the system integrity requirements nor could it offend the hearsay rule, having been generated without human agency.

VII. CRIMINAL EVIDENCE-GATHERING

There are many aspects of search and seizure law which relate to information which can be obtained against an accused through social media. We will pursue only two here: the question of reasonable expectation of privacy, and the range of warrants available and the different standards required for each. In the latter context, the important issue will be whether the requirements for those warrants and their underlying presuppositions actually match up with the nature of the information gathered.

An investigative technique will only qualify as a search for *Charter* purposes if the person concerned has a reasonable expectation of privacy. Broadly, a reasonable expectation of privacy can fall into one of three main types: personal, territorial, and informational. Any investigative technique dealing with social media is likely to invoke informational privacy, and is likely to encounter information worthy of protection.

Reasonable expectation of privacy is not determined by a risk analysis — that is, it is not undermined merely because it is possible that one’s privacy can be compromised. Rather, it is a matter of *entitlement* to privacy. The Supreme Court of Canada has observed that activities involving personal computers and the use of the internet are entitled to a high degree of privacy:

[105] . . . it is difficult to imagine a more intrusive invasion of privacy than the search of one’s home and personal computer. Computers often contain our most intimate correspondence. They contain the details of our financial, medical, and personal situations. They even reveal our specific interests, likes, and propensities, recording in the browsing history and cache files the information we seek out and read, watch, or listen to on the Internet.⁴⁴

Within that general category of “online activity,” there is a good argument that behaviour using social media is particularly entitled to protection, because it is the activity closest to a person’s “biographical core”:

[46] The closer the subject matter of the alleged search lies to the biographical core of personal information, the more this factor will favour a reasonable expectation of privacy. Put another way, the more personal and confidential the information, the more willing reasonable and informed Canadians will be to recognize the existence of a constitutionally protected privacy interest.⁴⁵

⁴³ *Saturley v. CIBC World Markets Inc.*, 2012 NSSC 226, 2012 CarswellNS 420 (N.S. S.C.).

⁴⁴ *R. v. Morelli*, 2010 SCC 8, 2010 CarswellSask 150, 2010 CarswellSask 151 (S.C.C.).

⁴⁵ *R. v. Cole*, 2012 SCC 53, 2012 CarswellOnt 12684, 2012 CarswellOnt 12685 (S.C.C.).

This expectation of privacy is not necessarily diminished because the activity is to a greater or lesser extent “public,” depending on the particular type of social media involved: section 8 protects, in part, the right to remain private in public spaces.⁴⁶

Since there will normally be a reasonable expectation of privacy, police will require authority from some source in order to be able to search constitutionally. Typically that will either be as a search incident to arrest, if a cell phone is involved, or under some kind of warrant. The law remains to a certain extent unsettled in both contexts.

With regard to searches incident to arrest of cell phones (in order to check text messages or other information) no single approach has been settled upon yet. Some courts have held that a cell phone is simply like any other object in an arrestee’s pocket and can be searched without restraint. The leading cases, however, suggests that a more measured approach is called for.

In *R. v. Manley*, the accused was arrested and a cell phone was taken from him and searched.⁴⁷ That particular search incident to arrest was found to be lawful because there was reason to wonder whether the cell phone itself was stolen, and if it was that would have been relevant to the arrest. In the course of deciding about the particular search, however, the Court of Appeal declined the Crown’s invitation to reject the approach in *R. v. Polius*.⁴⁸ *Polius* had held that the police were only authorized to seize a cell phone incident to arrest, but that because of the “deeply personal contents” a warrant was necessary to search it. Justice Sharpe in *Manley* held:

While I would not apply *Polius* in the particular circumstances of this case, I am far from persuaded that *Polius* was wrongly decided or that it ought to be overruled. Cell phones and other similar handheld communication devices in common use have the capacity to store vast amounts of highly sensitive personal, private and confidential information — all manner of private voice, text and e-mail communications, detailed personal contact lists, agendas, diaries and personal photographs. An open-ended power to search without a warrant all the stored data in any cell phone found in the possession of any arrested person clearly raises the spectre of a serious and significant invasion of the *Charter*-protected privacy interests of arrested persons. If the police have reasonable grounds to believe that the search of a cell phone seized upon arrest would yield evidence of the offence, the prudent course is for them to obtain a warrant authorizing the search.

⁴⁶ See *R. v. Ward*, 2012 ONCA 660, 2012 CarswellOnt 12133 (Ont. C.A.):

[75] By going on the website carookee.com, the appellant engaged with others in a public forum that was open to literally anyone around the world. The appellant did so, however, anonymously. Anonymity “to some degree at least” is a feature of much Internet activity: *Warman v. Wilkins-Fournier*, 2010 ONSC 2126, 2010 CarswellOnt 2737, 100 O.R. (3d) 648 (Ont. Div. Ct.), at para. 20. Depending on the totality of the circumstances, his anonymity may enjoy constitutional protection under s. 8.

⁴⁷ 2011 ONCA 128, 2011 CarswellOnt 803 (Ont. C.A.).

⁴⁸ 2009 CarswellOnt 4213, 196 C.R.R. (2d) 288 (Ont. S.C.J.).

The Ontario Court of Appeal adopted more or less the same approach in *Fearon*, speaking favourably of the *Polius* rule while not fully committing itself.⁴⁹ More recently still the Nova Scotia Court of Appeal, in *Hiscoe*, seems to have formally endorsed the *Polius* approach as correct.⁵⁰

Two points need to be discussed about searches of social media through the use of warrants. The first is that the extent to which a warrant will permit the search of social media information on a computer is not completely settled, though recent authority from the Supreme Court suggests that caution will be shown before allowing such a power to extend too far. In *R. v. Vu* the police had a warrant to search a building for evidence of ownership of the property.⁵¹ Upon entering the building an officer found a laptop which was already running several programs, including MSN messenger and Facebook: both of those programs were signed into accounts in the accused's name. The issue was whether that search had been authorized under the warrant.

The Supreme Court of Canada reached the conclusion that a warrant to search a place does not automatically carry with it the authority to search any computer or smart phone found in that location. They rejected the analogy to other receptacles found in a location, on the basis that computers were markedly different because of the sheer volume of material they store, because they store information of which the user is unaware, and because they continue to store information even after the user might think it has been deleted.

The decision in *Vu* makes clear that police can only search a computer or smart phone found in a location if the warrant specifically authorizes such a search: that obligation was imposed to make certain that the issuing justice will have fully weighed in the balance the extent of the privacy interest at stake. What remains somewhat unsettled is whether, having been given the specific authority to search a computer, police would be entitled to browse freely through a person's accounts on various social media sites. On the facts that issue did not arise in *Vu*, since the computer was already signed in to the accused's accounts on the relevant sites and the police did no more than look at the page which was already on the screen.

The Court's rationale that the competing interests need to be fully weighed would suggest imposing an additional obligation to seek prior authorization before engaging in the even greater infringement of privacy of looking through a person's social media history. On the other hand the Court already noted, in deciding *Vu*, that "a search of a computer connected to the Internet or a network gives access to information and documents that are not in any meaningful sense at the location for which the search is authorized."⁵² One might therefore conclude that that interest has already been weighed by the specific decision to authorize a search of the computer. It seems likely that this issue will be the subject of future litigation.

The second warrant-related issue concerns confusion over which of the many warrants in the *Criminal Code* should be considered the correct one in the context

⁴⁹ *R. v. Fearon*, 2013 ONCA 106, 2013 CarswellOnt 1703 (Ont. C.A.); leave to appeal allowed 2013 CarswellOnt 9433 (S.C.C.).

⁵⁰ *R. v. Hiscoe*, 2013 NSCA 48, 2013 CarswellNS 242 (N.S. C.A.).

⁵¹ *R. v. Vu*, 2013 SCC 60.

⁵² *Vu*, *ibid*, at para. 44.

of social media. There are many statutory provisions authorizing searches, most of which are based upon presumptions about the nature of the privacy interest involved. It is not at all clear that the particular warrants which are being used actually map correctly onto those privacy interests.

It is not necessary to have a detailed understanding of all the *Criminal Code* warrant provisions to see this point. One can think of search warrants in section 487 as creating a kind of baseline. Where the “ordinary” privacy interest is at stake, then the “ordinary” protections guaranteed by *Canada (Director of Investigation & Research, Combines Investigation Branch) v. Southam Inc.* are required: the existence of reasonable grounds to believe an offence has been committed and evidence will be found, and pre-authorization by someone capable of acting judicially.⁵³ Other searches use essentially the same standard, such as production orders under section 487.012, which are used with Internet Service Providers among others.

In some cases, however, a person is seen as having an enhanced privacy interest. The wiretap provisions in the *Criminal Code*, for example, are seen as particularly intrusive: “one can scarcely imagine a state activity more dangerous to individual privacy than electronic surveillance.”⁵⁴ Correspondingly, additional requirements must be met, beyond those necessary for a search warrant, before electronic surveillance can be authorized (for example, only judges can grant authorizations, they are for a limited time period, are only available for some offences, the order must be in the best interests of the administration of justice, and under s. 185(1)(h) the “investigative necessity” criterion must be met). In addition, there are “general warrant” provisions in the *Code* which are a kind of residual “catch-all” warrant, which authorize the police to do “any thing” which no other warrant provision can authorize.⁵⁵ They too involve higher protections than section 487 warrants.

In other cases, however, a person’s privacy interest is seen as reduced. A dial number recorder, for example, does not reveal the content of an accused’s conversations over a telephone, only the buttons which have been pushed. This was seen as being less intrusive on privacy than most searches,⁵⁶ and as a reflection of that they can be obtained based on mere reasonable *suspicion* rather than requiring reasonable belief.⁵⁷

It is because of these different levels of protection that the final issue relating to warrants arises. The *Criminal Code*’s current scheme presumes that private communications are entitled to greater-than-usual protection; that information stored within an accused’s computer or the computer system of some service provider is entitled to an ordinary level of protection; and that the keys pressed on a telephone keypad are entitled to lower-than usual protection. The difficulty is that in the con-

⁵³ (sub nom. *Hunter v. Southam Inc.*) [1984] 2 S.C.R. 145, 1984 CarswellAlta 121, 1984 CarswellAlta 415 (S.C.C.).

⁵⁴ *R. v. Sanelli*, (sub nom. *R. v. Duarte*) [1990] 1 S.C.R. 30, 1990 CarswellOnt 77, 1990 CarswellOnt 986 (S.C.C.).

⁵⁵ *Criminal Code*, supra note 29 at s. 487.01.

⁵⁶ *R. v. Fegan*, 1993 CarswellOnt 92, 80 C.C.C. (3d) 356, 21 C.R. (4th) 65 (Ont. C.A.).

⁵⁷ See *Criminal Code*, supra note 29 at s. 492.2.

text of social media, those pieces of information might all be exactly the same thing.

In *R. v. TELUS Communications*, for example, the police wanted to obtain text messages sent and received by two Telus subscribers over a 30 day period, part of which time predated the warrant application and part of which was prospective.⁵⁸ In fact they had obtained a general warrant to do so, but the issue in the case was whether some other warrant(s) had to be used, specifically for the prospective portion of the warrant.⁵⁹ It was argued at trial, for example, that the texts could otherwise be obtained, for example in part through the use of a dial number recorder warrant (which would assume a very low level of privacy). Alternatively, it was argued that the texts which had not yet been sent were really private communications, and so the interception of private communications provisions could be used (which would assume a very high level of privacy). Finally, it was argued that the police could just wait until further time had passed and then apply for an ordinary warrant or production order after the fact (which would presume a baseline level of privacy).

The majority of the Supreme Court struck down the general warrant on the basis that obtaining text messages was substantively equivalent to a wiretap. Three of the seven judges deciding, led by Justice Abella, went further and found that the interception of text messages actually *was* an interception of private communications, essentially because “text messaging bears several hallmarks of traditional voice communication: it is intended to be conversational, transmission is generally instantaneous, and there is an expectation of privacy in the communication.”⁶⁰

At a minimum, this demonstrates that the presuppositions which animate the warrant provisions in the *Code* do not yet map very well onto the reality of social media. It is true, as a matter of the way the technology works, that communications through social media, whether texting, Twitter, Facebook or otherwise, pass through or are stored on computer systems at some point. That is not to say, however, that the “lived experience” of social media for the participants is “I am creating a record.” Rather, that lived experience might well feel like “I am engaging in private communication.”

The Supreme Court has also shown some willingness in other decisions to recognise the distinction between what people feel they are doing on computers and what the computers are actually doing. In *Morelli*, above, for example, the Court found that a person will only possess an internet file if he or she downloads it rather than merely accesses it. They then carried on to acknowledge that every time a person accesses a file on the internet a computer will automatically download a copy of it to the person’s cache, which on the face of it means that a technological fact would collapse the legal distinction they had just drawn. They concluded, therefore, that an automatic download to the cache does not qualify as having

⁵⁸ *R. v. Telus Communications Co.*, 2013 SCC 16, 2013 CarswellOnt 3216, 2013 CarswellOnt 3217 (S.C.C.).

⁵⁹ One precondition for the use of a general warrant is that no other provision in the *Criminal Code* could authorise the particular investigative technique. If it could, a general warrant cannot be used: s. 487.01(1)(c).

⁶⁰ *TELUS*, *supra* note 58 at para. 1.

downloaded the file: it was a thing the computer did rather than a choice made by the person. In other words, what mattered was the lived experience of the accused, not the unregarded functioning of the machine. Much the same type of reasoning might be necessary in many contexts relating to social media.

VIII. EMPLOYMENT LAW

The law regarding employment of individuals and the termination of employment, both in the unionized and private employment contexts, has experienced some impact due to the widespread use of social media. The case law is not voluminous as yet, and reflects the slow engagement by employers, employees, counsel and the courts with the potential legal impacts of social media activity. There has been a challenge in figuring out what kind of an action or activity a particular social media use is — is a Facebook post to your 540 “friends” akin to a kitchen conversation, shouting from a street corner, or taking out an ad in a newspaper? A Twitter post is accessible to anyone in the world with an internet browser, but does its practical impact depend on how many people are likely to have read it, or can be *proven* to have read it?

The second stream has been ascertaining what the legal effect of social media use should be, which of course depends a great deal on how the first question was answered. Unionized workers are usually not disciplined for “shop floor talk,” but at what point has a social media-based conversation been taken beyond that threshold? An employee has a duty under the employment contract not to be insolent, or dishonest, or to wrongfully abuse the employer’s business interests. While the employee may think of their social media use as being done “at home” or socially and therefore not relevant to their employment, is this necessarily a reasonable expectation? Does it matter if they are Facebook “friends” with their fellow employees, or with their managers? Suppose an employee of XYZ Inc. posts on his Facebook page a link to a YouTube video of the Johnny Paycheck hit “Take This Job and Shove It,” along with a caption that says “It’s Monday morning . . . just sayin’, XYZ . . . LOL.” Has the employee repudiated the employment contract? Is this kind of behaviour subject to discipline?

The kind of decision that has made its way to reported status is, of course, fact-specific. In the most prominent Canadian case, the termination of an employee of an auto-detailing facility was upheld by the B.C. Labour Relations Board because of the employee’s Facebook postings.⁶¹ He made violent statements that could be interpreted as threats, insulting comments about his supervisors, and advised potential customers to patronize a competitor company rather than his employer, due to quality concerns. The case was widely and understandably viewed as a victory for employers.⁶² More complex or debatable cases are doubtless on their way down the pipe. Consider, by contrast, a recent UK decision in which an employee who had made homophobic statements on his Facebook page had his termination overturned by the court because the remarks were made in his personal ca-

⁶¹ *Lougheed Imports Ltd. v. U.F.C.W., Local 1518*, 2010 CarswellBC 3021 (B.C. L.R.B.). See also *Perez-Moreno v. Kulczycki*, 2013 HRTO 1074 (Ont. Human Rights Trib.).

⁶² “Not Just ‘Shop Talk’” (Spring 2011) (Newsletter), online: McKercher <<http://www.mckercher.ca>>.

capacity.⁶³ This was despite the fact that some of his Facebook friends were fellow employees, and that the Facebook page indicated he was employed by the employer.

IX. DEFAMATION

It is not surprising that the World Wide Web in general, and social media in particular, have had quite an impact on the law of defamation, since defamation is about the public communication of facts, ideas and opinions. Broader and more geographically widespread communication was inevitably going to move the goal-posts of defamation law. And indeed, while the core elements of defamation have remained the same (defamatory words, referring to plaintiff, published or re-published by a defendant) the case law reflects the many procedural aspects and elements of the tort that have required the courts to adapt to changing circumstances. The Supreme Court of Canada has had to consider whether comments published on a US website but targeted in part at Canadian readers could establish sufficient jurisdiction to sue in Ontario (its answer: yes, but because the comments were re-published in Canadian newspapers).⁶⁴ It also was forced to wrestle with whether a site that put in place a hyperlink to allegedly defamatory text had fulfilled the requirements of the publication element (its answer: no, unless the hyperlinker explicitly agrees with or adopts the defamatory material).⁶⁵

Lower courts have also wrestled with interesting procedural and substantive problems in the defamation context. There have been increasing attempts to use *Norwich*-type orders to compel ISPs and others to disclose the identity of users who posted allegedly defamatory comments online,⁶⁶ though not without some controversy over the use of unsubstantiated allegations to obtain what would otherwise be private information.⁶⁷ One case working its way through the Ontario courts has seen the trial judge decide that the type of heated and insulting conversation involved in certain political blog-based discussions cannot, in fact, constitute defamatory words;⁶⁸ the decision to base a summary judgment order on this point resulted in the matter being sent back for a full trial,⁶⁹ but the case is being watched with interest. UK press recently reported that Lord McAlpine is considering bringing actions against every individual who re-tweeted the false statement that he was im-

⁶³ *Smith v. Trafford Housing Trust*, [2012] E.W.H.C. 3221 (Ch).

⁶⁴ *Black v. Breeden*, 2012 SCC 19, 2012 CarswellOnt 4272, 2012 CarswellOnt 4273 (S.C.C.).

⁶⁵ *Crookes v. Newton*, 2011 SCC 47, 2011 CarswellBC 2627, 2011 CarswellBC 2628 (S.C.C.).

⁶⁶ E.g. *York University v. Bell Canada Enterprises*, 2009 CarswellOnt 5206 (Ont. S.C.J.); *Morris v. Johnson*, 2011 ONSC 3996, 2011 CarswellOnt 6964 (Ont. S.C.J.).

⁶⁷ *Warman v. Wilkins-Fournier*, 2010 ONSC 2126, 2010 CarswellOnt 2737 (Ont. Div. Ct.).

⁶⁸ *Baglow v. Smith*, 2011 ONSC 5131, 2011 CarswellOnt 8852 (Ont. S.C.J.); additional reasons 2011 CarswellOnt 11650 (Ont. S.C.J.); reversed 2012 CarswellOnt 7383 (Ont. C.A.).

⁶⁹ *Baglow v. Smith*, 2012 ONCA 407, 2012 CarswellOnt 7383 (Ont. C.A.).

plicated in child abuse — all 10,000 or so of them.⁷⁰ Can actions over Facebook defamation be far behind?

X. CYBER-BULLYING: A PARTICULARLY CHALLENGING PHENOMENON

A series of tragic teen suicides over the last several years, especially that of B.C. teenager Amanda Todd, has sensitized Canadians to a particularly harmful new version of an old problem, what is usually referred to as “cyber-bullying.”⁷¹ This is relevant here because what distinguishes cyber-bullying from the traditional version is that it occurs by way of electronic communication and in particular via social media. As a recent leading study by the Nova Scotia Task Force on Bullying and Cyber-bullying has noted,⁷² the use of social media has a magnifying effect on the bullying practices in several ways. Notably, the bullies are emboldened by the lack of human interaction and the resultant lack of immediacy of consequences or their observation. Also, while one can leave the schoolyard and escape live bullies, the sheer amount of online activity by teens means that they stay accessible to the bullies via their chosen and most necessary means of communication, social media. The scope of the bullying can be magnified as a result; in the Amanda Todd case, many of the individuals identified as having been involved in the bullying had never met Todd and simply “piled on” the antisocial behaviour for pure entertainment’s sake.

We note in passing that this is another place where we think the social media “generation gap” arises. Many adults, particularly older ones, are likely to respond to such problems by saying something like “well, just stay off the internet.” This reaction fails to recognize two things. First, such a statement is the equivalent of “stop going outside” or “stop opening your eyes” to most younger people. Second, the internet is no longer a place you “go to,” but rather a place that comes to you — given cell phones (and texting and tweeting thereon), everyone is connected to everyone nearly all of the time.

We raise this issue for two reasons. First, it seems clear that cyber-bullying is something that will be encountered by courts as it can have relevance across a spectrum of legal areas, whether it be criminal prosecutions, civil suits for infliction of mental suffering, or even negligence actions against school boards or the social media platforms themselves. The Supreme Court of Canada recently issued a deci-

⁷⁰ Paul Tweed, “Lord McAlpine and the High Cost of Tweeting Gossip” *The Guardian* (27 November 2012), online: <<http://theguardian.com>>.

⁷¹ “B.C. Girl’s Suicide Foreshadowed by Video” *CBC News* (11 October 2012), online: Canadian Broadcasting Corporation <<http://www.cbc.ca/news/>>.

⁷² Nova Scotia Task Force on Bullying and Cyber-bullying, *Respectful and Responsible Relationships: There’s No App for That* (2012), online: <<http://antibullying.novascotia.ca/taskforce>>. And see, most recently, CCSO Cyber-crime Working Group, *Cyber-bullying and the Non-Consensual Distribution of Intimate Images: Report to the Federal/Provincial/Territorial Ministers Responsible for Justice and Public Safety* (2013), online: <<http://www.justice.gc.ca/eng/rp-pr/other-audre/cndii-cdncii/index.html>>.

sion in a cyber-bullying case⁷³ where a teenager was a victim of a “spoofed” Facebook page that made derogatory and sexualized remarks about her. The applicant sought pre-action discovery of information which would allow her to identify the perpetrators and sue them in defamation, but was denied anonymization and a sealing order by the motions and appeal courts.

The Supreme Court permitted the teen to continue the proceeding anonymously, concluding (by way of an extraordinary amount of judicial notice) that the harm to a teenage victim of sexualized bullying by publicization of the information in the case could be presumed. This is a fairly major case as to procedure and the limits of the “open court principle,” amply demonstrating the impact social media are having on the law.

The second reason for raising cyber-bullying is to echo the findings of the Nova Scotia Task Force, to the effect that while there are legal mechanisms that can help to address some of the effects of the problem, social media can produce or facilitate socially harmful phenomena which exceed the ability of the law to resolve.⁷⁴

XI. CONCLUSION

The Americans have need of the telephone, but we do not. We have plenty of messenger boys.

— *Sir William Preece, chief engineer of the British Post Office, 1876.*

No single conclusion can be drawn unifying all of these disparate areas of law and their interactions with social media. The thing to recognise is that social media have effected dramatic changes which affect many people’s lives on a moment by moment basis. The reality which users perceive, the network with whom they see themselves as interacting at all times, is different than it would be without the presence of social media. It is not sufficient simply to regard things like Facebook or Twitter as a means of communication, or as a hobby in which some people engage, but otherwise as something which can be ignored. To be unaware of social media today has become like being unaware of television or telephones.

How the law has begun to react to social media is clear in some areas, murky in others. That it needs to develop further is clear. The challenge is for that development to reflect the new reality in which we live.

⁷³ *A.B. (Litigation Guardian of) v. Bragg Communications Inc.*, 2012 SCC 46, 2012 CarswellNS 675, 2012 CarswellNS 676 (S.C.C.).

⁷⁴ Task Force on Bullying, *supra* note 72.