Surveillance and spectacle: eighty-four observations on citizen journalism, social media, mobile devices and mobs

Jesse Hirsh

No mistakes, no forgetting: privacy in the age of social media

Kent Glowinski

November 2011

Commissioned by the Office of the Privacy Commissioner of Canada

Wired NDNAD Graphic – detail - Jan Thorp (Creative Commons)

Table of Contents

About the Authors

Kent Glowinski is an Ontario lawyer residing in Ottawa. He obtained a Bachelor of Arts degree from McGill University and a J.D. from the University of Victoria, British Columbia. He has been both in private practice and has worked for the Information and Privacy Commissioner of British Columbia, the Information and Privacy Commissioner of Ontario (OIPC), and the Government of Canada. While at the IPC he specialized in privacy issues surrounding social media. He has written extensively on privacy and consumer protection issues, including a recent paper on consumer rights to challenge information on consumer credit reports, as well as editorials in several recognized Canadian newspapers.

Jesse Hirsh is an internet strategist, researcher, and broadcaster based in Toronto, Canada. He has a weekly nationally syndicated column on CBC radio explaining and analyzing the latest trends and developments in technology using language and examples that are meaningful and relevant to everyday life. Educated at the McLuhan Program at the University of Toronto, his passion is educating people on the potential benefits and perils of technology.

Disclaimer: the views expressed are those of the authors and not those of the Office of the Privacy Commissioner of Canada

Preface from the Office of the Privacy Commissioner of Canada

From Seattle to Syria, from Lebanon to London, from Mexico City to Montreal, we have seen over the past decade an increasing saturation of surveillance. Whether from individuals or institutions, in the hands of police or protestors, miniaturization, mobile devices and new media now mean that while we may stand in public space, our presence in duly registered, recorded and increasingly reproducible for whatever reason. The devices we use and depend upon, the nature of interactive media we consume, the smart technologies we incorporate into our daily lives have now converged. In doing so, they also overturn many of our comfortable assumptions about privacy.

As both a technological phenomena and social reality, the 2011 riot in Vancouver demonstrates that Canada is now facing these issues head on. With the emergence of new kinds of citizen journalism and mobile camera technologies, we also have new potential breaches of privacy. With a view to informing the debate around these issues, the OPC commissioned two independent papers by Jesse Hirsh and Kent Glowinski. The authors lead us to consider some possible legal protection for privacy within social media.

We gave each writer separate sets of related issues to treat, asking them to approach these questions as they best saw fit to general thought and debate. Should authentication be required for certain websites? Should tort law be expanded to loss of reputation through social media? Is there room for regulation of surveillance technology in general? Should we discuss, as in Europe, enshrining a right to be forgotten? Should we develop a legal regime for redistribution of personal information by third parties? In their own way, each examines the underlying and unprecedented privacy issues. We hope the discussion between them will help us all assess and redefine privacy in this new context.

Surveillance and spectacle: eighty-four observations on citizen journalism, social media, mobile devices and mobs by Jesse Hirsh

The Rise of the Social Media Journalist

1. Social media, along with the software and devices that fuelled its development, might be generally viewed as a new phenomenon. Despite this new packaging however, the basic premise is very old. Capturing gossip, stirring emotion and debate, repackaging confrontational reality for the instant gratification of audiences has been going on as long as there have been polities to control. The difference now is that a broadcast tower, or printing press, is no longer part of the equation.

2. Mass media is no longer required to reach a mass audience. And even if payment can still be proffered for a scoop, the expectation is that the best eyewitness evidence of an unexpected public spectacle will turn up online first, and then reported on for the evening news or morning newspaper afterward. Citizen journalists are just more likely to be near a spontaneous scene than a professional one.

3. More significantly, though, this ability to distribute images through the internet can also tell a story that corporate outlets would be inclined to overlook.

4. Pocket cameras captured much of the action on the streets during the G20 Summit of June 2010, in spite of efforts by police to disrupt any filming and intimidate activists, through actions like the arrest of a security activist for tweeting about his counter-surveillance activities.

5. The activism that was sparked in Toronto during a similar meeting of world leaders in June 1988, along with the heightened intensity of demonstrations outside events like the World Trade Organization conference in Seattle in 1999, compelled authorities to designate a specific protest zone at Queen's Park. But the militarization of city streets heightened tensions for everyone.

6. What was supposed to be a space in which dissenters could express themselves without disruption, though, turned into an environment in which police exhibited intolerance toward anyone who was seen as a threat to their authority. Besides, the world leaders were a half-hour walk — and an impermeable security fence — away from the protest lawn.

7. The general mismanagement and accompanying absurdity of this situation received relatively little attention before the summit. And when the subsequent march morphed into vandalism, largely perpetuated by the Black Bloc members who were conscious about having their faces filmed, the spectacle distracted from the real story that played out through social media.

8. And eventually, the clout of the material posted to Twitter and YouTube served to transform the narrative. Comments about how officers were abusing their power in dealing with wrongfully arrested peaceful protesters, and a contentious "kettle" that detained bystanders for several hours after the summit itself ended, gained more poignancy after the fact. Gradually, the mainstream media tide turned, as the vast majority of G20 charges were dropped — and the behaviour of law enforcement became the subject of scrutiny.

9. The first reaction from the authorities was to discredit any video evidence of wrongdoing — particularly the one involving a violent takedown of a protester — on grounds that details could have been edited out, or selective frames removed. Public suspicion increased, however, when police appeared reluctant to identify themselves. What were they trying to hide behind that blue line?

10. Revelations that all the chaos was fuelled by a misinterpretation of a "secret law" passed by the province — which gave police excessive powers — and the regret expressed over the "kettling" contributed to the infamous aftermath of how G20 security was handled by authorities. One individual was granted bail after a year in custody for the offense of pointing to potential security holes — efforts that might have been appreciated under less confrontational circumstances.

11. As the aftermath of the summit continues on, including recent news that nine officers disciplined as a result of removing their name tags during G20 protests were turned down for promotions, it has shown how social media can play a role in overturning official versions of events and transforming the narrative of authority.

12. Moreover, the vast majority of the over 1,100 people arrested had their charges dropped. The power of social media to influence public opinion, therefore, also prevented a great citizens many from being humiliated for something police ought to have known was perfectly legal.

The Power of Attention and Social Media

13. While the identities of many of those photographed amidst the Stanley Cup Riots remained a mystery, in part because no charges were immediately laid, one couple did not hesitate to bask in the attention after a picture circulated of them on the pavement in the line of charging officers.

14. What was initially interpreted as a photo of a young man and woman getting a perverted thrill out of a passionate smooch, as Vancouver burned all around them, turned out to capture a moment where an Australian visitor was comforting his girlfriend after she fell to the ground in the path of shield-wielding police.

15. The image became iconic even before the actual story behind it was known. Before long, the couple was identified via Facebook, along with the man's father praising his son for "making love not war" — and not, as the linked news story suggested, "turned on by tear gas."

16. The kissing couple then eagerly submitted to the follow-up interviews that are now part and parcel of becoming a viral internet celebrity. After all, even if their six-month relationship wasn't meant to last forever, the young man figured it could help his stand-up comedy career.

17. So, when Vancouver police got around to putting up their own website to help identify 40 suspects at the beginning of September — at which point there were still no charges laid— the most famous shot related to the riots had no criminal implications whatsoever. The kissing couple, though, owed their feel-good fame to the fact that they were swept up in the chaos. And at least one of them was pursuing celebrity status beforehand.

18. Were the circumstances that found all those other suspects on the scene all that different? Would all the guys in question have resisted temptation to riot if they were accompanied by girlfriends who needed comfort? Big city streets are inevitably filled with revellers after the local team plays a big game. The contest sparks a desire to whoop it up with people who want to express some communal pride.

19. And there's still no apparent virtual surrogate for being swept up in the moment — that's why most of those 150,000 people were already outside to watch the game on big screens even if they had access to the same broadcast at home.

20. Win or lose, some reaction to the final game wasn't unexpected, given how similar circumstances resulted in 1994. But the peaceful enthusiasm that enveloped the city during the Winter Olympics led some to expect a more harmonious scene.

21. What failed to be considered, according to the official review, was the degree to which alcohol stoked a spirit of civil disobedience. Caution about inappropriate public behaviour was cast to the wind in this drunken environment. The rush of participating in a riot trumped rational worries that there might be cameras capturing all the chaos. Police couldn't possibly detain all the perpetrators, anyhow.

22. Rioting would be seen as wrong by everyone under more rational circumstances. But, when it's happening all around you without immediate ramifications, who wants to be right? Can we fault participants for living in the present without fear of consequence when an entire society acts as such?

23. Social media is a game where attention fuels your score. The sight of a burning police car triggers the immediate acknowledgement that it would make an awesome profile photo. And, in an age when it can be incredibly scarce, attention is an end that can be justified by almost any means.

Mobs beget Mobs and Vigilante Journalism

24. The website developed by the Vancouver Police Department to help identify riot suspects based on photos has offered an explicit description of what it plans to do with any tips from the public. Once a suspect is located, they will be investigated, arrested and have their criminal charges forwarded for charge approval. The investigation team also advises against re-posting the pictures through any social media website — as the material is copyrighted.

25. Police can't really monitor where the images are shared, let alone commented on behind their backs, but the caution reflects the experience of having a mob on the street become a counter-mob on the web. Criminal cases might then be compromised if suspects are hung out to dry ahead of a trial.

26. The officer in charge of the Integrated Riot Investigation team posted a note on the riot suspect website in an effort to clarify expectations. One local investigator cited "the CSI effect" for feeding the illusion that crimes can be solved in under an hour, along with

the misconception that instant messaging can lead to instant justice. "If you are in favour of speed," wrote the police officer "you are in favour of acquittals and lighter sentences."

27. Nonetheless, the swift reaction by the British system to the August 2011 riots led many to wonder if Canada should pick up the pace. Not even the 41 people who turned themselves in to Vancouver police had been charged after two months — while some U.K. residents who encouraged rioting and looting via Facebook were sentenced to four years in prison a week later.

28. The mayhem across England opened up a new layer to the issues surrounding civil unrest. Social media platforms, along with presumably confidential messages relayed through BlackBerry Messenger, became the focus of efforts to dissect why people took to the streets in what started out as a protest against a fatal police shooting, but escalated into something else altogether.

29. There must have been a reason why young Britons felt that setting fires and grabbing merchandise through broken windows was worth their energy. But this was an answer that couldn't be found with a Google search.

30. Research in Motion, whose BlackBerry system was a popular mobile option across all demographic groups in the U.K., thus became the focus of investigations into the instigation. Despite its promise of privacy, though, RIM had no choice but to express a willingness to cooperate with authorities if they were legally obligated to trace user details.

31. The promise of a highly encrypted messaging service might not have been the reason for all of its riot-prone subscribers, but it probably facilitated a feeling that BBM couldn't be easily intercepted. Consequences associated with being indiscreet on public social media could extend to private services, too. Police in Canada have raised similar hackles about Facebook and Skype, borne by echoed concerns about crime and public safety.

32. And as we spend more of our professional and social lives online, the easier it has become to volunteer an ultimately traceable trail of questionable behaviour. So, even if we're not the ones wilfully leaving the evidence behind, someone else might be monitoring.

33. Misinterpretations or mistaken identities based on the presentation of facts can leave permanent scars, however. Particularly when the legal system has a defined concept of serving time or paying fines. Google doesn't seem to be as forgiving. In this case, a perception of history may not be written by the winners, but those who have the greatest control over the spin — or an ability to manipulate search engines.

Violence and Media

34. Traditionally, journalists have been trusted as the intermediary between police and the public. Crime and other safety-related stories drew wide audiences that, in turn, attracted advertising dollars. None of this would've been possible without an overall feeling of trust.

35. As more people had access to self-publishing platforms, though, the mainstream media could be held up to scrutiny. With information once selectively used in the reporting process being increasingly made public online — without a filter — editors and reporters were theoretically subject to a higher standard, or risk having their credibility shot down by the unvarnished truth.

36. With these developments, more readers started to wonder if they should trust journalists at all, particularly the ones working for an organization tied to corporate interests or political points of view. The watchers were now just as likely to be watched.

37. This climate has been accompanied by the proliferation of cameras — including in the hands of law enforcement. While the law-abiding majority may not be bothered by all the surveillance, on the premise that it is also giving them greater security, it has annoyed those who are most aware of the growing number of electronic eyes. Particularly when it has been shown that closed-circuit television systems haven't deterred criminal behaviour as much as complicated it.

38. Riots are an amplification of what has generally been wrought by the increase in CCTV. Those who know criminal activities might be filmed will draw in co-conspirators to make their activities seem less circumspect. And a more elaborate criminal operation will result in more victims.

39. Limiting access through personal technology, as openly contemplated by British Prime Minister David Cameron, isn't feasible either. Particularly when the social networks

accused of prompting people to riot could rally even more people to help clean up the streets the morning after.

40. When the online communication and social media tools are used constructively – as opposed to destructively and irresponsibly – the medium itself becomes more credible than any single user or individual, more powerful than any government authority.

41. The challenge for our society now networked and wired as it is, is to acknowledge the exceptional difficulty for traditional notions we associate with the rule of law to hold given the discursive instant effects of new media.

42. Open courts, unbiased jurors, procedural fairness and due process were hammered out over centuries, in a legal world based on ink and paper. From all sides, we hear that none of that really matters anymore.

43. Quite the contrary, for if the rule of law is to continue, it must be democratized from the bottom up, open-sourced and rendered transparent and accessible, so that it reflects the values and culture of society as a whole, as it evolves.

44. Riots and social unrest around the world, while often driven by genuine social concerns, have also become inextricably linked to the use and spread of social media. Canada witnessed this profound shift in two recent events that took place one year apart: the political protests adjacent to the G20 Summit in Toronto in June 2010, and the Stanley Cup Riots following the loss by the hometown Vancouver Canucks in June 2011. And, in both instances, social media played a central role in amplifying and recording the chaotic events.

45. Our ability to respond to, and possibly regulate, these emerging phenomena will require an understanding of the context in which the disruptive events occurred. While our cultural environments often tend to seem invisible, they can also be incredible sources of insight towards where we are headed — rather than simply where we currently are.

46. The emergence of these new tools for personal expression and observation was more unexpected than the events in which they factored, as the G7 Summit had sparked controversial protests in Toronto in 1988, and Vancouver experienced a Stanley Cup Riot after a Canucks loss in 1994. Police officers that anticipated their responses based on chaotic street scenes of the past, though, were faced with a different set of technology-driven circumstances two decades later.

47. The ever-accelerated information age has nurtured a “fear of missing out” that has cemented our limited attention span to the immediacy of the moment, rather than the

rationality that comes with perspective and consequence. Because of the rapid flow of social media, and the rush that comes with getting an instant reaction, rabid users are fixated upon capturing the "now." Sharing an experience has become an integral part of an experience. For example, when it comes to being on the scene for potential confrontations with authorities, the proliferation of cameras can actually contribute to a greater spirit of accountability.

48. Yet, an imbalance of power between state and citizen has continued to pose challenges. Based on the experiences in Toronto and Vancouver, the widespread use of social media often complicated the clashes, and fuelled further online hostility after the fact. Both government and critics exploited their recordings of the event, neither giving ground.

49. The power of the social media-fuelled quest for attention can help justify any action in the heat of the moment. Facebook friends will be impressed by any picture from the midst of a newsworthy event — plus, when it comes to getting the perfect profile photo, the more dangerous the better. This can descend quickly into a thrill-seeking dynamic – the political equivalent of celebrity.

50. No matter how much effort is expended to intimidate young people through the tools of a surveillance society, a feeling of safety can still be found in the mob — as exemplified by people with decent jobs and stable backgrounds who were caught looting across England in August. Across the West, as populations age, a generational conflict is brewing. Youth in the US, UK and Canada, previously just resented, are now increasingly feared and subject to widening surveillance and control.

51. Mobs also beget mobs. And when there's no more attention to be reaped from witnessing havoc on the streets, the social media exhibitionist can change their spots and become an online vigilante, by expressing disdain for the very behaviour that they revelled in the night before.

52. Can we fault the contemporary consumer of online news for internalizing the age-old journalistic aphorism that if it bleeds it leads? Now that the broadcasting tools are accessible to anyone with a hand-held device, a greater awareness of the laws that resulted in a generally civil Canadian mainstream media might be necessary, although the chaos might also force a new model of regulation.

53. Perhaps we have witnessed the emergence of a new culture, which is able to hold power accountable in once-unimaginable ways, which will require the justice system to catch up. We have bloggers at the ready in every press conference, YouTube footage of

every significant police action, cell phone video of every political speech and off-the-record quip.

54. Does the technological shift provide greater hope for our society going forward? Or, will any sense of order be permanently replaced by the social media spectacle?

Conclusion: the Seductive Power of the Spectacle

55. Fear of missing out — also known as "FOMO" — has turned into the defining diagnosis of our times. The current social compulsion to keep tabs on all the detail streamed through social media consumes the attention of people from all ages and backgrounds, whether that means subconsciously peeking at a Smartphone at a dinner party, or dedicating an abundance of time to being an online voyeur.

56. Constant access to information about the real-time experiences of other people doesn't compensate for wanting to be part of a communal experience, though. The digital map is not the territory. Rather, updates about an event happening nearby will increase the desire to rush to the scene to witness it first-hand.

57. The network effects can certainly be positive — like catching a spontaneous "flash mob" performance by a Christmas choir, or scrawling a chalk tribute to Jack Layton, not to mention overthrowing a dictator in the Middle East. But the same impulses have also played a role in events with negative consequences.

58. Twitter was cited as a contributing factor to the violence that followed the last game of the Stanley Cup finals, if only because a message posted by one user in the minutes following the Canucks loss read, "Get ready for a riot, Vancouver."

59. Still, one publicly posted line did not spur 150,000 people to wreak havoc in the streets — especially when many of them were already there. Too often we forget, in the heated immediacy of events, that art and technology are mirrors, not hammers. Social media just reflect a wider reality; their ability to shape events is often overestimated.

60. Rather, the anticipation of another riot was based on the chaos of 1994, when the technology to relay these messages was in its prenatal state, and certainly not transmitted to devices that people kept in their pockets. Twitter was not around to blame back then. And neither were the teenagers who were motivated to riot.

61. Here is the paradoxical state we find Canada in. The digital generation has come of age in a world where cameras are everywhere along with the ability to relay those images to

the rest of the world within seconds. We have reared an entire generation in monitored schools, CCTV-scanned buses, watched and gated neighbourhoods.

62. Shouldn't those under 25 have been the most self-conscious about their public behaviour? How could they not realize or be aware of the extent to which their exploits would be recorded, when it was mostly their fellow revellers holding the cameras?

63. But they shed inhibition and abandoned intuition as they were caught up in the moment. This is a cohort raised with web cams and texting, reality television and celebrity blogs. A sense of consequences can easily be eclipsed by a fear of missing out.

64. However, in the aftermath, a different kind of mob emerged. And its vengeful behaviour was arguably more of a threat to our social norms, cohesion and trust than any burning car or broken window. A compulsion to identify and shame individuals suspected of rioting spawned public Facebook groups, and other photo websites, with the anticipation that names could be instantly attached to any visible faces.

65. Who needs the slow-grinding rigours of the Canadian justice system, after all, when a mob of online vigilantes were at the ready to perform a simultaneous cyber-trial and execution?

66. Surveillance replaces law, in this model. Cameras become the jury, anonymous bloggers the judges, everyone and no one the executioner. The corrosive effect on our justice system and rule of law comes instantaneously.

67. For those who wanted to blame and shame any rioters that could be easily identified through posted snapshots, the method was inevitably effective. Most prominently, a 17-year-old water polo star was vilified for a picture that showed him attempting to light a police car on fire. A public apology for being caught up in the moment wasn't enough to keep the young man from being suspended from the team, while his father was forced to suspend his medical practice, as the family fled its home.

68. For citizens in 21st century Canada, a purportedly educated and enlightened country, to resort to this form of ostracism and revert to a kind of frontier justice is remarkable. First, individuals take surveillance practices and tools into their own hands, next they seem to take the very law upon themselves.

69. Had a similar picture circulated in 1994, the teenager's fate would have been predominately determined by the criminal justice system — partly due to protections afforded a young offender, and partly due to the lack of channels through which to shame him. The forward steps afforded by personal technology could actually be pushing our sense of citizenship and community backwards.

70. Personal publishing platforms can result in suspects being wrongly identified and humiliated prior to an arrest or trial. They also empower potential pranksters. It doesn't take much for an outrageous comment to go viral — especially if the timing is right.

71. A status update posted to Facebook by one individual, who boasted of an improbable series of violent confrontations with police during the Stanley Cup Riots, generated plenty of outrage as it made the rounds online. But the supposed confession still drew less morbid curiosity than the apparent perpetrator who was bullied into revealing himself.

72. Anyone with a naive belief that online communication would inevitably bring us closer to accuracy and shared understanding is now likely re-examining their faith. The rush to judgment by online vigilantes has already begun to undercut our courts, communities and the basics of justice that we have developed in Canada over a century. Fear of missing out takes on a different definition in this situation. Find yourself in the wrong place at the wrong time — or even related to someone who is — and all of the supposed protections that the system affords can be very quickly stripped away.

Post-Script: Towards Regulation of Citizen Surveillance?

73. Little can arguably be done to control how people use technology. We can teach people about new tools, but restricting and binding their use is a heavy hand to play, and ultimately futile. However, if society develops a greater understanding of the implication of its abuses, it could contribute to a less confrontational culture overall. Technological exposure might desensitize us, but experience and education can counter-act that conditioning.

74. Conversely, as more people find their personal indiscretions, or unflattering criticism of their past behaviour, turning up in search results, the long-term damage may even be cancelled out. Individual mistakes may simply vanish into the digital noise of others' myriad misfortunes.

75. Certainly, embarrassing personal details that once might have tarred the reputations of people running for office just a few years ago are now passed over as trivial, on the basis that this kind of thing could happen to anyone. But because this kind of latitude still varies by jurisdiction, and generation, it may take some time for voters to turn a blind eye to the rear-view mirror.

76. Yet even the tabloid media have been forced to be more mindful of context. Prior to the last federal election, a Sun Media report that Jack Layton was caught by police in an unlicensed massage parlour 15 years before his electoral triumph was seen by the public as more tawdry than the anecdote itself.

77. Therefore, if greater embarrassment could emerge from drawing attention to the perceived misdeeds of another person online than the alleged offense itself, most would resist the easy temptation to violate privacy. Do we need a mechanism to shame those who shame, or simply insist on knowing their motives?

78. The emergence of increased authentication policies — like website comments being administered through Facebook and the controversial insistence by Google that its social network users have to be verified by their real names — suggests companies are trying to encourage and even enforce civility and responsibility online.

79. Journalism has been defended as a profession because of the accountability that comes with running a business, which includes being mindful of tort law. This culture of control may not be in place online. Yet, the most popular administrators of user-generated content have developed standards, in part because of the liabilities associated with spreading libel. As people who spread information online start to recognize the potential implications of what they post, photos of civil disobedience posted online to encourage informants and identification may actually backfire. Armchair policing can also lead to lawsuits or prosecution.

80. Police attempts to suppress monitoring of their conduct can backfire too, of course, as seen in the aftermath of the G20 Summit. The video of an officer ordering a protester not to blow soap in his face led to an animated satire of “Officer Bubbles” — who then gained further infamy after suing people who commented about him on YouTube for defamation. While the legal manoeuvre was seen as ridiculous, the officer also gained wider public recognition for it, and sightings of him on the job are reported on Twitter. Debate over his confrontation also raised the question as to whether any qualified officer in such a situation might wonder if the liquid being blown his way was simply soap.

81. So, what if the “kissing couple” of the Stanley Cup Riots were revealed to have taken to the streets in search of a violent thrill? Would they be seen as more deviant than the teenage water polo player photographed holding a rag and lighter near a police car gas tank?

82. The court of public opinion might already be more powerful than the court of law, if only because the former has the advantage of instantaneous speed and global reach. Public opinion has room and capacity to try all of us, all the time, and forever. While the court of law should never aspire to such alacrity, it will nonetheless have to acknowledge the perceived gap in relevance, accessibility and authority.

83. Technology is often mistakenly regarded as a force of nature whose impact is inevitable and whose regulation is impossible. Culture, on the other hand, tends to have its impact underestimated — especially a culture with no obvious precedent prior to this new century.

84. Canada has a long history in the field of cultural regulation, however. Governance of social concerns developed over decades, giving serious consideration to what the public wanted or feared, called for or hoped for. Maybe it's time for a similar process to be applied to the use and regulation of technology, explicitly surveillance technology — and the power of attention.

No mistakes, no forgetting: privacy in the age of social media by Kent Glowinski

"One cannot too soon forget his errors and misdemeanours; for to dwell upon them is to add to the offense."
- Henry David Thoreau

"No man is rich enough to buy back his past."
- Oscar Wilde

Sitting across from Bob (not his real name) in the café, you would never guess that this 60-something middle-class businessman from rural Canada had been a drug-dealer, smashed a few cars in drag-racing when he was a teenager, and has an active criminal record. What you would see is a clean-shaven, respected member of the local Chamber of Commerce, operating a successful restaurant with his family. Like most people whose youths were lived before 1990, Bob had the right to be forgotten. He did some stupid things when he was younger, paid the price for it, and then grew up. As anyone can see, he became a productive, useful member of Canadian society. Like every single person has done at one point, he made mistakes.

However, with the introduction of social media (Facebook, Twitter, Myspace, etc.) and the near universal use of digital devices, Canadians no longer have the right to be forgotten, and the stakes are high for making a mistake. Whereas pre-social media, a crime in small-town Canada may have been committed, hit the local paper, and then been filed into microfiche in a dusty, old public library; post-social media, that crime is likely being simulcast, tweeted, or posted on Facebook, with the dual consequences of providing the state with a perfect package of criminal evidence against the perpetrator, but also the more insidious, lifetime, online record which can be used to shame, harass and malign the perpetrator into perpetuity.

It's not that people are making any more or less bad decisions than in the past. Many people are doing today what Bob did forty years ago: vandalism, school-yard fights, or smoking a joint at a party. The difference for Bob is that no objective permanent record of most of those indiscretions remains. Witnesses forget, memories fade, and people forgive. *Time heals all wounds*. But, with social media, the documenting, recording and posting of the same indiscretions renders them permanent and timeless. Once they are tweeted, and then re-tweeted and then re-tweeted, the information has been stamped into the permanent electronic archive. Perhaps an apt expression would be: *timelessness does not let wounds heal.*

Pre social media, Bob and his generation also had the benefit of an institutional news media that was contained by region, too costly to compete against, required educational credentials

to enter, could be readily identified and compelled to follow the law, and (although this is debatable) voluntarily adhered to a code of journalistic ethics. Post social media, however, anyone with a cell phone camera and a Twitter account can broadcast information *about other people* - thus making them citizen journalists. Only, unlike pre-social media institutional journalists, post-social media journalists are everyday people, likely not versed in laws meant to protect privacy, such as those protecting the identities of accused persons under eighteen years of age[1]. Simply put, social media has helped to create an entire practice of vigilante journalism.

With all this in mind, the world after the introduction of social media is a world where one's personal information cannot be contained or controlled. Despite federal and provincial privacy commissioners advocating for users of social media to take advantage of tokenistic privacy settings[2] in those social media applications, one's attempt to control his or her own privacy is trumped by the fact that no privacy settings exist to stop other people from posting personal information about someone else on social media applications[3]. For example, the function of 'tagging' photographs of other people on Facebook or tweeting, blogging or posting information about someone else without their consent or knowledge.[4]

In effect, post social media, attempts to boycott or avoid the use of social media applications do not insulate individuals from having their own personal information posted online. Whether we like it or not, we are on the grid.

Bob's generation may be the last to have unwittingly enjoyed the right to make mistakes, the right to be forgotten, and to have had the privilege of 'starting over' - to have had the ability to metaphorically walk into the mountains and disappear, insulated and separated from the rest of society.

Post social media the world is less forgetting and thus less forgiving. A mistake has a worldwide audience, and thus a worldwide amount of shame, moral outrage, and memory. A joyride recorded and posted online goes from being a moment of bad judgment and reckless spontaneity to a dangerous driving conviction; a minor act of vandalism captured on a digital

[1] *Youth Criminal Justice Act*, S.C. 2002, c. 1, section 110: (1) Subject to this section, no person shall publish the name of a young person [defined as a person under 18 years of age], or any other information related to a young person, if it would identify the young person as a young person dealt with under this Act.

[2] See, for example, Elizabeth Denham, Assistant Privacy Commissioner of Canada: *Report of Findings into the Complaint filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc. under the Personal Information Protection and Electronic Documents Act*, 16 July 2009.

[3] Libel and slander law will still protect individuals from false and harmful information posted about someone on a social media application; however, at common law, 'truth' is a complete defence to allegations of libel and slander – meaning that truthful posts, photographs or information, however harmful, are not against the law.

[4] Facebook's *Terms of Use* (Date of Last Revision: 26 April 2011) do state, under the heading *Protecting Other People's Rights*: 9. You will not tag users or send email invitations to non-users without their consent. The privacy settings default is that 'tags' are permitted and can only be removed *ex post facto*. One must actively change the privacy settings to pre-screen 'tags'. This is also a fairly recent privacy setting addition.

camera and posted to Facebook is considered an act of terrorism and the offender, offender's family and employer receive death threats.[5] Mistakes are exaggerated and multiplied, eternally and digitally archived, and through ever-changing and refined internet search algorithms become the baseline things that define our worldwide reputation for the rest of our lives. *The genie cannot be put back in the bottle*. Thanks to social media, we are slaves to the most embarrassing moment, illegal act or inappropriate behaviour in our past.

This paper will discuss the evolving Canadian jurisprudence and legal treatment of social media, especially in light of some citizens' seeming willingness to actively share and broadcast self-incriminating information about involvement in crime, fellow citizens' appetite to capture and broadcast information on criminal behaviour of other citizens (citizen-on-citizen surveillance or citizen journalism), and law enforcement's pro-active monitoring of and engagement in social media.

As will be discussed, privacy is not so much a right in and of itself, but a "cluster of rights". What that cluster of rights is at any given moment changes with societal values, jurisprudence, and political will (or lack of it). In this post social media world, what that cluster does not include is the right to be a little bit bad – and get away with it. Victimless crimes and petty bad behaviour are not brushed off, because they are now visible, broadcast, and *remembered*. This is the most fundamentally troubling part: second chances no longer exist. There is no delete function. There is no edit function. There is no box to append a personal statement or provide a little bit of context. There is no 'Are you sure?' prompt when you are about to post something stupid, illegal or inappropriate.

There is no *un-remember.*

What is privacy and what is the right to privacy?

"I never said 'I want to be alone.' I only said 'I want to be let alone.' This is all the difference."
- Greta Garbo

There is no one conclusive definition of "privacy".

On the Treasury Board of Canada Secretariat's website, the Treasury Board explains privacy as follows:

[5] Vancouver Sun: *Employers of Vancouver riot participants victims of public backlash* (22 June 2011) and *Rioting teen Nathan Kotylak and family face backlash, forced to leave home* (20 June 2011)

> "In a classical or historical sense, privacy has meant "the right to be left alone". In the 21st Century however, privacy has taken on a multitude of definitions. To some it means the right to enjoy private space, to conduct private communications, to be free from surveillance and to respect the sanctity of one's body."[6]

The Office of the Privacy Commissioner of Canada defines privacy as:

> "...the right to control access to one's person and information about one's self. The right to privacy means that individuals get to decide what and how much information to give up, to whom it is given, and for what uses."[7]

It is also important to consider the legal definition of privacy and the differences between privacy as a civil cause of action *between citizens*, and privacy as a constitutional right and protection as *between the state and its citizens*.

From a civil, legal perspective, there is no common law cause of action specifically covering "invasion of privacy" in Canada, only statutory ones in various provinces. In Ontario, Courts have now conclusively decided that there is a tort of invasion for "intrusion upon seclusion" after several years of musing that the cause of action may exist[8]. In British Columbia, while there is a provincial *Privacy Act,* RSBC 1996, c 373[9] which permits actions based on a statutory cause of action, it is difficult to determine the general quantum of damages for invasion of privacy alone as lawsuits for privacy breaches are almost always part of a larger defamation action. Of all the provinces, Quebec would appear to have the strongest civil protections for citizens' privacy, with the *Code Civil du Quebec,* LRQ, c C-1991[10] and the Quebec Charter of Rights*, la Charte des droits et libertés de la personne,* LRQ, c C-12 specifically recognizing privacy as a fundamental human right[11]. In actual civil litigation in Québec, however, privacy breaches rarely result in significant damage awards – leading one to question the actual importance of privacy as a human right in Québec[12].

---

[6] Treasury Board of Canada Secretariat website: http://www.tbs-sct.gc.ca/pgol-pged/piatp-pfefvp/course1/mod1/mod1-2-eng.asp, accessed August 2011.
[7] Treasury Board of Canada Secretariat website: http://www.tbs-sct.gc.ca/pgol-pged/piatp-pfefvp/course1/mod1/mod1-2-eng.asp, accessed August 2011 and speech by Privacy Commissioner of Canada, speech given at the Freedom of Information and Protection of Privacy Conference, 13 June 2002.
[8] Court of Appeal of Ontario, *Jones v. Tsige*, 2012 ONCA 32, January 18, 2012.
[9] See subsection 1(1) of the B.C. *Privacy Act: It is a tort, actionable without proof of damage, for a person, wilfully and without a claim of right, to violate the privacy of another.*
[10] Article 35 of the *Code Civil du Québec* reads: *Every person has a right to the respect of his reputation and privacy. No one may invade the privacy of a person without the consent of the person unless authorized by law.*
[11] Article 5 of *la Chartre* reads: *Every person has a right to respect for his private life.*
[12] A review of Québec jurisprudence puts basic privacy breach damages in the $5,000 range.

On a federal level, the *Personal Information Protection and Electronic Documents Act,* S.C. 2000, c 5 ("*PIPEDA")* provides a statutory cause of action against an organization that has been found to have breached the *Act*, but a pre-condition of commencing an action is making a complaint to the Privacy Commissioner of Canada and waiting for either a finding or a complaint discontinuance from the Commissioner[13]. The investigations that lead to these findings can take months or years even.[14]

In terms of privacy as between the state and the citizen, such as when law enforcement is investigating crime or conducting searches, it is section 8 of the *Charter of Rights and Freedoms,* and evolving jurisprudence, which defines a citizen's right to privacy in Canada.

As Canadian criminal and regulatory law jurisprudence has established, the "right to privacy" is not a stand-alone right, but a cluster of rights depending on circumstances and context. Courts determine whether a right to privacy exists based on a judicial test known as the *reasonable expectation of privacy* test, which, as will be discussed below, appears to be a moving target.

Section 8 of the *Charter of Rights and Freedoms* states:

> "Everyone has the right to be secure against unreasonable search or seizure."

The Supreme Court of Canada has found that section 8 includes the constitutional right to privacy, in particular:

> "In cases involving s. 8, the appropriate starting point is the reasons of this Court in *Hunter*, supra. In that decision, Dickson J. (as he then was) held that the reasonableness of searches and seizures would be measured by balancing the state's interest in law enforcement against the individual's interest in privacy. However, he also held that the *Charter* could not, and did not, protect against any and all intrusions by the state into the lives of individuals. Rather, s. 8 would only be implicated if the individual who was claiming a *Charter* breach could show that he or she had a reasonable expectation of privacy in the place searched or the material seized. If no such expectation exists, there can be no *Charter* breach, as s. 8 only protects people, not places or things."[15]

But the right to privacy, as determined by the Court, is often fact-specific and lacks a principled judicial test that would allow citizens to accurately decipher when they do have a reasonable

[13] *PIPEDA,* subsection 14. (1).
[14] Jennifer Stoddart, Privacy Commissioner of Canada: *Making Privacy Protection More Effective for Canadians,* Remarks at the Centre for Law, Technology and Society of the University of Ottawa, 19 January 2011, Ottawa, Ontario.
[15] *Schreiber* v. *Canada (Attorney General),* [1998] 1 SCR 841 at para. 18

expectation of privacy. The concept of privacy is simply too abstract and the legal decisions to date have been inconsistent and confusing:

> "The degree of privacy which the law protects is closely linked to the effect that a breach of that privacy would have on the freedom and dignity of the individual. Hence, a person is entitled to an extremely high expectation of privacy in relation to his or her bodily integrity (as in *R*. v. *Stillman*, 1997 CanLII 384 (S.C.C.), [1997] 1 S.C.R. 607, or *R.* v. *Dyment*, 1988 CanLII 10 (S.C.C.), [1988] 2 S.C.R. 417) or residence (see *R.* v. *Feeney,* 1997 CanLII 343 (S.C.C.), [1997] 2 S.C.R. 117), and entitled to a much lesser expectation in relation to a vehicle in which he or she was merely a passenger (as in *Belnavis*, supra) or an apartment to which he or she was a visitor (as in *Edwards*, supra)."[16]

Keeping in mind that Courts are concerned with the judicial test of whether a citizen has a reasonable expectation of privacy, how have contemporary Courts viewed citizens' reasonable expectation of privacy in relation to social media?

The legal status of social media in relation to the reasonable expectation of privacy

"My wife and I had decided not to let anybody take pictures of our home because it was just the last place on earth we had that was unscathed. But people have climbed over the fence; they've taken aerial shots. They've gotten my address and put it on the Internet."

- Steven Tyler

The leading judgments on the right to privacy in relation to social media have been primarily from civil cases in which a party to the litigation wants to get access to the opposing party's Facebook, Twitter or Myspace account in the context of discovery.

In the New Brunswick case *Carter* v. *Connors*, 2009 NBQB 317, Justice Ferguson granted the Defendant's motion to have access to the Plaintiff's Facebook page for the purposes of discovery. In concluding his decision, he stated:

> "…I believe that the probative value of the information requested is of such a level that its disclosure will not infringe upon a reasonable expectation of privacy. That is so because the information sought is not, at least at this stage of proceedings, information that could qualify as revealing very personal information over which most right thinking

[16] *Schreiber* v. *Canada (Attorney General),* [1998] 1 SCR 841 at para. 19

> Canadians would expect a reasonable expectation of privacy. Put another way, it does not reveal: "intimate details of the lifestyle and personal choices of the individual."[17]

It would appear that one's privacy settings on Facebook are also irrelevant when it comes to Courts permitting access to the content of a Facebook page. As Justice Brown stated in *Leduc* v. *Roman*, 2009 CanLII 6838 (ON SC):

> "A party who maintains a private, or limited access, Facebook profile stands in no different position than one who sets up a publicly-available profile."[18]

Although, in *Schuster* v. *Royal & Sun Alliance Insurance Company of Canada*, 2009 CanLII 58971 (ON SC), in the same level of Ontario Court as *Leduc*, Justice Price concluded the decision with:

> "The Plaintiff has set her Facebook privacy settings to private and has restricted its content to 67 "friends." She has not created her profile for the purpose of sharing it with the general public. Unless the Defendant establishes a legal entitlement to such information, the Plaintiff's privacy interest in the information in her profile should be respected."[19]

Photographs of parties posted to social media profiles have been admitted as evidence relevant to demonstrating a litigant's ability to engage in sports and recreation: *Cikojevic* v. *Timm*, 2008 BCSC 74; *R. (C.M.)* v. *R. (O.D.)*, 2008 NBQB 253; *Kourtesis* v. *Joris*, [2007] O.J. No. 2677 (S.C.); and *Goodridge (Litigation Guardian of)* v. *King*, 161 A.C.W.S. (3d) 984 (Ont. S.C.). In one case, photographs of a party posted on a MySpace webpage formed the basis for a request to produce additional photographs: *Weber* v. *Dyck*, [2007] O.J. No. 2384 (S.C.).

In short, it would appear that in the current state of the law, Canadians *may* have a reasonable expectation of privacy in their social media profiles and information posted to social media accounts; however, it is unlikely that heightened social media privacy settings or claims of privacy will trump the Courts', and likely law enforcement's, ability to access such information. The only way for a citizen to have true, legal privacy rights in relation to social media websites and applications is to avoid having accounts or profiles on social media websites and applications in the first place. Even if one takes all precautions to avoid the use of social media, one's personal information may still end up exposed through social media as a result of the actions of fellow citizens.

[17] *Carter* v. *Connors*, 2009 NBQB 317 at para. 38.
[18] *Leduc* v. *Roman*, 2009 CanLII 6838 (ON SC) at para. 32.
[19] *Schuster* v. *Royal & Sun Alliance Insurance Company of Canada*, 2009 CanLII 58971 (ON SC) at para. 53.

Citizen journalism and/or citizen-on-citizen surveillance

"Journalism largely consists in saying "Lord Jones is dead" to people who never knew Lord Jones was alive."
- G.K. Chesterton

It's almost funny to look back to 2002 and think that closed-circuit television cameras (CCTV) in public spaces were the pressing issue on the minds of Canadian privacy commissioners. George Radwanski, then Privacy Commissioner of Canada, called the video monitoring of public places "the most urgently important privacy issue facing Canadian society today."[20]

Not even a decade later, the concern is less over state-controlled surveillance and its implications for citizens' privacy, but citizen-controlled surveillance of each other through digital devices and information published and broadcast to social media (and, in turn, likely to be read by law enforcement). The 2011 Vancouver, B.C. Hockey Riot provides a valuable example: it was not official state-surveillance that led to most arrests of the alleged perpetrators; it was that every citizen with a cell phone and every business with a camera formed a private network of complete public surveillance.[21]

As a result of the presence of digital devices in the proximity of the Vancouver riot, the Vancouver Police were provided with millions of incriminating images and videos of rioters by other citizens[22]. Further, various social media groups were set up by citizens, not law enforcement, for the sole purpose of identifying rioters in order to help police lay charges against alleged perpetrators.[23]

Citizens conducting surveillance on other citizens, or acting as "citizen journalists" raises another set of troubling questions: what are the legal limits to broadcasting or publishing photographs and personal information of other persons on social media applications - especially in the context of pending criminal charges or legal action?

However, the first major dilemma is that there exists no objective definition of "citizen journalism." Effectively, it is a self-identifying term, where anyone with a blog or Facebook page can adopt the title. There is no education required, no self-regulatory body, and no need to

[20] CBC In Depth: *Canadian security, Security cameras, Someone is watching: should we worry?,* Last updated 9 February 2007, http://www.cbc.ca/news/background/cdnsecurity/cameras.html, accessed August 2011.
[21] Vancouver Sun*: Dedicated Facebook users continue search for culprits*, 6 August 2011, http://www.canada.com/vancouversun/news/westcoastnews/story.html?id=d67d3ef7-19f6-49d2-add5-dcf8f5531a3b&k=85157.
[22] CBC: *1 million riot photos sent to police*, 19 June 2011, http://www.cbc.ca/news/canada/british-columbia/story/2011/06/19/bc-stanley-cup-riot-charges.html.
[23] CBC*: Facebook groups aim to ID rioters, help clean up*, 16 June 2011, http://www.cbc.ca/news/canada/british-columbia/story/2011/06/16/bc-riot-vancouver-facebook.html.

apply. It also means that it is difficult to determine whether or not a citizen is engaging in "journalism" when sharing others' photos and personal information through social media applications.

Mark Glaser, editor of the blog *Media Shift* attempts to describe citizen journalism as follows:

> "The idea behind citizen journalism is that people without professional journalism training can use the tools of modern technology and the global distribution of the Internet to create, augment or fact-check media on their own or in collaboration with others…
>
> […]
>
> One of the main concepts behind citizen journalism is that mainstream media reporters and producers are not the exclusive center of knowledge on a subject the audience knows more collectively than the reporter alone."[24]

Whereas the traditional mainstream media is limited to the form and content of its reporting through regulation and editors, and can be sanctioned through legislation and court-ordered publication bans, citizen journalists who publish through online social media still fall within a grey area of the law. As a striking example, Ontario's *Libel and Slander Act*, R.S.O. 1990, c. L.12 applies to words "broadcast" or published in a "newspaper" and provides broadcasting and newspaper defendants with a window of six weeks in which they must receive notice of the defamation as a precondition to a defamation lawsuit being launched. With the advent of the internet and social media, Ontario courts have had to grapple with the question of whether words on a blog or social networking website constitute a "broadcast" or publishing in a "newspaper."

In the Ontario Court of Appeal decision *Weiss* v. *Sawyer*, 2002 CanLII 45064 (ON CA), the Appeal Court declined to decide whether an online version of a newspaper was, in fact, a "newspaper" as defined in the *Libel and Slander Act.* However, in the case of *Ottawa-Carleton District School Board* v. *Scharf*, 2007 CanLII 31571 (ON SC), at para. 27, Justice Morin found:

> "The libel in this case was not contained in a newspaper or in a broadcast. It was published by way of e-mail, fax and posted on a website. Arguably then, the notice required by Section 5 (1) of the Act is not required to be provided to the defendants."[25]

[24] Mark Glaser, *Digging Deeper: Your Guide to Citizen Journalism*, MEDIASHIFT, 27 September 2006, http://www.pbs.org/mediashift/2006/09/digging_deeperyour_guide_to_ci.html, accessed August 2011.

In short, it would follow that citizen journalists posting information to social media applications would not benefit from the same protections afforded to traditional mainstream newspaper, radio and television broadcast media in certain civil actions.

But perhaps there is good reason to decline to provide certain legal protections to citizens who take it upon themselves to publicly post photographs, commentary and personal information of other people online when purporting to act in the capacity of citizen journalist.

As Molly A. Dugan, Assistant Professor of Journalism and Communication Studies, California State University at Sacramento, argues in her paper, *Journalism Ethics and the Independent Journalist,* citizen journalists are not subject to any editorial review or consequences for incorrect or harmful content, there is no ethical code of conduct to follow, there is no requirement to avoid or declare conflict of interest, and there is no need to correct inaccuracies.[26]

Similarly, Andrew Keen, author of *The Cult of the Amateur: How Today's Internet is Killing our Culture*, spoke with CBC Radio in 2009 about whether citizen journalists, in the age of social media, are noble amateurs or nosy busybodies:

> "Citizenship and journalism have nothing to do with one another and when you bring them together, it's very dangerous because what you're saying is anyone who wants to improve the world should go out and report it so virtue then replaces professionalism. Good intention makes one a good journalist and that results in incompetence.
>
> I don't have a problem with democratizing the media, provided that there are editors and competent people involved in the process. My problem with the blogosphere and with the web 2.0 revolution is the idealization of amateurs, the innocent, the old sort of Rousseau notion that the child knows more than the adult so I'm all in favour of new more irreverent magazines or online periodicals coming along and challenging conventional wisdom."[27]

---

[25] *Ottawa-Carleton District School Board* v. *Scharf*, 2007 CanLII 31571 (ON SC) at para. 27.

[26] Molly A. Dugan, Assistant Professor of Journalism and Communication Studies, California State University at Sacramento, *Journalism Ethics and the Independent Journalist*, McGeorge Law Review, Vol. 39, Issue 1, University of the Pacific, McGeorge School of Law. Dugan notes that the four cornerstones of journalistic ethics from the Society of Professional Journalists are: 1. Seek the Truth and Report It, 2. Minimize Harm, 3. Act Independently, and 4. Be Accountable.

[27] CBC Radio: Transcript: *Andrew Keen's views about 'News 2.0'*, CBC Radio Sunday Edition documentary News 2.0. Series air date on CBC Radio: Sunday, June 21 and Sunday, June 28, 2009, http://www.cbc.ca/news/canada/story/2009/06/17/f-transcript-andrew-keen-news-20.html.

Furthermore, citizen journalism and non-commercial citizen-on-citizen surveillance is not subject to any provincial or federal legislation. The *Privacy Act,* R.S.C., 1985, c. P-21 [28] only applies to information held by government institutions, as do provincial *Freedom of Information and Protection of Privacy* legislation. *PIPEDA*[29] only applies to personal information that is collected, used or disclosed in the course of commercial activities, and it is highly unlikely citizen journalists are conducting commercial activities. It is of note that *PIPEDA* also contains a limiting clause in paragraph 4(2)(c) that exempts personal information obtained by an organization for commercial, journalistic purposes. It is unsettled law whether a citizen journalist is, in fact, able to engage in commercial "journalism" as recognized in *PIPEDA.*

One also wonders if citizen-on-citizen surveillance, conducted not for commercial reasons, but only for the purpose of providing incriminating evidence against the target of the surveillance to law enforcement, renders that citizen conducting surveillance an agent of the state, along with all of the requisite legal and constitutional restraints?

As the reaction to the 2011 Vancouver riot on social media websites also underscores, citizen journalism does not believe itself to be bound by the legal constraints that traditional media must respect. Take, for example, the posting of photographs and identification information by citizens of accused persons who were implicated in the riot. Many accused were under the age of eighteen years, thus protected by Part 6 of the *Youth Criminal Justice Act*, S.C. 2002, c. 1: Publication, Records and Information, Protection of Privacy of Young Persons. Despite this legal prohibition, many of their photographs and identifying information appeared online.

Specifically, section 110 of the *Youth Criminal Justice Act* states*:*

> "110. (1) Subject to this section, no person shall publish the name of a young person [defined as a person under 18 years of age], or any other information related to a young person, if it would identify the young person as a young person dealt with under this Act."

A case in point was a 17 year-old who was caught on video allegedly lighting a Vancouver Police car on fire. His photo was posted on social media websites across the world, leading to him being publicly identified on such social media applications and, in turn, broadcast through

[28] Section 2 of the *Privacy Act* states "The purpose of this Act is to extend the present laws of Canada that protect the privacy of individuals with respect to personal information about themselves held by a government institution and that provide individuals with a right of access to that information."
[29] Subsection 4(1) of *PIPEDA* states: "This Part applies to every organization in respect of personal information that (a) the organization collects, uses or discloses in the course of commercial activities."

mainstream media[30]. No doubt he became the lightning rod for rage directed at Vancouver rioters when it was learned he was a private-school educated, elite polo player, who came from a life of privilege – rather than a member of a small group of organized anarchists, as was commonly (and wrongly) believed were most rioters.[31]

Keeping the *Youth Criminal Justice Act* in mind, the entire policy basis behind not naming or identifying young persons who committed crimes is centred upon the right to be forgotten, to engage in youthful indiscretions and to then start over[32]. For this individual, he will likely not have the benefit of ever living down his alleged role in the 2011 Vancouver riot. Does one always have the right to be forgotten? Likely not.

Courts also grapple with citizen journalism when attempting to impose publication bans in cases where a young person is a complainant or is the accused, or a matter is so sensitive that it should be heard in the absence of media. Justice Molloy explains in *R*. v. *G.C.,* 2009 CanLII 89067 (ON SC) that publication bans, in a time of social media, may not be effective. At para. 28:

> "There is also a very real concern about the effectiveness of any ban that I might impose. This trial will be conducted in a public courtroom. The court has no real means to police the broadcasting of information, whether innocently or deliberately, by those who attend the trial. Given the proliferation of twitter, facebook postings, blogs and the general posting of information on internet sites, a publication ban might well serve only to restrict responsible reporting by established media and do nothing to control the general dissemination of information. (See *R.* v. *Puddicombe*, April 2, 2009, per Benotto J. at para. 19.)" [33]

All this leads to the troubling realization that, more and more, it is fellow Canadian citizens, and not the state, who are conducting surveillance, encroaching on the privacy of other citizens, and actively working with law enforcement to indentify and implicate others involved in bad behaviour and criminal activity. While citizen journalism may not benefit from certain protections of the law, it also operates outside of constraints of ethics, regulation and legal and

---

[30] CBC*: Vancouver rioter outed as elite athlete: Water polo organization suspends player during probe,* 17 June 2011*,* http://www.cbc.ca/news/canada/calgary/story/2011/06/17/calgary-vancouver-riot-athlete.html.

[31] See, for example, the editorial piece by Brian Hutchinson in the Full Comment section of the National Post in which he quotes Vancouver Mayor stating that "the violence, he repeated was caused by "a small group of troublemakers." *Organized 'anarchists' were not behind the Vancouver riot*, Brian Hutchison, National Post, 16 June 2011, http://fullcomment.nationalpost.com/2011/06/16/brian-hutchinson-organized-anarchists-were-not-behind-the-vancouver-riot/.

[32] Subsection 3(b) of the *Youth Criminal Justice Act* specifically identifies the policy issues underlying the law: (b) the criminal justice system for young persons must be separate from that of adults and emphasize the following: (i) rehabilitation and reintegration, (ii) fair and proportionate accountability that is consistent with the greater dependency of young persons and their reduced level of maturity, (iii) enhanced procedural protection to ensure that young persons are treated fairly and that their rights, including their right to privacy, are protected.

[33] *R*. v. *G.C.*, 2009 CanLII 89067 (ON SC).

privacy obligations. With this in mind, even one's attempt to control personal information in the post social media era will inevitably fail as others, often without one's consent or knowledge, are sharing and broadcasting one's personal information.

Law enforcement and social media: an on again, off again affair

"I've never had a problem with drugs. I've had problems with the police."
- Keith Richards

Social media is, to a certain extent, an unregulated world where governments must decide to intervene or not; mostly because, while social media may facilitate crime, it also provides an easy stream of self-incriminating idiots who allow law enforcement to pick off low hanging fruit and secure prosecutions.

2011 was the *Year of the Riot*, yet police forces cannot seem to reach a consensus on how they feel about social media. On one hand, social media helped the Vancouver Police obtain millions of incriminating photographs of the perpetrators of the 2011 Vancouver riot; on the other hand, the British government claimed social media was the cause for the 2011 North London riots and considered ways to limit Facebook and Twitter during times of social unrest[34].

While British law enforcement mulls a ban on social media, it still wants to retain the control to conduct surveillance on citizens and obtain incriminating evidence from the very same medium[35]. In a sense, law enforcement wants to have it both ways. For the United Kingdom, this is not surprising. While on the surface, the United Kingdom appears to be a progressive, Western society that respects basic human rights, many credible organizations have pointed out just how sad the state of privacy is in the country. For example, in 2007, *Privacy International*[36], a well-known non-profit organization, released a comprehensive worldwide rating of how well 47 different countries protect privacy. For the United Kingdom, *Privacy International* had the following to say:

> "A recent and widely publicised ranking of 47 countries by the privacy rights watchdog Privacy International found the UK's level of surveillance to be "endemic", worst among EU countries and on par with Russia, China, and Singapore. The previous Labour government's tough crime policy and its large parliamentary majority resulted in an unprecedented number of new laws limiting human rights, including freedom of

[34] BBC: *England riots: Government mulls social media controls*, 11 August 2011, http://www.bbc.co.uk/news/technology-14493497.
[35] The London, England police used Facebook as a way to charge several individuals involved in the 2011 North London riots – something they would have likely been unable to do so quickly without social media.
[36] See their website at https://www.privacyinternational.org, accessed August 2011.

> assembly, privacy, freedom of movement, the right of silence, and freedom of speech, leading the former Information Commissioner to warn that the UK was "sleepwalking into a surveillance society".[37]

As for Canadian privacy protections, *Privacy International* stated in its worldwide rating that Canada had "Some safeguards, but weakened protections", which is only one level better than the United Kingdom. It is of note, however, that Canada dropped in its privacy protection rating from the year before, that being "Significant protections and safeguards."[38]

It can be argued that the United Kingdom's greater appetite to interfere with privacy rights likely comes from its recent history of domestic terrorism involving Northern Ireland. But with the waning of such domestic terrorism, privacy-intrusive legislation has simply been misused for other purposes. As Michael Mansfield, QC, a British barrister, noted in *The Telegraph* newspaper:

> "Organisations have been accused of misusing the Regulation of Investigatory Powers Act, originally intended to tackle terrorism and organised crime, by applying the legislation to trivial matters such as littering and dog fouling."[39]

It is also of note that the United Kingdom has 4.2 million CCTV cameras posted in public spaces in Britain - about one for every 14 people.[40] The number of CCTV cameras in Canada is impossible to determine as there is no national network of cameras and their usage is still fairly limited[41].

So, although law enforcement has claimed that social media has caused or facilitated crime, it is still more than willing to use social media to its own advantage – especially in the surveillance society of England.

---

[37] Privacy International: *United Kingdom - Privacy Profile*, 26 January 2011, https://www.privacyinternational.org/article/united-kingdom-privacy-profile, accessed August 2011; and, Privacy International, *Leading surveillance societies in the EU and the World*, September 2006-2007, https://www.privacyinternational.org/article/leading-surveillance-societies-eu-and-world-2007, accessed August 2011

[38] Privacy International, *Leading surveillance societies in the EU and the World*, September 2006-2007, https://www.privacyinternational.org/article/leading-surveillance-societies-eu-and-world-2007, accessed August 2011.

[39] The Telegraph: *Britain's surveillance society 'beyond Orwell's worst fears', warns Michael Mansfield,* 2 September 2009, http://www.telegraph.co.uk/news/uknews/law-and-order/6125068/Britains-surveillance-society-beyond-Orwells-worst-fears-warns-Michael-Mansfield.html.

[40] BBC: *Britain is 'surveillance society': Fears that the UK would "sleep-walk into a surveillance society" have become a reality, the government's information commissioner has said*, 2 November 2006, http://news.bbc.co.uk/2/hi/uk_news/6108496.stm.

[41] Surveillance Camera Awareness Network (SCAN): *A Report on Camera Surveillance in Canada, Part One, January 2009,* http://qspace.library.queensu.ca/bitstream/1974/1906/1/SCAN_Report_Phase1_Final_Jan_30_2009.pdf, accessed August 2011: "It is difficult to know exactly the current number of open-street surveillance cameras in Canada because the systems are in frequent flux, depending on the local situation. By 2007, at least fourteen Canadian cities had implemented open-street cameras and at least sixteen municipalities were considering initiating camera schemes or had considered camera surveillance in the past."

The British government fails to see the irony that, thanks to two North London riot organizers having publicly posted their "event" on Facebook in the first place (and this is not a joke: "Warrington Riots" - with a date, time and location - for "massive Northwich lootin"), in less than a week after the riot, a British court was able to quickly determine guilt and to sentence the pair to four years in prison[42]. The severity of the punishment, however, will be discussed further on.

Clearly, law enforcement is happy to receive evidence that makes the investigation and prosecution process efficient and easy. It is also no surprise that, considering there is likely very little reasonable expectation to privacy on one's social media profiles, police often gladly surf through social media applications looking for evidence or admissions of wrongdoing.

Both in Canada and the United States, law enforcement regularly reviews Twitter updates, Facebook profiles and blogs. In one example, the New York City Police set up a special unit to patrol social networks for evidence of gangs, rowdy house parties and other potential criminal activity by juveniles. Police in Toronto are also using social networks to help with investigations[43]. It does not hurt public acceptance of law enforcement's practice of snooping into social media with positive news like the NYPD's social network unit catching a murderer in March 2011 after he admitted to killing someone at a house party on his Facebook profile[44].

With self-incrimination via social media posing a real risk of arrest, another question is raised: are citizens aware of their *lack of* legal rights vis-à-vis what they post on social media? Do they have a basic understanding of what reasonable expectation of privacy they *do not* have in their social media activities?

Tony Wilson, a Vancouver lawyer, writes about the stupidity of some people willing to self-incriminate on social media websites during the 2011 Vancouver hockey riot in *Canadian Lawyer Magazine*:

> "Some of these rioters were pretty stupid. I mean "bag-of-hammers" stupid. One guy all over the papers here is the poster boy for bad behavior and self-incrimination. Assuming his Facebook page wasn't hacked by someone showing him rioting... [h]is Facebook page read the early morning of the riot "Maced in the face, hit with a baton, tear gassed twice, 6 broken fingers, blood everywhere . . . Through the jersey on a burning cop car,

[42] CBC: *U.K. riot Facebook page authors get 4 years: British courts fast-track riot sentences with 24-hour sessions*, 17 August 2011, http://www.cbc.ca/news/world/story/2011/08/17/britain-riots-sentence.html.
[43] San Francisco Chronicle: *PRIVACY: Law enforcement's monitoring worries civil libertarians*, 13 August 2011, http://articles.sfgate.com/2011-08-13/business/29883179_1_facebook-and-twitter-facebook-updates-social-media.
[44] New York Daily News: *NYPD forms new social media unit to mine Facebook and Twitter for mayhem,* 10 August 2011, http://articles.nydailynews.com/2011-08-10/local/29887819_1_social-media-facebook-and-twitter-kamisha-richards.

> flipped some cars, burned some smart cars, burned some cop cars, I'm on the news . . . one word . . . history :) :) :).” [45]

While it is easy to blame the police for going on “fishing expeditions” to find crime online, who could resist keeping a fish that jumped right into the boat?

To say the least, social media has been quite friendly to Canadian law enforcement, making the investigation and prosecution of crime much easier. A review of case law supports the assertion that social media, such as Facebook and Myspace, are a solid evidentiary tool for Canadian police and that courts are open to accepting social media posts and profiles as evidence at trial. Often that evidence is self-incriminating and was unwittingly produced by the accused.

In *R*. v. *Huxford*, 2010 ONCJ 33, the accused was sentenced to six months of prison time after attempting to purchase a handgun online. In the humourous judgement, Justice Nicholas notes that the accused was “posing on Facebook like a player” and stated at paras 2 to 3:

> “Fortunately for police, Huxford had no privacy settings on his Facebook page. Det. Obrien easily accessed his Facebook Page without needing to be added as a friend and observed Huxford holding what appeared to be a Glock handgun. He was able to identify the accused through the photos he had posted on Facebook and a police mug shot. Huxford had posted his name, date of birth and phone number on his page. Police were able to confirm that he did not possess a firearm licence, or a firearm acquisition licence, and did not have any firearms registered.”[46]

In *R*. v. *Sather*, 2008 ONCJ 98, the accused was originally charged by police with threatening to cause death or serious bodily harm due to postings he made on his Facebook page, but was finally acquitted of those charges after the defence's expert witness testified that:

> “…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.”[47]

In *R.* v. *Tscherkassow*, 2010 ABPC 324, the accused was convicted of assault after the Court was presented with his Facebook status updates directly after the attack “I superman punched a guy”. The accused had tried to convince the Court that the Facebook post was just an

[45] Canadian Lawyer Magazine*: The morning after the night before, Letter from Law Land*, 27 June 2011, by Tony Wilson, http://www.canadianlawyermag.com/3756/the-morning-after-the-night-before.html.
[46] *R*. v. *Huxford,* 2010 ONCJ 33.
[47] *R*. v. *Sather,* 2008 ONCJ 98.

"embellishment" to impress his military buddies and provided inconsistent testimony at trial, but at para. 137 of the judgment, Justice Kerby stated:

> "This admission/statement on Facebook is not a minor inconsistency. I find I cannot rely on his evidence. I do not think he is being truthful. He's not a credible or reliable witness. I do not believe his evidence."[48]

Tscherkassow demonstrates that Facebook postings, an objective record from a point-in-time, provide Courts with credible evidence that will be hard for an accused to explain away or live down.

2011 Vancouver riot aside, recent high-profile cases of people posting their own crimes online, and then being subsequently arrested and charged, have gained attention, including:

1. A gang rape of a 16-year-old girl at a party in Maple Ridge, B.C. that went viral on Youtube, Facebook and Myspace[49]. It is also of note that, due to the video being immediately uploaded to a social networking website after the assault, the R.C.M.P. were unable to contain the spread of the video and it still continues, to this day, to circulate on social media websites;
2. An Oregon man posting a Youtube video of himself driving 220km/hr on a highway[50]. When arrested, the man stated his intention was to post his speed, and subsequent arrest, on Youtube; and
3. Several high-school fights recorded with digital devices and uploaded to social networking websites and Yotube, such as a fight at Hamilton, Ontario's Cathedral High School in which a 14 year-old was charged with aggravated assault[51], the "Nicole Vs. Taylor Bitch Fight" involving Kamloops, British Columbia high school students[52], and six students from Grey Highlands Secondary School in Flesherton, Ontario attacking one other student at lunch hour and now facing criminal charges.[53]

It would appear that social media is providing law enforcement with an invaluable tool to discover crime, obtain evidence, identify perpetrators and secure convictions.

What is most alarming, however, is the willingness of certain individuals to so freely admit guilt through social media applications, post full accounts or recordings of their crimes and,

---

[48] *R.* v. *Tscherkassow,* 2010 ABPC 324.
[49] Globe and Mail: *Photos of gang rape go viral on Facebook*, September 16, 2011, http://www.theglobeandmail.com/news/national/british-columbia/photos-of-gang-rape-go-viral-on-facebook/article1710072/.
[50] Toronto Star: *Man jailed after filming himself going 220 km/h,* February 14, 2011, http://www.thestar.com/wheels/article/938336--man-jailed-after-filming-himself-going-220-km-h.
[51] CHCH: *Teen charged in YouTube fight,* January 21, 2011, http://www.chch.com/index.php/home/item/1839-teen-charged-in-youtube-fight.
[52] The Kamloops Daily News: *School district investigates YouTube fight video*, 9 June 2011, http://www.kamloopsnews.ca/article/20110609/KAMLOOPS0101/306099985/-1/kamloops/.
[53] National Post: *Lunchtime assault posted on YouTube, six students face criminal charges*, 3 June 2011, http://news.nationalpost.com/2011/06/03/lunchtime-assault-posted-on-youtube-six-students-face-criminal-charges/.

accordingly, self-incriminate. Criminal law scholars estimate that there is a need for a confession in order to secure a conviction in approximately one in every four cases[54]. This means that social media could help improve the statistical chance of conviction - as social media use becomes more prolific and its users become more comfortable with posting risky confessions online.

Law enforcement's use of social media does not only help to secure convictions, however, it also helps to discover crime that would otherwise not be reported in the first place. From political, societal and legal perspectives, is this a positive thing? Without down-playing the serious consequences of certain crime, some crimes going unreported would have absolutely no negative impact on the world and society in general. Take the example of an individual speeding, alone, down a deserted highway at high speeds qualifying for dangerous driving under the *Criminal Code.* If no one ever discovers this victimless crime has occurred, there is no impact[55]. However, if posted to a social media website and discovered by police, this crime becomes known, the individual is charged and likely convicted, and obtains a criminal record. With this criminal record, the individual's ability to travel and secure certain employment (amongst other consequences) will be impacted for the rest of his or her life.

And this is why law enforcement's use of social media has helped to take away the right to be forgotten. Petty crime and vandalism, speeding, and school-yard fights are often youthful indiscretions in which all people engage at some point in their lives. But should these mistakes tar and feather someone's future reputation? Do these minor crimes thus warrant state intervention and a life-time of metadata that reappears each time a human resource department does an internet search check on a prospective employee?

Just like directly paying a repair shop to fix someone else's car after a minor fender-bender, instead of alerting the insurance company to avoid the long-term consequences of increased premiums and loss of driving points, sometimes it's just better to let things go.

Stupid Mistakes 2.0

"Be not ashamed of mistakes and thus make them crimes."
- Confucius

[54] University of Utah College of Law: *Handcuffing the Cops: Miranda's Harmful Effects on Law Enforcement*, NCPA Policy Report No. 218, August 1998, by Paul G. Cassell, http://www.ncpa.org/pdfs/st218.pdf.
[55] I do concede that the opposing side could argue that there may be a deterrent effect on this individual so that he or she does not engage in this behaviour again and possibly save future lives.

In the 2004 judgement *Barrick Gold Corp*. v. *Lopehandia*, 2004 CanLII 12938 (ON CA), Appeal Justice Blair said of defamation on the Internet:

> "Internet defamation is distinguished from its less pervasive cousins, in terms of its potential to damage the reputation of individuals and corporations, by the features described above, especially its interactive nature, its potential for being taken at face value, and its **absolute and immediate worldwide ubiquity and accessibility**. The mode and extent of publication is therefore a particularly significant consideration in assessing damages in Internet defamation cases." [emphasis added][56]

It comes as no surprise that information disseminated on the internet can be particularly damaging due to its potentially instant and worldwide reach. Whereas traditional media sources were limited to broadcast range by geography, technology and lack of interconnectivity, meaning information would often be limited to specific cities, regions, or social groups, internet facilitates the complete and immediate sharing and re-sharing of information.

But the internet is not social media, and *vice versa*. Information published generally on the internet, on a random unknown website, may garner the odd web-crawl or notice through a search engine; but fundamentally the general internet, accessible through search engine or hyperlink (i.e. by "surfing" from website to website) is a technology that requires user input in order to provide information. This is known as the "push-pull" dichotomy of social media and the internet. Google searches are a form of "pull", whereas algorithm-generated stories or automated wall-posts on Facebook and Twitter are an example of "push".

The result is that post social media websites and applications play a non-stop broadcast function that constantly share, deliver and "push" information to an audience, whether requested or not. Personal information of others is quickly and instantly pushed to third parties who never had the desire or need to look for it in the first place. Details that otherwise would have remained limited by geography or social groups are posted, crawled, processed through an algorithm and blasted to an innumerable amount of users who the social media application (based on past usage or interests) has calculated may have a desire to view the non-requested information[57]. On the other hand, traditional Google or web searches remain constrained by the need for a user to input data. The user has to have some pre-existing knowledge, need or

[56] Barrick Gold Corp. v. Lopehandia, 2004 CanLII 12938 (ON CA) at para. 34.
[57] Science 2.0: How to Get Control on Facebook and How The Algorithms Work, 19 October 2010, by Jean-Sebastien Miousse, http://www.science20.com/science_and_music_your_ears/blog/how_get_control_facebook_and_how_algorithms_work, accessed September 2011.

desire to seek out that information. Similar to the expression *on a need-to-know basis*, internet web searches are rarely initiated by a user looking for absolutely nothing.

It also means that the idea of "control" over personal information in the post social media world is much more difficult. A user may have some control over the appearance of personal information that results when others search on Google: either by its page placement, its link describing content, or the impugned reference to the content itself. For example, one can go to court and attempt to compel search engines to alter or remove content, and thus protect the individual from future "pulls" on that negative information. In the post social media world of Web2.0, it is not only impossible to contain the spread of "pushed" personal information, by the time the individual becomes aware of its existence it is already too late and beyond containable; the fact someone knows about the personal information means it has already been automatically and simultaneously broadcast.

Thus, it is surprising that privacy advocates have not appeared to respond to the stark differences in privacy implications of "push" media versus "pull" media. To be fair, in 2010, the Office of the Privacy Commissioner of Canada did state that it was "looking at the issue" of Google Buzz and the fact that it pushes personal information of recent Google Mail contacts to each other[58]. But the general lack of official interest may simply be due to the fact that it is difficult to differentiate new social media websites and applications that actively push information from the general rubric of 'the Internet.' For many they are one in the same. This difficulty in identifying and differentiating whether a website is part of the old internet or the new "push" media internet, such as Facebook or Twitter, is discussed in *Key Differences between Web1.0 and Web2.0,* a paper prepared by Graham Cormode and Balachander Krishnamurthy of AT&T Labs–Research. In their paper Cormode and Balanchander state:

> "Web 2.0" captures a combination of innovations on the Web in recent years. **A precise definition is elusive** and many sites are hard to categorize with the binary label "Web1.0" or "Web2.0". But there is a clear separation between a set of highly popular Web2.0 sites such as Facebook and YouTube, and the "old Web". These separations are visible when projected onto a variety of axes, such as technological (scripting and presentation technologies used to render the site and allow user interaction); structural (purpose and layout of the site); and sociological (notions of friends and groups)." [emphasis added][59]

[58] CBC: *Privacy commissioner reviewing Google Buzz,* 16 February 2010, http://www.cbc.ca/news/technology/story/2010/02/16/google-buzz-privacy.html.
[59] AT&T Labs–Research*: Key Differences between Web1.0 and Web2.0*, 13 Feburary 2008, by Graham Cormode and Balachander Krishnamurthy, http://www2.research.att.com/~bala/papers/web1v2.pdf.

In fact, Cormode and Balanchander go as far as to call Web2.0 “largely a marketing term.” For many users as well, the issues arising from Web2.0 appear to be less about privacy and more about reputation management and marketing. In short, it’s about looking good. In a 2009 article entitled *Smarter Social Media Distinguishes Push from Pull*, the website Smartertechnology.com made reference to a study conducted by Intel Lab's People and Practices Research:

> “What Intel found was that people are more concerned with maintaining an image than with privacy, and have a clear distinction between the "push" of social media (when people are trying to establish the image of their personal brand) and the "pull" of social media (when people try to attract like-minded cohorts).
>
> Their major finding was that privacy settings at current social media sites are inadequate, since they just allow sharing (friend) or don't allow sharing (not a friend). Whereas what people really wanted most, in the study, was for the non-friends to see a more filtered view of them, one that pushed a carefully crafted image of them, while friends had unfettered access to the pull of more intimate details.” [60]

There is also very little existing academic discussion on the concerning privacy implications of push versus pull dissemination of information on social media. Rather, internet searches on the subject result in overwhelming discussions of the endless marketing potential of “push” via social media: *Forbes Magazine: Facebook Fans Vs. Twitter Followers: Which are More Valuable - One offers push; the other, pull,* October 12, 2010 [61].

Perhaps these are the reasons Canadian privacy commissioners focus mainly on warning users to “control” their own personal information online[62]- while not appearing to notice that third-parties and non-human algorithms are sharing the exact same information (without a user’s consent or knowledge): (1) like most people, the commissioners may not truly understand the difference between Web1.0 and Web2.0; or (2) the commissioners inherently recognize the hopeless impossibility of attempting to control the personal information posted by third-parties about someone else on social media. It may be that the commissioners recognize their own limited ability to regulate and intervene in Web2.0.

---

[60] Smartertechnology.com: *Smarter Social Media Distinguishes Push from Pull*, by R. Colin Johnson, http://www.smartertechnology.com/c/a/Technology-For-Change/Smarter-Social-Media-Distinguishes-Push-from-Pull/, accessed September 2011.

[61] http://www.forbes.com/2010/10/12/facebook-twitter-nike-followers-fans-social-media-marketing-zynga-cmo-network.html, accessed September 2011.

[62] Dr. Ann Cavoukian, Information and Privacy Commissioner of Ontario, *How to Protect your Privacy on Facebook: A Step-by-Step Guide*, http://www.ipc.on.ca/english/Resources/Educational-Material/Educational-Material-Summary/?id=615, accessed September 2011. Although the website notes that the original brochure from May 3, 2007 on protecting privacy on Facebook has been removed due to constant privacy policy changes on Facebook, the general advice still remains*(1) “think before you post” - when posting anything on Facebook ; and (2) users should use the maximum privacy settings for any information that they would like to have restricted to a limited network of social contacts.*

In a sense, Canadian privacy commissioners' mantra about individual responsibility in self-censoring postings on social media websites (i.e. *think before you post*), and choosing the highest social media privacy settings, is apt for a Web1.0 world. However, most (but definitely not all) rational citizens already understand the need to use discretion when posting online and to choose the highest privacy protections on social media websites: a recent May 2010 Pew Research Center's Internet & American Life Project report *Reputation Management and Social Media* indicates that 71% of social networking users ages 18-29 have changed the privacy settings on their profile to limit what they share with others online[63]. In the Web2.0 world, the pressing question for privacy commissioners then becomes: who is protecting citizens from third-parties who push and broadcast personal information about them without their consent or knowledge? Could this be the next major battle on the horizon for Canadian privacy commissioners versus the social media giants?

With the foregoing push-pull dichotomy in mind, it also means that the audience for potential bad behaviour or criminal activity posted on Facebook, tweeted on Twitter, or uploaded to Youtube is limitless – with social media users discovering the content that is "pushed" to them without even having searched for it. Petty vandalism in Nanaimo, B.C. can instantly become a worldwide sensation in minutes. And, with the worldwide attention, a simple act seems legendary, requiring an equally as legendary response by flustered domestic law enforcement desperate to look like they are "taking action" in the eyes of the world.

Little mistakes become large very quickly.

The legal response to the recent British riots is a fitting example of just how small crimes, when committed and broadcast through social media applications, can result in major consequences. Two individuals, both twenty-two years of age, were sentenced to four years in prison for "inciting disorder via Facebook" for their roles in organizing the 2011 North London riot. Their crime? Hosting an "event" on Facebook. Even legal scholars in England have explained that the sentences are disproportionate, and only major, violent crimes such as kidnapping carry such a sentence.[64] Suddenly, organizing a Facebook event morphs into inciting and organizing riots.

The jail sentence for the Facebook riot organizers is not the only example of a heavy-handed response to crimes via social media. Facebook "threats" also resulted in an 18 year-old being

[63] The Pew Research Center*: Reputation Management and Social Media*, by Mary Madden, Aaron Smith, http://www.pewinternet.org/Reports/2010/Reputation-Management.aspx, 26 May 2010.
[64] The Guardian, *England riots: will harsher sentences act as a deterrent?,* 17 August 2011, *http*://www.guardian.co.uk/uk/2011/aug/17/england-riots-harsher-sentences-deterrent.

sentenced to prison (it was believed to be the first time cyber-bullying resulted in jail time)[65]. Badly-written poetry about the emotional impacts of his job, which were subsequently posted on Facebook, led to uttering threats charges against an Ontario Coroner employee who transported dead bodies[66].

Albeit a non-criminal examples of the consequences due to the scope and reach of social media, within minutes of Canadian Cabinet Minister John Baird texting and tweeting that "Thatcher has died", the Canadian Prime Minister's Office started preparing an official Government of Canada response and Buckingham Palace was contacted about former British Prime Minister Margaret Thatcher's death. It turns out that "Lady Thatcher" was actually the name of Baird's sixteen-year-old cat that had just died and the Iron Lady was very much still alive.[67] Or the case of a Québec woman posting to Facebook pictures of herself on vacation, smiling – only to have her long-term depression and anxiety disability benefits cut by her insurance company. Apparently, she did not appear anxious and depressed on her Facebook profile[68].

The result is that indiscretions or crimes committed on, or exposed through, social media websites and applications are treated more harshly, as if the extensive exposure demands an equally as harsh and extensive punishment. Even after the proportionate legal punishment is meted out, the disproportionate punishment of shame via social media continues, demanding a further pound of flesh.

On one hand, advocates of social media espouse the values of free speech, liberalization of large scale mobilization/gatherings of people, and the flow of ideas; but on the other hand, social media ironically requires its users to self-censor and act with extreme restraint, while carefully assessing the risk of associating with others having less than stellar reputations. Whereas an off-colour joke made with no malicious intent, and which could be interpreted as racist or sexist, gets recounted in a small social gathering and quickly dismissed as tasteless, the same act committed on a social media website could lead to the end of a career, criminal investigations, and endless public shaming. A moment of bad judgment, remembered forever, framing one's reputation until death. There are no retention and no disposal periods for that information.

---

[65] Daily Mail: *Facebook bully jailed: Death threat girl, 18, is first person put behind bars for vicious internet campaign*, 21 August 2009, http://www.dailymail.co.uk/news/article-1208147/First-cyberbully-jailed-Facebook-death-threats.html.
[66] *R.* v. *Lee*, 2010 ONCJ 291
[67] CBC: *U.K. press purrs over Baird's 'Thatcher dead' text,* 13 November 2009, http://www.cbc.ca/news/world/story/2009/11/13/thatcher-dead-cat-baird-rumour.html.
[68] CTV News: *Woman loses disability benefits due to Facebook photos*, 23 November 2009, http://www.ctv.ca/CTVNews/SciTech/20091123/facebook_insurance_091123/.

For this reason, I feel sorry for many other teenagers who make one stupid mistake in the post social media world. For them, no punishment is greater than having his name and the lifetime of shame that will come with it. His crime is two-fold: (1) the crime itself, and (2) being unlucky enough to have the commission of it "pushed" through social media.

In the words of Vancouver Lawyer, Tony Wilson:

> "Justice should be merciful. The 18- or 19-year-old from a loving family, who has good grades and a great future but who made a stupid mistake on June 15, 2011 isn't in the same category as the 25-year-old low-life who uses the F-word in each sentence and came to the riot with a hammer and a criminal record under his belt. So convict, and, if warranted, incarcerate the worst of the lot. But show some understanding to first offenders about the mistakes human beings make, especially when they're young. One can only hope it will make some of them better, more responsible citizens when they're old."[69]

Conclusion

I had always told myself that if life got too difficult, I would just sell everything I owned and move to a little European village to sell baguettes and cappuccino to the other townsfolk. I would start over. Disappear. Throw my law degree and writing out the window. Remake myself. Adopt a mysterious, new persona. Become a baker, a waiter, a barista. Live simply. Like in the *Sound of Music* I would walk through rolling hillsides, grass up to my waist, basking in the vastness of the world, and my new-found anonymity.

But, inevitably, my dream of disappearance and re-birth would be short-lived when a tourist with an iPhone would come to town, take a picture of me and the quaint little bakery I serve cappuccinos in, and instantly upload the pictures to Facebook - only to have a former Facebook friend, perplexed by my sudden disappearance, see the photograph of me and tweet to his fifteen-thousand followers that I was found, with hyperlinks to the pictures. And so, the dream would be shattered. Try as I might to avoid it, I would be back on the grid. *Sigh.*

After all of these predictions of gloom, fellow citizen informers ratting each other out, and cops with an increasing appetite for Twitter feeds, everybody wants to know: what are the next

[69] Canadian Lawyer Magazine*: The morning after the night before, Letter from Law Land*, June 27, 2011, by Tony Wilson, http://www.canadianlawyermag.com/3756/the-morning-after-the-night-before.html.

steps? How does one take action to make it all better? How does the genie get stuffed back in the bottle? These are questions that nobody can answer. Some will muse that the answer is to legislate social media, some will advocate for regulation, and others will argue that only an outright ban would be a solution. However, the harms of social media (if there are harms at all), and how to mitigate those harms, are still a part of a greater conversation on the nature of "the Internet" and the practical, political and philosophical ability to regulate it, ban it, or do nothing at all. But, maybe it's not an issue of legislating, regulation or control.

Maybe it's an issue of ever-changing and evolving human relations and empathy. Younger generations, spoon-fed on the internet and maturing into the solid food of social media, may be forced to become more compassionate, forgiving and able to see life in context – because everybody (and I mean everybody) in the post social media era will have skeletons in their online closet.

Like the cringe-worthy photographs of friends with 1980s hair and clothes that everyone would rather forget (but have to accept) perhaps younger generations will just learn to accept that a tainted online reputation, rife with old poetry, immature wayward opinions, and bad behaviour, are the consequences of simply living life and growing up.

Forgiving and forgetting may have to be the new normal in a world where privacy has evaporated and everyone knows just how bad everyone else really is. And, that might make us all better, and less judgmental, people.

"And remember, no matter where you go, there you are."
- Confucius