The New Social Media Paradox: A Symbol of Self-Determination or a Boon for Big Brother?

Sara M. Smyth[1]
Bond University, Australia

Abstract

In the past ten years or so, mobile phone and Internet technologies have been instrumental in nearly every instance where people have gathered to demand political reform. With the help of 'new social media' applications, like Facebook and Twitter, Internet and mobile phone users can conduct real-time exchanges with millions of people across the globe. Following the Introduction, this Article begins, in Part I, with a discussion of how these tools were used by protesters around the world in 2011. Part II discusses how the same tools were used by governments, both democratic and authoritarian, to respond to the violence and mayhem during that year. In Part III, I turn to a discussion of the relevant policy concerns, first in the American, then the Canadian, legal contexts. It is significant that Canada is the first country to complete an extensive investigation into Facebook's privacy practices. As a result, Facebook users across the world now enjoy stronger privacy protections for their personal information, in terms of how it is collected, used and disclosed. In conclusion, I note that this case has important implications for other online social networking sites, even those based in other countries, which are collecting and using the personal information of Canadians in a way that does not comport with Canadian privacy laws.

Keywords: Internet, Canada, Facebook, Twitter, Privacy, Policy concerns.

Introduction

2011 was the year of the protester (Andersen, 2011).[2] The world, as we witnessed, appeared to be poised on the brink of rebellion. The events that precipitated this puzzling period of insurgency began in Tunisia, a small Arab state, where the people's frustration with the ill-treatment and injustice underpinning Zine el-Abidine Ben Ali's corrupt twenty-three year tyranny provoked angry protests, seemingly overnight. It was, in fact, the harassment of a young street vendor named Mohamed Bouazizi, who hailed from the small town of Sidi Bouzid (125 miles south of Tunis), by a female police officer that eventually drove Ben Ali into exile (Shane, 2011).

When Bouazizi, a 26-year-old produce-seller, walked to a provincial capital building to complain that the policewoman harassed him, and received no response from anyone in government, he doused himself with flammable liquid and set himself ablaze (Andersen, 2011). This audacious act of defiance garnered worldwide attention and reverberated

[1]Associate Professor, Faculty of Law, Bond University, University Drive Gold Coast, Queensland 4229, Australia. Email: ssmyth@bond.edu.au

[2] Time Magazine named "The Protester" its most influential "Person of the Year" in 2011.

around the planet. While several produce sellers joined Bouazizi in protest outside the government building, the incident would not likely have sparked dissent throughout Tunisia had it not been for the fact that Mr. Bouazizi's cousin posted a video of the ghastly spectacle on Facebook (Andersen, 2011).

Fervent revolts erupted in other parts of the country, then throughout the Middle East and North Africa, followed by an unprecedented wave of public defiance - in New York, London, Athens, Oakland, Tel-Aviv, and other parts the world - as throngs of citizens took to the streets to declare that the political systems and economies within their respective countries had become stagnant and corrupt; engineered, they claimed, to give preference to the rich and powerful, at the expense of everyone else (Andersen, 2011). What is remarkable is that thousands of people stepped into the role of civilian journalists to share their experiences, through Internet blogs, photos, videos and social networking sites, and demand change (Preston, 2011b). The so-called 'Arab Spring' put the democratic power of social media to the ultimate test and, along with it, exposed the dangers of using new technologies for the purposes of enforcing brutal state crackdowns.

In this article, I explore how social media has become a valuable political tool, not only in the Middle East, but throughout the world. It is an unparalleled instrument for the purpose of mobilization, denouncing state violence and other human rights abuses, as well as enabling democratization. Information technologies are no longer just in the hands of powerful elites; they are widely used, even in the most authoritarian corners of the world, to promote social engagement and revolutionary zeal. At the same time, new social media tools, as well as facial recognition software, are a boon for commercial dealers and totalitarian despots alike.

We can assume that many social media users are not aware of how or why their personal information is being harvested and misused. Indeed, it is very easy to share too much online. Users must be conscious of the fact that crimes are being solved because the perpetrators unwittingly provide information about them on Facebook; and, law enforcement officials around the world are now enlisting private organizations and civilians in the surveillance process. The Vancouver Stanley Cup riots and the UK riots of 2011 provide a good example of how suspects were apprehended because others used their cell phone cameras to record the disturbances and uploaded them to the Internet. As the world witnessed, social media went far beyond merely chronicling public unrest – it generated, coordinated and intensified it. It also provided opportunities for police to tap into an evolving stockpile of personal information.

Increasingly, the protection of personal information and privacy are global concerns. Yet, the United States – where many of the world's popular social networking sites are headquartered - has a robust framework shielding commercial service providers from liability, even when customers are angry that their personal information has been misused and their confidence betrayed. Then again, Internet powerhouses are not immune from accountability; Canada recently compelled Facebook to adhere to its privacy laws, ensuring that the privacy of all people using the site will be better protected from now on.

Following this Introduction, this Article begins, in Part I, with a discussion of how new social media tools were used by protesters in 2011. Part II discusses how the same tools were used by governments, both democratic and authoritarian, to respond to the violence and mayhem that year. I also discuss the use of facial recognition software by government and industry, particularly with respect to online social media tools. In Part III, I turn to a discussion of the relevant policy concerns, first in the American, then the Canadian, legal

contexts. It is significant that Canada is the first country to complete an extensive investigation into Facebook's privacy practices. As a result, Facebook users across the world enjoy stronger privacy protections for their personal information, in terms of how it is collected, used and disclosed. In conclusion, in Part V, I note that this case has important implications for other social networking sites, even those based in other countries, which are collecting and using the personal information of Canadians in a way that does not comport with Canadian privacy laws.

I. New Social Media as an Instrument of Rebellion

In the past ten years or so, mobile phone and Internet technologies have been instrumental in nearly every instance where people have gathered to demand democratic and political reform (Diamond, 2010). Mobile phone technologies are perfect for grassroots organization because they are capable of transmitting and receiving a large volume of messages extremely quickly. With the help of cutting-edge 'new social media' applications, like Facebook and Twitter, Internet and mobile phone users can conduct exchanges with millions of other people across the planet. Indeed, Facebook is now available in seventy languages, and had 901 million monthly active users at the end of March 2012 (Facebook, 2012a). Approximately eighty percent of its monthly active users reside outside Canada and the United States (Facebook, 2012a). The media has characterized the precipitous rise in the number of Facebook users during the past decade in stark terms: the social network can be viewed as the world's third largest country in terms of its population size (Mal & Parikh, 2011).

There is no question that Facebook contains an enormous trove of personal information about its users. Facebook users create online profiles where they can post photos of themselves, list contact information, employment and educational information, as well as their gender, political and religious views, relationship status, and birth date, and post photo albums or personal blog posts. As well, Facebook users accumulate lists of friends that they link to, post public comments on their profiles, and transmit private messages. Facebook users can also join and create groups of people with similar interests, as well as announce events, and invite people to those events. Facebook further allows users to post "status updates" about themselves – everything from what they had for breakfast to the birth of a new baby – and it allows the user's friends to post comments about the status updates.

Facebook also enables people to look up users by name; however, users can configure their privacy settings to show their personal information (other than their name and photo) to only "Friends," "Friends of Friends," or "Everyone," (i.e. everyone on the Internet). When Facebook users upload photos to the system, they can click on (i.e. "tag") a person in the photo and enter the person's name, and create a link to the "tagged" person's profile. Tagging can be done by any Facebook user, even those who do not know the "tagged" person; however, tagged persons can remove the tags if, for example, another user posts an unflattering picture of them or an image that depicts them engaging in embarrassing or incriminating behaviour (Findlay, 2009). However, the un-tagged the photograph can remain on the social networking site, and can still be accessed by other people who are familiar or unfamiliar with the individual. The person posting the photo can also identify the individual in plain text, which does not create a link or result in sharing of the image, and the identified person cannot have his or her name

removed unless the photo violates the website's terms of use (in which case, Facebook can remove the photo).

In September 2009 alone, Twitter, a social network and micro-blogging service, had twenty million visitors (Levine, 2011). Twitter is different from Facebook in that it allows users to set up personal profiles and create lists of friends, but its primary function is a "micro-blogging" service, which enables users to send and read user messages called "tweets" (Chahal, 2011). These tweets are comprised of up to 140 characters displayed on a user's profile page. Tweets are publicly visible; however, users can restrict their transmission to only those on their friends list. Users can also sign up to receive tweets from other users, even people they do not know, and this is called 'following.'

YouTube was officially launched in May 2005, as an online tool for the sharing of video content and by December it was getting several million views per day (Seabrook, 2012). In October, 2006, it was bought by Google for USD$1.65 billion (Seabrook, 2012. It has become the world's most popular global media outlet: it hosts eight hundred million unique users from around the globe per month, with an astonishing forty-eight hours of new video uploaded to its site every minute; and it receives more than three billion views per day (Weiman, 2010). YouTube is more than simply an innovative media platform; it is, in effect, a vast cultural landscape that allows anyone to upload original content and instantly reach a diverse global audience, for free.

It's interesting that social media connections are, far more often than not, loosely built around insubstantial, or irrelevant, social bonds. For example, Twitter is used for 'following' people we have frequently never met; and, similarly, Facebook allows us to keep up with the 'friends' we would otherwise not necessarily stay in touch with (Gladwell, 2010). Thus, it's a platform for sharing ideas and information, while keeping a safe distance from other people, ensuring that one is not overly involved in the real substance of other people's lives. It's also useful for entertainment, collaboration, the dissemination of ideas; but, as a general rule, our interactions with Facebook friends tend to be simplistic, if not superficial. Along the same lines, social media is effective at motivating and assembling large networks of loosely-affiliated, leaderless participants, mainly because their involvement is so effortless and low-risk (Gladwell, 2010).

Returning to the events in Tunisia that sparked the protests in 2011, it is noteworthy that one third of all Tunisians use the Internet and three-quarters of them have Facebook accounts. Thus, it is not surprising that the posting of the Bouazizi video on the Internet galvanized people who were fed up with the regime, and provoked unrest in towns and cities throughout the country (Andersen, 2011). The video, which was posted on Facebook, gave citizens a powerful example of resistance they could identify with (Andersen, 2011). It didn't take long before other young Tunisians were capturing footage of local rebellions on their mobile devices and uploading them to Twitter, where they were viewed by hundreds of thousands of people in January of 2011 (Andersen, 2011).

At around the same time as protests were being waged in Tunisia, an underemployed twenty-eight year old Egyptian man named Khaled Said was arrested in Egypt and beaten to death by police (Andersen, 2011). In response, Wael Ghonim, an Egyptian Google executive in his late twenties, created a Facebook page called, "We Are All Khaled Said". The page became an overnight triumph amongst young Egyptians, and it quickly attracted more than four hundred thousand supporters (Preston, 2011d). Subsequently, tens of thousands of educated middle-class Egyptians, many of whom had never attended a

political rally in their lives, began to meet online and plan their now-infamous march on Cairo's Tahrir Square (Andersen, 2011).

Most of the Egyptians who joined in the demonstrations in the week leading up to the February 1st "March of Millions" in Tahrir Square said that their involvement was spontaneous (Gosh, 2011). Yet, the event had been planned weeks in advance by a loose coalition of activists who used social media sites to organize. Nationwide protests erupted throughout the country, including in Al Mahalia, 80 miles north of Cairo, where striking textile workers, joined by angry protesters, raged against President Mubarak (Darwish, 2008). These clashes, which ultimately led to calls for an end to the autocratic rule that existed in Egypt for more than fifty years, were captured by citizens on their video cameras and mobile phones, and later watched by millions of people on YouTube and Facebook.

Approximately two weeks before the demonstrations in Egypt, Arabs throughout the Middle East and North Africa were awestruck as they watched the uprising in Tunisia unfold on satellite TV and saw Ben Ali flee in haste (Gosh, 2011). Through the use of social media, Tunisians were able to show millions of their neighbours how to peacefully, and successfully, overthrow the regime, and they provided them with the courage to do it (Andersen, 2011). Indeed, prior to the January uprisings, protests were uncommon in Egypt because they were not tolerated by the heavy-handed Mubarak regime. However, every newbie was able to turn to the Internet for guidance and strategies, including a twenty-six page pamphlet entitled "How to Protest Intelligently" which contained advice about where to go, which slogans to chant, and even what clothing to wear (Gosh, 2011).

Later that same year, beginning in September, 2011, following an encouraging 'tweet' from the anti-capitalist magazine Adbusters, Occupy Wall Street protesters took to the streets of Lower Manhattan to demonstrate against corporate greed and corruption in the United States (Preston, 2011f). Shortly thereafter, for roughly two months, street demonstrations and occupations cropped up in other cities across North America, Asia and Europe, as activists from Rome to Sydney, Tokyo, Cape Town and Berlin used cell phones and social networking sites like Twitter, Facebook and YouTube to spread their defiant messages globally (Preston, 2011e). Ultimately, the movement gave rise to more than four hundred Facebook pages with over two and a half million supporters around the world; and on Twitter there were more than one hundred such accounts with tens of thousands of followers (Preston, 2011e). Without a doubt, technological innovations, like inexpensive and easy to use recording devices (including hand-held digital cameras, mobile phones, Blackberries, and the like), as well as social networking tools (including chat-rooms, video-sharing sites, social media and other online communities) helped to empower individuals, facilitate communication and mobilization, and prompt movements for change. In this sense, the Internet is a form of 'liberation technology' for the masses (Diamond, 2010).

Social networking sites are indispensable tools for the promotion of free speech, in terms of sharing information, giving people a voice, and enabling them to organize, particularly in developing states with authoritarian regimes (Christiansen, 2001). In the Middle East, they allowed activists to compile membership lists, distribute information about detained protesters, organize meetings and rallies, as well as to encourage turnout, while steering clear of government-monitored (and censored) news outlets and Websites (Diamond, 2010). At the same time, though, one must not over-estimate the power of online social networks to bring about real and lasting change. Since they don't have any

focal leadership or centralized decision-making authority, they have trouble reaching agreements, developing long-term strategies, setting goals, and resolving internal disputes (Gladwell, 2010). What is, then, the real significance of Internet technologies for these movements?

Internet technologies provide a mechanism for the formation of networks, enabling dialogue within communities; the promotion of transparency by means of up-to-date and uncensored photos and videos; and grassroots mobilization and coordination. From this perspective, the technologies are not merely tools but self-reflecting mirrors through which political, social and economic experiences are filtered and defined. While Internet technologies are not necessary to facilitate disobedience, as witnessed during the American civil rights movement in the 1960s (Gladwell, 2010), they are invaluable instruments for leveraging democratic values and inciting the ideological fervour necessary for social activism to take flight.

It is noteworthy, for instance, that the leader behind Egypt's "We Are All Khaled Said" campaign, Wael Ghonim, was a young, well-educated, English-speaking Google executive who was poised to succeed in Mubarak's increasingly modern, liberal economic regime (Gause, 2011). Yet, instead, Ghonim risked his life to rally Egyptians against the state, in the name of dignity and human rights. This suggests that the Mubarak regime was short-sighted to think that stability can be achieved through financial gain and economic liberalization alone (particularly when this produces other destabilizing inequalities), without also addressing the need for democratic reform and the rule of law. Moreover, the Net generation appears to understand the power of social media to communicate this message, as few things resonate more forcefully than images of wanton brutality, such as a bloody government crackdown against unarmed civilians.

Of course, social media and mobile devices do not supplant real-world activism and physical confrontation; although it facilitates them, allowing demonstrators to communicate more easily and assemble more quickly and efficiently than in the past. As well, the communities established through online social networking sites have enhanced activists' ability to convey their messages to worldwide audiences, obtain support (through outside pressure from world leaders), and, ultimately, stage their campaigns live, before a global audience, without any cooperation from the mainstream media. However, we cannot overlook the fact that these same instruments have been used by governments to monitor, disrupt and quash revolts.

II. New Social Media as an Instrument of Repression

The clichéd terms "Twitter Revolution" and "Facebook Revolution" have been widely criticized for being utopian, and overlooking, or discounting, the use of social media by ruling elites to filter and control Internet content, as well as to identify and punish dissidents (Christensen, 2001). It is true that social media platforms and the Internet, in general, have helped to broaden the public sphere, inviting multiple points of view, generating diverse news accounts and vibrant discourse in ways that are impracticable for the traditional mass media; and, they are also instrumental for promoting accountability and transparency in government (Diamond, 2010). At the same time, though, they have proven essential to the success of authoritarian regimes, in the sense that they facilitate intimidation, surveillance, information-gathering and suppression. This is not unexpected, given that social networking sites, like Facebook, contain a treasure trove of data about what their users look like, what their beliefs and lifestyle choices are, who

they associate with, places they have been, and things they do. And, when a specific entity amasses so much personal information, it raises a wealth of privacy concerns, not least of which is the possibility that it could be misused (Chahal, 2010).

If one considers the fact that until very recently, the Middle East was dominated by a handful of authoritarian dictators, including Muammar al-Qaddafi who came to power in Libya in 1969, Mubarak who took charge of Egypt in 1981, and Ben Ali who claimed Tunisia's presidency in 1987, all of whom managed to stay in power for decades by repressing dissent (Gause, 2011), it should come as little surprise that they sought to use Internet technologies for the purposes of control (Shane, 2011). Indeed, information-control has traditionally been a cornerstone of authoritarian regimes throughout the world, since long before the advent of computer technologies (Diamond, 2010). While these aging despots may have been out of touch with the Net generation, they should have been able to master the same technological tools that their adversaries embraced (Shane, 2011). Why, then, were they unable to exploit the power of the Internet to keep the masses under control?

Clearly, both liberals and despots compete for control over new technologies, and historic economic, social and political factors determine the outcomes in each state (Diamond, 2010).

There is no question that the Internet has made it easier for governments to manage the reporting of events by the media, both mainstream and grassroots, and to target almost any kind of political speech within their borders, by blocking specific kinds of communications, or immobilizing the entire national cyber-infrastructure (Christensen, 2001). Indeed, there are scores of examples of cyber-repression campaigns witnessed during the Arab Spring in 2011: the Libyan government swiftly disabled the Internet and mobile phone access within its borders; Bahrain's regime blocked YouTube and slowed Internet traffic by twenty percent; and Egyptian human rights organisations documented cases of the authorities kidnapping 'cyber-protesters' who were interrogated by police seeking their Facebook passwords (Darwish, 2008).

Many authoritarian states, such as China and Iran, have extraordinary technological capabilities to filter and control the Internet, and they use these powers to identify and punish dissidents. China has the world's largest population of Internet users – more than 380 million people in 2010 - yet it also oversees the most sophisticated system for monitoring and controlling Internet and mobile phone usage ever conceived (Diamond, 2010). With blocking occurring at multiple points in the network and extending to a large variety of subjects, China operates "The Great Firewall," which is the most technologically advanced and extensive system of Internet censorship in the world (Smyth, 2012). Google has abandoned China in protest over government censorship, while YouTube, Facebook, and other global social networking sites are significantly blocked or otherwise impeded (Diamond, 2010). Chinese companies that provide search and networking services are subjected to even more restrictive censorship rules than their international counterparts. Connection to the Internet is maintained by a small group of state-run operators that block and censor data according to the will of the CPP, and tens of thousands of cyber-police monitor Internet usage within the country and remove 'harmful' information (Diamond, 2010).

In June 2009, Iran was facing its most significant political turmoil since the overthrow of the Shah in 1979 (Morosov, 2011). When President Mahmoud Ahmedinejad's election victory was proclaimed on June 13, 2009, amidst furious accusations of election

fraud, thousands of Iranians took to Internet blogs, chat-rooms, and social media sites, including Twitter, Facebook, and Persian-language platforms, such as Balatarin and Donbleh, to distribute news, personal opinions, and calls for protest (Diamond, 2010). In the days that followed, opposition supporters used social media sites to attract tens of thousands of demonstrators to rally in Tehran (Diamond, 2010). Throughout the month, Internet users continued to organize nation-wide protests and other demonstrations throughout the city, which reportedly attracted between two and three million participants (Diamond, 2010). Yet those uprisings were quickly quashed, as protesters were beaten and gunned down on the streets by the authorities, while thousands more were arrested. YouTube provided a platform for Iranians to post pictures and videos of the appalling human rights abuses perpetrated against peaceful demonstrators, including the death of Neda Agha-Soltan (Diamond, 2010).

The Western media shone its spotlight on how the Internet seemed to be providing a vehicle for democratic reform in Iran. Within hours after the first protests, Western journalists were commenting about the robustness of the social networking site Twitter, even as the regime slowed Internet traffic within the country to a crippling creep, enabling authorities to mine the data for intelligence-gathering purposes (Morosov, 2011). The regime also used torture to obtain Iranians' passwords, and posted photos of unidentified activists on the Web, encouraging Iranians to identify them. Notwithstanding this grim reality, Western pundits vociferously proclaimed that Twitter had upended the totalitarian regime (Morosov, 2011). However, as the so-called 'Green Revolution' lost momentum in the ensuing months, it became clear that technology itself, notwithstanding its unique power to galvanize its youthful devotees, would not be powerful enough to overcome its most cold-blooded totalitarian adversary. Indeed, the Iranian regime proved very capable of using the same tools to quash the unrest. In the months following the Green Revolution, the government established a group of officials who were tasked with finding false information (i.e. "insults and lies") and identifying those spreading it; the authorities also tracked down the Facebook profiles and email addresses of Iranians living abroad and ordered them to stop supporting the Green Revolution unless they wanted to bring harm to their relatives back in Iran (Morosov, 2011).

Ironically, the role played by Twitter in the unsuccessful Green Revolution had the unintended consequence of providing leverage for the Iranian government to rail against what it viewed as Internet-facilitated foreign intervention, particularly from the United States, which was accused of having precipitated revolutionary discord within the country (Morosov, 2011). When all was said and done, the Green Revolution augmented the climate of fear, uncertainty and anxiety in Iran, further strengthening Ahmadinejad's dominance, and making it more difficult for Iranians to use the Internet to foster political and social change within their country (Morosov, 2011). Since the Iranian people don't know exactly what their government is capable of, in terms of using the Web to identify and locate dissidents, simply knowing that they might be observed by state agents is enough to deter them from engaging in the online subversion tactics carried out in the spring of 2009 (Morosov, 2011).

The brutal social network crackdown witnessed in Iran also occurred in other parts of the Arab world, whereby state officials used information blockades to quash protest movements. Until the 2011 uprisings in Egypt, the Egyptian government limited itself to monitoring the online communications of its citizens; yet, in response to the mass demonstrations, it swiftly began targeting content, such as Facebook and Twitter, and

even shut down its communications infrastructure, including all mobile phone and Internet services, in an effort to stifle dissent (Dunn, 2011). In fact, the Egyptian government's assault on the media began in late 2010, with an effort to suppress virtually any form of opposition during parliamentary elections (Dunn, 2011). On the day of the elections, websites hosting major opposition newspapers were blocked to counter hostility and allegations of election fraud (Dunn, 2011). Then, during the revolts in late January 2011, the government resorted to blocking access to entire social networking sites, including Facebook and Twitter, in an attempt to undermine the coordination of protests using Twitter, and the "We are all Khaled Said" Facebook page campaign, discussed above (Dunn, 2011).

The Egyptian government (through the police and hired informants) also hijacked protesters' blogs and Facebook pages in order to transmit government propaganda to its citizens (Darwish, 2011). However, these efforts were not met with much success given that the protesters were able to upload their own videos showing stark examples of the ongoing police brutality (Darwish, 2011). In response, the Egyptian government targeted prominent activists by shutting down their mobile phone lines, in accordance with disrupting access to Facebook and Twitter; although, the activists were able to use circumvention software to access these sites (Dunn, 2011). When these efforts failed to stop the demonstrations from gaining momentum, the Egyptian regime ultimately halted all Internet and SMS services within the country for several days, which forced the population to turn to satellite television, radio, and face-to-face discussion for information about the uprisings (Dunn, 2011). The Ministry of the Interior and the military then forced national mobile service providers to send out text messages urging Egyptians to stop demonstrating; and, this appropriation of SMS message services by the government continued after SMS services were restored for consumer use (Dunn, 2011).

In a similar vein, the Syrian government cracked down on dissidents' use of social media and the Internet to promote their 2011 revolt only three months after allowing citizens to have open access to Facebook and YouTube (Preston, 2011c). Security officials in Syria demanded that protesters hand over their Facebook account passwords and prevented them from uploading videos to YouTube by shutting off electricity and the 3G mobile phone network in neighbourhoods with the most mayhem (Preston, 2011c). Supporters of President al-Assad, calling themselves the Syrian Electronic Army, also used social media tools to try and undermine and discredit dissidents (Preston, 2011c). For example, the Syrian government turned to Facebook to monitor criticism, plant pro-regime propaganda, and seek out dissidents; those who refused to give up their passwords risked being jailed or even killed by establishment officials (Preston, 2011c).

In some cases, dissidents have been able to evade government monitoring and avoid detection through the creation of multiple Facebook accounts with fake identities (Preston, 2011c). In other cases, such as within Syria, people were able to use Facebook and other restricted sites through proxy servers that allowed them to circumvent the government's firewall, which also blocks Wikipedia, Amazon, and other sites (Preston, 2011a). The free software, Tor, which is popular in Iran and Saudi Arabia, allows users to hide their browsing habits by redirecting traffic through multiple relays, making it difficult for the regime to monitor transmissions (Morosov, 2011). However, given that a vast amount of online activism takes place on pubic computers, these kinds of programs, which require the installation of software, are not within easy reach. This is particularly true if the Internet is accessed from Internet cafes and the like, as they typically do not allow

patrons to install new software (Morosov, 2011). On the other hand, Twitter is difficult to censor because there are so many ways for posts to originate, such as from a mobile phone, a Web browser, or a specific application, as well as many different sources through which those posts can appear (Stone and Cohen, 2009). When the Internet was shut down entirely in Egypt, many protesters simply called their friends outside Egypt, using landlines, to have them 'tweet' for them. Similarly, they were able to access tweets on air through satellite television, which also provided telephone numbers for access to Google's newly established Speak2Tweet program (Dunn, 2011).

What is the significance of these developments? And, more fundamentally, why were these obfuscation tactics successful in some Arab states and not in others (Dunn, 2011)? Without a doubt, the outcomes of the various Arab Spring revolutions (including Iran's Green Revolution in 2009) point more towards the prevailing social, political and institutional realities within these states than the capacity of Internet technologies to facilitate democratic change in repressive regimes (Srinivasan & Fish, 2011). The lesson might be that virtually any government has the power to prevent its citizens from accessing and communicating information electronically, as well as to spy on them, in ways that are previously unimagined. This is particularly true in authoritarian regimes where the line between public and private actors is extremely blurry; such as in Iran, for example, where the Iranian Revolutionary Guard owns the primary Internet Service Provider, the Telecommunication Company of Iran. This made it easy for the authorities to cripple the country's Internet services during the Green Revolution, and difficult, if not impossible, to hold it accountable to the public (Deibert & Rohozinski, 2010).

The path taken by the Egyptian government illustrates just how far a regime is willing to go in order to stifle dissent. Indeed, disabling or crippling the national communications infrastructure at important moments, such as during widespread public demonstrations, may be the most powerful tool for influencing political and social outcomes (Deibert & Rohozinski, 2010). Ultimately, though, as was the case in Egypt, those tactics can also help to trigger a regime's downfall, notwithstanding that they were only implemented on as 'as-needed' basis (Deibert & Rohozinski, 2010), avoiding allegations of unremitting Internet censorship that could be made against other authoritarian states, like China. Nevertheless, unlike what happened in Iran in the wake of the Green Revolution, Egypt's leaders lost credibility with their own citizens, particularly the business community, as well as the international community, which is evidenced by the fact that the Egyptian government was condemned by the United Nations, the European Commission, and the United States government (Dunn, 2011). Moreover, it showed international firms operating within Egypt, principally cellular service providers, that they were being kept under the thumb of the oppressive regime.

It is noteworthy that social media sites were also used by Western democratic nations in response to social unrest last year; albeit, not with anywhere near the same degree of heavy-handedness witnessed during the Arab Spring uprisings. When, in August 2011, protests spilled onto the streets in several cities in the United Kingdom, demonstrators used social media sites, like Facebook, to encourage public disorder and to incite criminal damage and burglary. Black Berry Messenger (BBM) was used by rioters to organise disturbances in UK cities including, London, Birmingham and Manchester. In response, on August 9, 2011, the Greater Manchester Policy 'tweeted' the following message on Twitter: "If you have been using social networking sites to incite disorder, expect us to come knocking on your door very soon" (Dzieza, 2011). Police also tracked and located,

then arrested, rioters using tweets, posts and text messages, and, indeed, over a dozen people were charged with posting messages on social media sites (e.g. Facebook and Twitter) inciting criminal damage and burglary.[3] Similarly, individuals were charged with using BBM to incite violence, with help from Research in Motion (RIM), the Canadian manufacturer of BlackBerry (Dzieza, 2011). That same week, the New York Police Department announced that it formed a new unit to track young suspects who brag about their crimes on social networking sites, like Twitter and Facebook (Parascandola, 2011).

We live in an era of ubiquitous computing, whereby individuals are more and more well connected through mobile devices, such as Smartphones, Blackberries, iPads, and so on. These mobile devices are increasingly linked through cloud computing, which makes it possible to run facial recognition software through them (Acquisti, Gross & Stutzman, 2011). Increasing self-disclosure through online social networks, particularly the sharing of personal photographs, has also become the norm; indeed, in 2010, 2.5 billion photos were uploaded by Facebook users *per month (*Acquisti, et al., 2011). Individuals often use their real first and last names on social networking sites, such as Facebook, LinkedIn, and so on. At the same time, automatic facial recognition software has been steadily improving, and is now used by a number of mainstream companies, such as Google, Apple and Facebook *(*Acquisti, et al., 2011).

Recent studies have confirmed that when we share personal information on social networking sites, we increase the likelihood that someone might use it to make inferences (from other data available online or offline) about who we are, making it easier for them to monitor, control, and influence our behaviour (Morosov, 2011). For example, a series of three experiments by researchers at Carnegie Mellon revealed that it is possible to make accurate inferences about individuals by combining publicly available online social networking data with commercially-available facial recognition software *(*Acquisti, et al., 2011). These 2010 studies demonstrate that as long as social networking sites are linked to real people, who are providing truthful information about themselves (in terms of their age, gender, location, and so on), it's amazingly easy to link them with all sorts of other information about those same people on the Web.

In the first experiment, the researchers downloaded publicly-available primary profile photos from Facebook account members in a single North American city and used them to identify the people in anonymous profiles (containing facial images and pseudonyms) on Match.com, one of the most popular dating sites in the United States. They used PittPatt, a facial recognition program recently acquired by Google, to compare the photos and found that one out of ten of the dating site's 'pseudonymous members' was identified *(*Acquisti, et al., 2011). This software enables face detection (i.e. automatically locating human faces in digital images) and face recognition (i.e. measuring similarity between any pair of faces to determine if they are of the same person). In the second experiment, the researchers used publicly available images from a Facebook college network to identify students on the same college campus. The researchers used a webcam to take three photos per college student participant, which were gathered over a two day period. Approximately one out of three subjects was identified by the facial recognition software and matched to their Facebook profile pictures and the average computation time per participant was less than three seconds *(*Acquisti, et al., 2011).

[3] Note that in Britain, it is a criminal offense to incite criminal activity through media.

In the final experiment, the researchers inferred the names, date of birth, and other demographic information from the Facebook profiles of the participants in the second study. With that information, they then predicted the participants' social security numbers, with 27% accuracy, from a publicly-available online social security number databank (Acquisti, et al., 2011). The study demonstrates that, with the help of commercially-available facial recognition software, it is possible to 'predict' a wealth of sensitive personal information about a person (in the United States, at least) from an anonymous image of the person's face. Quite clearly, any correct association between data linked to the person's real identity and their virtual identity can negate the anonymity of the latter (Acquisti, et al., 2011).

What are the implications of these findings? We have already seen that authoritarian governments do not shy away from using the Internet to conduct sweeping surveillance campaigns, particularly when they are concerned that their grip on society is loosening. The use of Internet surveillance by both democratic and undemocratic regimes is becoming more widespread and sophisticated (Diamond, 2010). And digital surveillance is getting a helping hand from the mainstreaming of facial recognition software. Facial recognition software manufacturers are already partnering with social network providers to tag billions of images uploaded by users, and the 'tagging' of one's self and others in photos has become commonplace (Diamond, 2010).

For example, Facebook has 'opted-in' all users to this service by default, so that whenever a user uploads a photo, the system automatically uses facial recognition software to match it to other photos he or she is tagged in (Paul, 2011). The software then groups similar photos together, and, wherever possible, suggests the name of the person in the photo. The user can then confirm Facebook's guesses and get through tagging friends in photos more quickly. While Facebook users might regard this feature as helpful and harmless, it allows the company to build up an enormous global databank of billions of images of people which can be shared with any private or public entity, for any reason.

This is significant given that an important, albeit innovative, use of facial recognition software is to allow government officials to quickly identify the people photographed during street protests and riots. For example, when you combine Gigapixel photos with automated systems of matching faces to real identities, plus social-network tagging systems, the result is the removal of anonymity. This is evident from a hi-resolution 2,110 megapixel aerial-view photograph online (located at: http://www.gigapixel.com/image/gigatag-canucks-g7.html), which is made up of 218 photos stitched together, taken over a 15-minute span with a robot-like Photo Galleries GigaPan camera attachment, in downtown Vancouver, British Columbia, where thousands of Canucks hockey fans gathered for Game Seven of the Stanley Cup Final on June 5, 2011 (CBCTV.ca, 2011). Only hours after the photos were taken, the city erupted into a large-scale riot, in which shop windows were smashed and cars were torched, following the Canucks' loss to the Boston Bruins.

The moniker above the online photograph reads: "Canucks Fans: Find yourselves and your friends in the Game 7 crowd, then tag and share on Facebook! Tell all your friends!" The online photograph allows users to zoom in and find tiny details with the click of a mouse. So far, the picture has been tagged more than 9,500 times (Daily Mail, 2011); and, this is surprising given that the local municipal police forces, together with the RCMP, have been searching for those who caused trouble during the riots, and are encouraging the public to identify suspects online. Facial recognition software was also

used by British Transport Police to help find suspects following the 2011 London riots, in addition to using images from traditional sources, including still images captured from closed circuit cameras, pictures gathered by officers, footage shot by police helicopters and images taken by members of the public (Dodds & Satter, 2011).

Of course, government officials can also use photos from their own databanks to identify people, with the help of facial recognition software. For example, a Massachusetts man was surprised to learn that he had his driver's licence revoked after an antiterrorism computerized facial recognition system that scans a database of millions of state driver's license images had picked his as a possible fraud (Irons, 2011). It turned out that his image was accidentally flagged because he looks like another driver, not because it was being used to create a fake identity (Fogarty, 2011). This is an example of what can happen when mistakes are made, and people are wrongly identified by facial recognition software tools, which still perform much worse than humans when recognizing faces *(*Acquisti, et al., 2011). Nevertheless, dozens of law enforcement agencies in the United States are reportedly being outfitted with a hand-held facial recognition device known as MORIS, or Mobile Offender Recognition System, which attaches to an iPhone, enabling an officer to snap a picture of a face from up to five feet away, or scan a person's irises from up to six inches away, and do an immediate search to see if there is a match with a database of people with criminal records (Steel & Angwin, 2011).

Facial recognition technology is likely to assist vigilantes, and other hard-liners, to identify dissidents and turn them in to authorities. Indeed, there are scores of examples, in both the Canadian and American contexts, of social networking sites being used by members of the public to "tip off" the police with respect to criminal misconduct, such as the use of illegal drugs and the serving of alcohol to minors. It also serves as a potential boon to the commercial sector. Imagine a world where you walk into your favourite store and are greeted by a sales person by name, who already knows a host of vital strategic information about you, because they scanned your face when you came through the door. While this scenario might seem more maddening than alarming, it is important to keep in mind that governments around the world are quickly beginning to harness the awesome intelligence power of social networking sites and facial recognition software. And, over time, it's inevitable that databases of identified images of individuals will become larger and facial recognition software will become faster and more accurate at identifying facial images.

III. Relevant Policy Considerations

We need to accept that it will become increasingly easy for strangers to identify and accurately predict sensitive information about us. Since the results are based on publicly available information, self-regulation, and "opt-in mechanisms" are not likely to be feasible (Acquisti, Gross & Stutzman, 2012). Thus, we need to think about the kinds of solutions or strategies that might be useful in this area. From a policy perspective, it is important to note that most, if not all, of the popular social networking sites, such as Facebook, Twitter and YouTube, are owned and operated by companies headquartered in the United States and are thus within the jurisdiction of the United States legal system. Many Canadians would be surprised to discover that there is a lack of privacy protection available to communications via social networks under the laws of the United States, particularly with respect to Facebook, which is currently the most popular social networking site in the world (Semitsu, 2011). However, the Privacy Commissioner of

Canada has affirmed that when you're a company doing business in Canada, collecting information about Canadians, you ought to respect Canadian privacy law. This section will begin with a review of American law as it relates to Facebook, followed by a discussion of recent rulings by the Privacy Commissioner of Canada regarding complaints against Facebook on a variety of privacy grounds.

a. The American Legal Context

The language of the Fourth Amendment of the United States Constitution proscribes intrusions into the "persons, houses, papers, and effects" of individuals unless a government official obtains a warrant supported by probable cause (U.S. Const., amend. IV, § 1). Under contemporary American privacy law, a communications medium or platform is not vested with Fourth Amendment protection unless the user has as "reasonable expectation of privacy" therein (Chahal, 2011). This two-part test emanates from *Katz v. United States* (1967), in which the U.S. Supreme Court famously recognized that the Fourth Amendment protects people, not places. The Court articulated a new analytical framework – the *reasonable expectation of privacy* test – which requires, first, that a person have an actual subjective expectation of privacy and, second, that the expectation is one that society is prepared to recognize as reasonable (*Katz v. United States,* 1967). If both aspects of the test are satisfied, the government must obtain a warrant, with its related probable cause requirement, to search the protected area or information. Improperly collected evidence may be subject to the "exclusionary rule" and prove inadmissible in a court of law (*Mapp v. Ohio*, 1961).

Generally speaking, a person's expectation of privacy will only be deemed 'reasonable' when it's supported by the right to exclude others. In *Smith v. Maryland* (1979), the U.S. Supreme Court, in holding that the defendant did not have a subjective expectation of privacy in a pen register (a device installed by telephone companies that can track the dialled phone numbers for outgoing calls), indicated that records handed over to third parties are not entitled to Fourth Amendment protection. The court based its understanding of privacy on the notion of secrecy, in that an individual would only have a reasonable expectation of privacy in information that was not exposed to the public (Solove, 2001). Relying on *Katz* (1967), the Supreme Court held in *California v. Ciraolo* (1986) that the mere likelihood of exposure to the naked eye diminishes or even negates the individual's expectation of privacy. Similarly, in *California v. Greenwood* (1988), in which the police searched inside plastic garbage bags that the defendant left on the curb for collection, the Court held that there was no reasonable expectation of privacy in the garbage because it is widespread knowledge that plastic bags left on or at the side of a public street are easily accessible to animals, children, scavengers, snoops, and other members of the public.

However, the opposite is also true: where a person "seals" or otherwise takes steps to conceal their information, this creates a reasonable expectation of privacy (*United States v. Jacobsen*, 1984). For example, it is well-understood that the Fourth Amendment's protection against 'unreasonable searches and seizures' protects a citizen against the warrantless opening of sealed letters and packages addressed to her in order to examine the contents (*United States v. Choate*, 1978). Hence, Fourth Amendment protections are typically engaged when government officials access or expose information that would otherwise have remained hidden or concealed from view. However, as with the phone numbers they dial, individuals do not enjoy a reasonable expectation of privacy in what

they write on the outside of an envelope (*United States v. Hernandez*, 2002). The principle is that once the information is exposed to others, the individual has forsaken his right to exclude (Kerr, 2004).

Applying these Fourth Amendment principles to social networking sites suggests that the individual does not have a reasonable privacy interest in the information that he or she posts on social networking sites. Indeed, it is likely that the social networking profile is not subject to Fourth Amendment protections at all because the photos, wall posts, and other information about its owner, including his or her name, gender, sexual preference, birthday, political and religious views, relationship status, lifestyle choices, educational and employment history, have been voluntarily disclosed to either the person's 'friends,' or to any member of the public, or both (Hass, 2006). This point is all the more pertinent when one considers that in order for a person to join Facebook the company only requires the new user to provide their name, email address, date of birth and gender; all other information is disclosed voluntarily by the user for the exclusive purpose of sharing it with others (Denham, 2009).

And, moreover, Facebook users have often reported, forwarded, or otherwise provided law enforcement agents with access to evidence of unlawful activities posted by other people, especially when minors are concerned (Semitsu, 2011). Clearly, there is an argument to be made that by simply accepting 'friends' to their profile, which can number in the hundreds, or even thousands, they are repudiating their reasonable expectation of privacy in the information by disclosing it to third parties. Yet this also raises a number of important questions: do people truly understand their limited privacy rights when they post personal information on social networking sites; and, for that matter, what are users' rights; and how should governments collect and use information contained within online social networks?

These questions are particularly salient if we acknowledge that it is not easy to tie each piece of information to a single person. For example, a photograph can be posted that depicts multiple people, without their knowledge or permission. Thus, it becomes difficult to know who has the right to expose the photograph to others and, in doing so, whose privacy rights are infringed, especially as this information can easily be accessed by third parties (Chahal, 2011). An additional question might be whether the other individual is tagged or not; one might consider such an action as an express manifestation of consent by the individual, whereas the withholding of this consent might indicate the person's unwillingness to give other third parties the right to access the image (Findlay, 2008).

In some cases, the content of the photograph may be sufficient to secure an objectively reasonable expectation of privacy. For example, if the photograph depicts highly personal interactions, or if it is taken in a private as opposed to a public setting, society might be more prepared to recognize the expectation of privacy as reasonable.[4] This is especially important now that the Internet, and online social networking, in particular, has made it easy for recordings of both consensual and non-consensual sexual activity to be publicly displayed and distributed to others (*R. v. Desilva*, 2011).

[4] In the Canadian context, individuals can be prosecuted pursuant to the criminal harassment and voyeurism provisions under ss. 264 and 162 of the *Criminal Code* (R.S.C. , 1985, c. C-46) and the child pornography provisions under s.163.1, depending, of course, on the age of the victim and the circumstances.

There is also the question of whether law enforcement agents can access these materials without a warrant, and whether this violates the Fourth Amendment's prohibition against illegal searches and seizures (Findlay, 2008). Although Facebook has taken steps to warn its users about these pitfalls, privacy expectations (and their corresponding rights) on social networking sites remain uncertain in the United States, particularly regarding photographs posted by third parties, and users would best be advised that any disclosure of personal information on these sites is to be undertaken at the users' own risk (Hodge, 2006).

Facebook is also subject to the requirements of the *Communications Decency Act* (CDA) (1998) which further limits its liability regarding the content posted by its users on its site and offers the company protection against legal challenges brought by a user. Section 230 of this Act states that, "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider" (CDA, 1998). The term "interactive computer service" is defined in that section as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet." Furthermore, an "information content provider" is defined as "any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service." As such, Facebook is an interactive computer service, and any Facebook member may be an information content provider (Hashemi, 2009).

In *Zeran v. America Online, Inc.* (1997), a case in which Mr. Zeran sued America Online, Inc. (AOL) for its failure to remove a false advertisement that directed interested buyers to call him to order t-shirts supporting the 1995 Oklahoma City bombing (Mr. Zeran notified AOL that he received death threats over the advertisement and demanded its removal), the Fourth Circuit held that the *CDA* gives interactive computer services immunity against tort claims, even after information content providers notify the services of defamation or threats, "because the insupportable legal burden imposed by potential tort liability would undermine the CDA's goal of promoting speech on the Internet." Likewise, in *Carafano v. Metrosplash.com, Inc.* (2003), where the Ninth Circuit considered whether a commercial Internet dating service may be legally responsible for false content in a dating profile provided by someone posing as another person, the court held that the CDA granted immunity to Matchmaker.com. Circuit Judge Thomas explained:

> The specter of tort liability in an area of such prolific speech would have an obvious chilling effect. It would be impossible for service providers to screen each of their millions of postings for possible problems. Faced with potential liability for each message republished by their services, interactive computer service providers might choose to severely restrict the number and type of messages posted. Congress considered the weight of the speech interest implicated and chose to immunize service providers to avoid any such restrictive effect (*Carafano v. Metrosplash.com, Inc.*, 2003).

Similar sentiments were echoed by the Third Circuit in *Green v. America Online* (2003), in which the court upheld immunity for the transmission of defamatory messages and a program designed to disrupt the recipient's computer.

Given these findings and their emphasis on the government's interest in promoting free speech on the Internet, it would appear that Facebook would be granted immunity under the *CDA* if a user brought a claim against it concerning content that another individual posted to its site. Facebook may not, therefore, need to take any action to shield itself from liability in this context, within the American legal system. Users who dislike how Facebook handles their personal information may find that they have little recourse, apart from terminating their accounts. However, Facebook has made a number of changes to its privacy and terms of use in recent months, making it more responsive to the concerns of privacy advocates, as discussed below. The Statement of Rights and Responsibilities now reads as follows:

You own all of the content and information you post on Facebook and you can control how it is shared through your privacy and application settings. In addition:

1. For content that is covered by intellectual property rights, like photos and videos (IP content), you specifically give us the following permission, subject to your privacy and application settings: you grant us a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook (IP License). This IP License ends when you delete your IP content or your account unless your content has been shared with others, and they have not deleted it.
2. When you delete IP content, it is deleted in a manner similar to emptying the recycle bin on a computer. However, you understand that removed content may persist in backup copies for a reasonable period of time (but will not be available to others) (Facebook, 2012b).

It is also worth noting that U.S. federal agents have created fake identities on Facebook, and other social networking sites, in the hopes that suspects (or their friends) will allow access to private information, help plot social networks, and make incriminating disclosures (Semitsu, 2011). Indeed, law enforcement agencies throughout the country have disclosed that they have no reservations about going undercover on Facebook and creating fake identities for these purposes (Semitsu, 2011). Facebook, for its part, has revealed that it receives between ten and twenty law enforcement requests per day (Chahal, 2011).

Government agents can also compel social networking sites to turn over logs of the times and dates that users have logged into the network, as well as content, through a warrant under the *Stored Wire and Electronic Communications and Transactional Records Access Act (*"the Stored Communications Act*")*, which regulates the collection of digital evidence stored and transmitted on computer networks (The *Electronic Communications Privacy Act*, 2006). The *Stored Communications Act* forbids government access to stored content on third party servers; however, section 2702 provides an exception for disclosures to a law enforcement agency, or pursuant to a court order (Semitsu, 2011). Moreover, section 2703(d) allows the government to compel the disclosure of all content related to specific individuals, pursuant to a subpoena, without probable cause or meaningful notice. And, based on Facebook's own interpretation of federal privacy laws, a warrant is only needed to compel the disclosure of messages less than 181 days old (Semitsu, 2011). Everything else can be obtained by U.S. federal police with subpoenas that do not even require reasonable suspicion (Semitsu, 2011).

b. The Canadian Legal Context

There are a number of examples in both the civil and criminal law contexts of Canadian courts relying on information that Facebook users have posted on their profiles in order to draw inferences about the individual's lifestyle, activities, and personal choices. For example, in *R. v. Huxford* (2010), a police 'guns and gangs' unit was advised by an informant that Huxford was seen on Facebook flashing a gun, posing in an intimidating stance with his arms flexed with what the court described as a "you want a piece of me" look; he was subsequently arrested following an undercover sting operation. Similarly, in *R. v. Lee* (2010), the accused was charged with threatening death as a result of a posting he put on his Facebook page. In *Schuster v. Royal & Sun Alliance Insurance Co. of Canada* (2009), the defendant insurer sought an interim order preserving documents contained in the plaintiff's Facebook page in the hope that it contained evidence that the injuries she sustained in an accident were not as serious as she claimed. And, lastly, in *S.O. v. Alberta (Child and Family Services Authority)* (2012), the fact that the petitioner posted pictures on her Facebook page showing her holding a marijuana leaf and bud was seen as demonstrating her "remarkable immaturity and naivety, as well as continuing lack of good judgment" and was one of the reasons that the British Columbia Supreme Court denied her custody and access to her child.

It must be kept in mind that Facebook, along with most of the other popular social networking sites used by Canadians, is headquartered in the United States. In the recent case of *St-Arnaud c. Facebook Inc.* (2011), Deziel, J.S.C. held that the Superior Court of Quebec is *forum non conveniens* for a Montreal-based motion to authorize the bringing of a class action against *Facebook* regarding its privacy policies. The court relied on s.15.1 of the Terms of Use, as they existed in January 2007, when the Motion of Authorization was filed:

> 15. Disputes
> You will resolve any claim, cause of Action or dispute ("claim") you have with us arising out of or relating to this Statement or Facebook exclusively in a state or federal court located in Santa Clara County. The laws of the State of California will govern this Statement, as well as any claim that might arise between you and us, without regard to conflict of law provisions. You agree to submit to the personal jurisdiction of the courts located in Santa Clara County, California for the purpose of litigating all such claims.

Given that Facebook users must agree to this term, which is part of the Terms of Use, when they sign up for membership to the site, it would appear that legal claims against the company must be undertaken in the state of California, the site of its corporate headquarters, and not in a Canadian province. It is noteworthy, though, that a Quebec court upheld a 2008 judgment rendered by a California court ordering the defendant to pay USD$ 873,277,200 in damages for sending unsolicited email and unauthorized appropriation of data following intrusions into Facebook users' accounts (*Facebook Inc. c. Guerbuez*, 2010). The court found that the purpose of the California decision was to "denounce behaviour that incurs censure not only in the U.S. and Canada, but also worldwide;" thus, it regarded it as being consistent with Canadian public policy and concluded that the judgment be upheld in Quebec (*Facebook Inc. c. Guerbuez*, 2010).

Canadian law enforcement officials also conduct undercover investigations on social networking sites, like Facebook, and make formal requests for access to subscriber information and electronic data. This is particularly true with respect to cases involving allegations of child luring, as illustrated by the case of *R. v. McCall* (2011) in which the accused was convicted of child luring, under s.172.1 of the *Criminal Code*, after he used Facebook to communicate with an undercover police officer posing as a fourteen year old girl. At the same time, however, section 8 of the Canadian *Charter of Rights and Freedoms* contains a robust constitutional protection against government intrusion into the private sphere of the individual. Building on the framework established by the common law, s.8 creates certain areas of personal autonomy where government agents cannot intrude without judicial authorization.

Section 8 of the Charter provides: "Everyone has the right to be secure against unreasonable search and seizure." The Supreme Court of Canada has stated that this provision protects the citizens' reasonable expectation of privacy in a free and democratic society (*Hunter v. Southam*, 1984). he Supreme Court of Canada has established a purposive approach to s.8 in which the protection of privacy is the overriding principle (*R. v. Tessling*, 2004). Emphasis is placed on examining the totality of the circumstances, with regard to the reasonableness of one's subjective expectation of privacy (*R. v. Edwards*, 1996). The Court's insistence on legal authority for searches and seizures involving new surveillance technologies is consistent with its goal of preventing unjustified searches before they happen. In the words of Dickson J., in *Hunter v. Southam* (1984), "this can only be accomplished by a system of prior authorization, not one of subsequent validation." This approach is reflected in a number of surveillance technology decisions dealing with the requirements for a reasonable search and seizure under s.8 (*R. v. Wong*, 1990; *R. v. Duarte*, 1990; *R. v. Plant*, 1993).

If a search is found to be unreasonable under s. 8 of the *Charter*, such that the statutory requirements under the *Code* have not been met, the evidence can be excluded under s. 24(2) of the *Charter*, which provides that:

> Where, in proceedings under subsection (1), a court concludes that evidence was obtained in a manner that infringed or denied any rights or freedoms guaranteed by this Charter, the evidence shall be excluded if it is established that, having regard to all the circumstances, the admission of it in the proceedings would bring the administration of justice into disrepute.

The Supreme Court of Canada has stressed that the purpose of s. 24(2) is to maintain the integrity of and public confidence in, the criminal justice system *(R. v. Grant*, 2009). In spite of the fact that Facebook is headquartered within the United States, they have Canadian offices. As such, Canadian law enforcement officials can issue production orders to compel them to produce documents or data to be used in criminal investigations. The relevant provisions governing the use of production orders are set out in ss. 487.012 through 487.017 of the *Criminal Code*. A production order is a type of judicial order that is similar to a search warrant.

The Personal Information Protection and Electronic Documents Act (PIPEDA) (S.C. 2000, c. 5), which is Canada's private sector privacy law, establishes rules for the collection, use and disclosure of personal information by private organizations involved in commercial activities. The Privacy Commissioner of Canada is mandated by Parliament to oversee compliance with *PIPEDA*, which applies to federal works and undertakings, including

ISPs, such as *Facebook* and other social networking sites, which use personal information in the course of commercial activities *(PIPEDA*, S.C. 2000, c. 5). Personal information is defined in s.2 (1) as "information about an identifiable individual but does not include name, title, business address or telephone number of an employee of an organization" *(PIPEDA*, S.C. 2000, c. 5). One of the central principles behind *PIPEDA* is that consent must be obtained before information can be collected from an individual, and then used or disclosed. The standard of the "reasonable person," as it is used in *PIPEDA,* requires private organizations to collect, use and disclose personal information "for purposes that a reasonable person would consider appropriate in the circumstances," in compliance with ten broad privacy obligations specified in Schedule 1 of the Act *(PIPEDA*, S.C. 2000, c. 5).[5]

It is noteworthy, though, that *PIPEDA* permits the collection and disclosure of personal information *without* the knowledge and consent of an individual in certain circumstances. An organization can *collect* personal information without the knowledge and consent of an individual under s. 7(1)(e)(ii) if the collection is made for the purpose of making a disclosure that is required by law *(PIPEDA*, S.C. 2000, c. 5). An organization can *disclose* personal information, without the knowledge and consent of the individual if, pursuant to section 7(3) (c.1), the disclosure is made to a government institution and (iii), the disclosure will be made "for the purpose of administering any law of Canada or a province" *(PIPEDA*, S.C. 2000, c. 5). In this respect, *PIPEDA* is designed to both protect individual privacy and facilitate information sharing between third parties and government organizations, for law enforcement purposes.

In 2009, the Office of the Privacy Commissioner of Canada completed a detailed investigation into a complaint about the privacy practices and policies of *Facebook*, which was filed by the Canadian Internet Policy and Public Interest Clinic (the "CIPPC") on May 30, 2008 (Denham, 2009). The case was decided by the then-Assistant Privacy Commissioner of Canada, Elizabeth Denham, who released her report on July 16, 2009, in which she concluded that four aspects of the complaint were well founded (Denham, 2009). This case marks a significant step in determining how Canadian privacy law influences online social networking sites, particularly a global giant like Facebook. Moreover, since it represents the most comprehensive official investigation of Facebook privacy practices ever undertaken, and particularly since Facebook agreed, in response, to make comprehensive policy and technical changes to its global operations, the decision goes a long way toward protecting the rights of users in jurisdictions other than Canada (Geist, 2009; Stoddard, 2010).

The central issue in the CIPPC's allegations was whether Facebook was providing "a sufficient knowledge basis for meaningful consent" by documenting the purposes for the

[5] These include the following: collection limitation (the parties should limit how information is collected; collection must be with consent and knowledge that the information is being collected); data quality (the data must be accurate and relevant); purpose specification (the party must specify the purpose for which the information will be collected); use limitation (once information is collected for one purpose it cannot be used for another purpose unless the individual consents or this is authorized by law); security safeguards (the information must be secured from risk, e.g. from attacks by hackers); openness (transparency i.e. the individual should know what is being done with her information); individual participation (the individual should have access to her information and be able to look at it and correct inaccuracies); and accountability (there must be an oversight mechanism).

collection, use and disclosure of personal information, and providing that information to individual users in a "reasonably direct and transparent" manner (Denham, 2009). A key concern was that, although Facebook provides information about its privacy practices, it was frequently confusing or incomplete (Office of the Privacy Commissioner of Canada, 2009a).

The Assistant Privacy Commissioner's report recommended more transparency, to ensure that users have the information they need to make meaningful decisions about how they share personal information. Facebook was given thirty days to respond and explain how it would address these concerns. Under *PIPEDA*, the Privacy Commissioner could apply to the Federal Court of Canada to have her recommendations enforced. The company replied by agreeing to add important new privacy safeguards, as well as other changes, in order to conform to Canada's privacy law. Following is an overview of the key issues raised during the investigation and Facebook's response.

Facebook agreed to amend the language of the pop-up box that users see when registering that explains the purpose for collecting the date of birth. It also agreed to make changes to the language of its Privacy Policy with respect to its use of personal information for advertising and has stated that it is dedicated to "full disclosure as to the collection and use of information for advertising purposes" (Office of the Privacy Commissioner of Canada, 2009b). Facebook also committed to introducing a means whereby users would be able to select a low, medium, or high privacy setting. This selection would dictate more granular default settings. Users who choose the "high" setting would not be included in public search listings (Office of the Privacy Commissioner of Canada, 2009b).

A central allegation, which was upheld by the Assistant Privacy Commissioner of Canada, related to Facebook's disclosure of personal information to third-parties who create applications, such as games, quizzes and classified advertisements, which run on Facebook. There are more than a million of these third-party application developers in 180 countries around the globe. When users add an application, they consent to giving the third-parties access to their personal information, as well as that of their "friends." The Assistant Privacy Commissioner determined that *Facebook* did not have acceptable safeguards in place to prevent unauthorized access by third-party application developers to users' personal information, and it was not adequately ensuring that meaningful consent was obtained from these individuals prior to the disclosure of their personal information (Denham, 2009).

The Assistant Privacy Commissioner recommended that Facebook implement technological measures to restrict third-parties' access to only the user information essential to run a specific application (Denham, 2009). In other words, there was too much personal information being shared with third-party application developers, without adequate monitoring. She also requested Facebook to ensure that users are informed about the specific information that an application requires, and what its purpose is (Denham, 2009). She further recommended that users signing up for an application be asked for express consent to provide their personal information to third-party developers (Denham, 2009).

In response, Facebook agreed to redesign its application platform so as to prevent any application from accessing information until it obtains express consent for each category of personal information it wishes to access (Office of the Privacy Commissioner of Canada, 2009b). Under this new model, users adding an application are advised that the application

wants to access specific categories of information; and, the user is able to control which categories of information an application is permitted to access. There is also a link to a statement by the third-party application developer as to how it will use the data.

Another of the Assistant Privacy Commissioner's concerns was that Facebook provided confusing information about the difference between account deactivation and deletion (i.e. whether the users' personal information is stored on Facebook's servers or removed) (Denham, 2009). As well, she recommended that Facebook implement a retention policy under which the personal information of users who deactivated their accounts would be deleted from the site's servers after a reasonable period of time (Denham, 2009). Facebook responded by agreeing to make it clear to users that they have the option of either *deactivating* or *deleting* their accounts (Office of the Privacy Commissioner of Canada, 2009b). This distinction is now explained in Facebook's privacy policy and users receive a notice about the delete option during the deactivation process.

With respect to the concern that people should have a better way to provide meaningful consent to have their account "memorialized" after their death, the Privacy Commissioner concluded that Facebook should be transparent in its privacy policy that it will keep a user's profile online after death so that friends can post comments and pay tribute (Denham, 2009). In response, Facebook agreed to change the wording in its privacy policy to explain what will happen in the event of a user's death (Office of the Privacy Commissioner of Canada, 2009b). Lastly, the Assistant Privacy Commissioner found that Facebook should better protect the privacy of non-users who are invited to join the site (Denham, 2009). In response, Facebook agreed to include more information in its Terms of Use (Office of the Privacy Commissioner of Canada, 2009b). Facebook also confirmed that it does not use email addresses to track the success of its invitation feature, nor does it maintain a separate email address list for this purpose.

In a subsequent, albeit separate, complaint against Facebook, in August 11, 2010, three individuals complained to the Privacy Commissioner of Canada that they received an email invitation to join Facebook, along with so-called "friend suggestions" (i.e., a list of Facebook users and profile photos that the complainants knew) (Office of the Privacy Commissioner of Canada, 2012). The complainants alleged that the company accessed their electronic address books (or that of their friends) and used the personal information contained therein without their consent. The Office of the Privacy Commissioner of Canada concluded that Facebook failed to meet the knowledge and consent requirements under *PIPEDA* by failing to obtain consent for the use of a non-user's email address; failing to inform non-users of the proposed use of their email address; and failing to establish a procedure for opting-out prior to the use of a non-user's email address (Office of the Privacy Commissioner of Canada, 2012).

The complaint stemmed from a change Facebook made to its site in October 2009, whereby, in an effort to expand its subscriber base, it introduced a Friend Suggestion feature (Office of the Privacy Commissioner of Canada, 2012). The feature allows Facebook users to upload the email addresses of non-users to their Facebook contacts and to invite people they may know to join the site. Non-Facebook users are persuaded to subscribe to the site through a series of email reminders, some of which include friend suggestions (Office of the Privacy Commissioner of Canada, 2012).

A key concept behind *PIPEDA* is that of ensuring an individual's control over their personal information; and control, within the framework of the legislation, is largely in relation to knowledge and consent. Consent is meaningful if the individual is clearly

informed about the purposes for collecting, using and disclosing personal information. As a result of the Commissioner's findings, Facebook now provides clear notice to non-users that their email addresses may be used to generate friend suggestions, and offers them an easy-to-use opt-out mechanism (Office of the Privacy Commissioner of Canada, 2012). The unsubscribe notice now plainly states, "If you don't want to receive these emails from Facebook in the future, or have your email address used for friend suggestions, you can unsubscribe" (Office of the Privacy Commissioner of Canada, 2012). Individuals who unsubscribe are added to Facebook's "do not email" list, with their email addresses being retained for the purpose of ensuring that the individual no longer receives messages from the site (Office of the Privacy Commissioner of Canada, 2012).

Conclusion

Social networking sites are revolutionary new platforms that provide a wide range of benefits for individuals throughout the world, in terms of promoting social engagement, recreation, cultural flourishing, and much more. They also encourage people to disclose more personal information than people would have felt comfortable with only a mere decade ago. The events of 2011 demonstrated that there can be significant consequences to sharing personal information in these contexts, particularly for those who reside in jurisdictions with far less robust privacy regimes than our own. These risks stem largely from the extent to which this information can be accessed by third parties, including government officials who are using it to locate and apprehend dissidents.

The fact that information posted by users on social networking sites are being accessed by many different entities, and not just other users, suggests that these venues contain a vast treasure-trove of information about us. Controlling our personal information is only feasible if users are able to provide meaningful consent to the collection, use and disclosure of their personal information. That is difficult when Canadians are increasingly sharing their personal data online by means of social networking sites based in other jurisdictions. Recent history has proven, though, that even in the borderless world of online social media, Canada's privacy and data protection watchdog can bring about meaningful changes in these areas.

Clearly, Facebook is a dynamic environment that has undergone many changes during the past decade or so. It is incumbent upon Canadians to hone their expectations about how social networking sites should handle our personal information. As a world leader in the enactment and enforcement of private-sector privacy laws, Canada has a role to play in ensuring that other online social network providers operating in Canada are complying with Canadian laws. In doing so, Canada can play an important role on the world stage in ensuring that these sites are mindful of securing the privacy rights of all their customers, at least with respect to the collection, use and disclosure of personal information.

References

Andersen, K. (2011, December 26). Time's Person of the Year – The Protester. *Time*, *178*(5), 54-89.

Acquisti, A., Gross, R., & Stutzman, F. (2011) Faces of Facebook: Privacy in the Age of Augmented Reality. Proceedings from BlackHat USA Conference. Retrieved from 12th April 2012 from http://www.heinz. cmu.edu/~acquisti/research.htm.

Acquisti, A. Gross, R., & Stutzman, F. (2012) Face Recognition Study – FAQ. Retrieved from 12th April 2012 from http://www.heinz.cmu.edu/~acquisti/face-recognition-study-FAQ/.

California v. Ciraolo, 476 U.S. 207, 213 (1986).
California v. Greenwood, 486 U.S. 35 (1988).
Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1122-24 (9th Cir. 2003).
Chahal, S. (2011). Balancing the Scales of Justice: Uncovering Investigations on Social Networking Sites. *Journal on Telecommunications & High Technology Law*, *9*(1), 285-312.
Christensen, C. (2011) Discourses of Technology and Liberation: State Aid to Net Activists in an Era of "Twitter Revolutions." *The Communication Review*, *14*(3), 233-253.
Communications Decency Act 47 U.S.C. § 230 (1998).
Criminal Code (R.S.C., 1985, c. C-46).
Daily Mail Online. (2011, July 15). Nine Thousand Tags... and Counting: Vancouver Ice Hockey Fans Race to ID Themselves in Amazing Crowd 'Stitch' Photo for Facebook Record Attempt. Retrieved from 12th April 2012 from http://www.dailymail.co.uk/sciencetech/article-2014816/Facebook-tagging-record-attempt-Vancouver-hockey-fans-race-ID-gigapixel-photo.html#ixzz1tGhy67ll.
Darwish, A. (2008). The Last Word. *Middle East*, 391, 66-66.
Deibert, R., & Rohozinski, R. (2010) Liberation vs. Control: The Future of Cyberspace. *Journal of Democracy*, *21*(4), 43-57.
Denham, E. (2009, July 16). *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*. Retrieved from 12th April 2012 from http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.pdf.
Diamond, L. (2010). Liberation Technology. *Journal of Democracy*, *21*(3), 69-83.
Dodds, P., & Satter, R. G. (2011, August 11). Facial Recognition in Use after London Riots," *Yahoo! News*. Retrieved from 12th April 2012 from http://news.yahoo.com/apnewsbreak-facial-recognition.
Dunn, A. (2011). Unplugging a Nation: State Media Strategy During Egypt's January 24 Uprising. *Fletcher Forum of World Affairs*, *35*(2), 15-24.
Dzieza, J. (2011, August 12). Caught Red Thumbed. *The Daily Beast*. Retrieved from 12th April 2012 from http://www.thedailybeast.com/articles/2011/08/12/london-riots-police-use-social-media-to-track-rioters.html.
Electronic Communications Privacy Act, 18 U.S.C. §§ 2701-2712 (2006).
Facebook (2012a). Key Facts. Retrieved from 12th April 2012 from http://newsroom.fb.com/content/default.aspx?NewsAreaId=22.
Facebook (2012b) Statement of Rights and Responsibilities. Retrieved from 12th April 2012 from http://www.facebook.com/legal/terms.
Facebook Inc. c. Guerbuez, [2010] J.Q. no 9727.
Findlay, D. (2008). Tag! Now You're Really It. *North Carolina Journal of Law and Technology*, *10*(1), 171-202.
Gause, F. G. (2011). Why Middle East Studies Missed the Arab Spring: The Myth of Authoritarian Stability. *Foreign Affairs*, *90*(4), 81-90.
Ghosh, B. (2011, February 14). The Revolutionaries. *Time*, *177*(6), 36-40.
Geist, M. (2009, July 16). Privacy Commissioner Finds Facebook Violating Canadian Privacy Law. Retrieved from 12th April 2012 from http://www.michaelgeist.ca
Gladwell, M. (2010, October 4). Small Change: Why the Revolution will not be Tweeted. *The New Yorker*, *86*(30), 42-49.

Grainger, P. (2011, June 13). GigaPan creates 'Where's Waldo' of Sports Canucks fan Zones. *CTV News*. Retrieved from 12th April 2012 from http://www.ctvbc.ctv.ca/servlet/an/local/CTVNews/20110613 /bc_gigapan_canucks_fans_110613/20110613/?hub=BritishColumbiaHome.

Green v. America Online, 318 F.3d 465, 470-471 (3d Cir.2003).

Hashemi, Y. (2009). Facebook's Privacy Policy and Its Third-Party Partnerships: Lucrativity and Liability. *Boston University Journal of Science & Technology Law*, *15*(1), 140-161.

Hass, N. (2006, January 8). In Your Facebook.com. *The New York Times*, pp. 4A.

Hodge, M. J. (2006). The Fourth Amendment and Privacy Issues on the "New" Internet: Facebook.com and MySpace.com. *Southern Illinois University Law Journal, 31,* 95-122.

Hunter et al. v. Southam Inc. [1984] 2 S.C.R. 145.

Irons, M. E. (2011, July 17). Caught in a Dragnet. *Boston.com*. Retrieved from 12th April 2012 from http://articles.boston.com/2011-07-17/news/29784761_1_fight-identity-fraud-facial-recognition-system-license.

Katz v. United States, 389 U.S. 347 (1967).

Kerr, O. S. (2004). The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution. *Michigan Law Review*, *102*(5), 801-888.

Levine, D. (2011). Facebook and Social Networks: the Government's Newest Playground for Information and the Laws That Haven't Quite Kept Pace. *Hastings Communication & Entertainment Law Journal*, *33*(3), 481-498.

Mal, A., & Parikh, J. (2011). Facebook and the Right to Privacy: Walking a Tight Rope. *NUJS Law Review*, *4*(2), 299-322.

Mapp v. Ohio, 367 U.S. 643, 655 (1961).

Morosov, E. (2011) *The Net Delusion*. New York, NY: Public Affairs.

Office of the Privacy Commissioner of Canada (2009a, July 16). *News Releases - Facebook Needs to Improve Privacy Practices, Investigation Finds*. Retrieved from 12th April 2012 from http://www.priv.gc.ca/media/nr-c/2009/nr-c_090716_e.asp.

Office of the Privacy Commissioner of Canada (2009b, August 25). *News Releases - Letter from OPC to CIPPIC Outlining its Resolution with Facebook*. Retrieved from 12th April 2012 from http://www.priv.gc.ca/media/nr-c/2009/let_090827_e.asp.

Office of the Privacy Commissioner of Canada (2012, February 8). *PIPEDA Report of Findings #2012-002 - Facebook Didn't Get Non-Members' Consent to Use Email Addresses to Suggest Friends, Investigation Finds*. Retrieved from 12th April 2012 from http://www.priv.gc.ca/cf-dc/2012/2012_002_0208_e.asp.

Parascandola, R. (2011, August 10). NYPD Forms New Social Media Unit to Mine Facebook and Twitter for Mayhem. *NY DailyNews*. Retrieved from 12th April 2012 from http://www.NYDailyNews.com.

Paul, I. (2011, June 9). Facebook Photo Tagging: A Privacy Guide. *PC World*. Retrieved from 12th April 2012 from http://www.pcworld.com/article/229870/facebook_photo_tagging_a_privacy_guide.html

Preston, J. (2011a, February 10). Syria Restores Access to Facebook and YouTube, Raising Fears of Monitoring Users. *The New York Times*, pp. 8A.

Preston, J. (2011b, March 13). When Unrest Stirs, Bloggers are Already in Place. *The New York Times*, pp. 3B.

Preston, J. (2011c, May 22). Seeking to Disrupt Protesters, Syria Cracks Down on Social Media. *The New York Times*, pp. 10A.

Preston, J. (2011d, October 8). Protest Spurs Online Dialogue on Inequity. *The New York Times*, pp. 22A.

Preston, J. (2011e, October 17). Occupy Wall Street and Its Global Chat. *The New York Times*, pp. 7B.

Preston, J. (2011f, November 24). Protesters Look for Ways to Feed the Web. *The New York Times*, pp. 28A.

*Personal Information Protection and Electronic Documents Act (*S.C. 2000, c. 5).

R. v. Desilva, [2011] O.J. No. 1298.

R. v. Duarte, [1990] 1 S.C.R. 30.

R. v. Edwards, [1996] 1 S.C.R. 128.

R. v. Grant, [2009] 2 S.C.R. 353.

R. v. Huxford, [2010] O.J. No. 482.

R. v. Lee, [2010] O.J. No. 3060.

R. v. McCall, [2011] B.C.J. No. 115.

R. v. Plant, [1993] 3 S.C.R. 281.

R. v. Tessling, [2004] 3 S.C.R. 432.

R. v. Wong, [1990] 3 S.C.R. 36.

S.O. v. Alberta (Child and Family Services Authority), [2012] B.C.J. No. 566.

Schuster v. Royal & Sun Alliance Insurance Co. of Canada, [2009] O.J. No. 4518.

Seabrook, J. (2012, January 16). Streaming Dreams. *The New Yorker*, 87(44), 24-30.

Semitsu, J.P. (2011). From Facebook to Mug Shot: How the Dearth of Social Networking Privacy Rights Revolutionized Online Government Surveillance. *Pace Law Review*, *31*(1), 291-381.

Shane, S. (2011, January 29). Spotlight Again Falls on Web Tools and Change. *The New York Times*. Retrieved from 12th April 2012 from http://www.nytimes.com/2011/01/30/weekinreview/30shane.html.

Smith v. Maryland, 442 U.S. 735, 743-44 (1979).

Smyth, S. M. (2012). Internet Law and Policy from a Canadian Perspective. In Ismaili, K., Sprott, J. B., & Varma, K. (Eds.), *Canadian Criminal Justice Policy: Contemporary Perspectives* (pp. 326 - 357). Toronto: Oxford University Press.

Solove, D. (2001). Digital Dossiers and Dissipation of Fourth Amendment Privacy. *Southern California Law Review, 75,* 1083-1168.

Srinivasan, R., & Fish, A. (2011). Revolutionary Tactics, Media Ecologies, and Repressive States. *Public Culture*, *23*(3) 505-510.

St-Arnaud c. Facebook Inc., 2011 QCCS 1506.

Steel E., & Angwin, J. (2011, July 13). Device Raises Fear of Facial Profiling. *The Wall Street Journal*, pp. 11A.

Stoddard, J. (2010, November 22). Speech: Privacy in the Era of Social Networking: Legal Obligations of Social Media Sites. Retrieved from 12th April 2012 from http://blog.privcom.gc.ca/.

Stone, B. & Cohen, N. (2009, June16). Social Networks Spread Iranian Defiance Online. *The New York Times*, pp. 11A.

U.S. Const., amend. IV, § 1.

United States v. Choate, 576 F.2d 165, 174 (9th Cir.1978).

United States v. Hernandez, 313 F.3d 1206, 1209-10 (9th Cir. 2002).

United States v. Jacobsen, 466 U.S. 109, 114 (1984).
Weiman, G. (2010). Terror on Facebook, Twitter, and Youtube. *Brown Journal of World Affairs*, *16*(2), 45-54.
Zeran v. America Online Inc. 129 F.3d 327, 330 (4th Cir. 1997).