Modern Technologies and Privacy Rights
Leading Canadian and U.S. Case Law

Selected cases as of May 13, 2013

By Brock Jones[1]

[1] Brock Jones, Assistant Crown Attorney, Ministry of the Attorney General; Adjunct Professor, Faculty of Law, University of Toronto. The views expressed herein are personal to the author and do not represent those of the Attorney-General of Ontario nor the Crown Attorney's Office.

Computers

Case Name and Court	Summary of the Facts	Key Holdings
U.S. v. Mitchell 565 F.3d 1347 (11th Circuit Court of Appeals, 2009)	Mitchell was investigated by federal agents for possibly having visited and utilized a website known for facilitating access to child pornography. He allowed agents into his home and confessed his computer "probably" had child pornography on it. But he did not consent to a search of one computer located in his basement.	**Nature of the Individual's Privacy Rights:** The Court of Appeals described an individual's computer as being capable of holding a "universe of private information." The Court illustrated this point by referencing several examples: "Computers are relied upon heavily for personal and business use. Individuals may store personal letters, e-mails, financial information, passwords, family photos, and countless other items of a personal nature in electronic form on their computer hard drives." **Warrant Requirement:** Even though Mitchell admitted the computer had child pornography on it, he did not consent to a *search* of the computer – thus police required a warrant to search the computer's contents.
R. v. Morelli [2010] 1 S.C.R. 253	Police officers executed a search warrant of Morelli's computer based on inaccurate and misleading information. The Supreme Court found a serious violation of his rights under section 8 of the *Charter*. Notwithstanding he was facing charges of possessing child pornography, the majority	**Nature of the Individual's Privacy Rights:** The Supreme Court described a search of one's personal computer as follows: [2] It is difficult to imagine a search more intrusive, extensive, or invasive of one's privacy than the search and seizure of a personal computer.

	of the Supreme Court excluded the evidence under section 24(2) of the *Charter*, noting that it was "difficult to conceive a s. 8 breach with a greater impact on the *Charter*-protected privacy interests of the accused than occurred in this case."	[3] First, police officers enter your home, take possession of your computer, and carry it off for examination in a place unknown and inaccessible to you. There, without supervision or constraint, they scour the entire contents of your hard drive: your emails sent and received; accompanying attachments; your personal notes and correspondence; your meetings and appointments; your medical and financial records; and all other saved documents that you have downloaded, copied, scanned, or created. The police scrutinize as well the electronic roadmap of your cybernetic peregrinations, where you have been and what you appear to have seen on the Internet -- generally by design, but sometimes by accident.
U.S. v. Ziegler 474 F.3d 1184 (9th Circuit Court of Appeals, 2007)	Ziegler was employed by a corporation as a Director of Operations. He kept his work computer in a private office with a lock. Access to his computer required a password. Routine monitoring of the company network located child pornography on Ziegler's computer. The employer contacted the FBI and consented to a search of the computer. No search warrant was obtained.	**Work Computers and 3rd Party Consent:** Ziegler maintained a reasonable expectation of privacy in the work computer. The fact it was not his own personal, private computer was but one factor to consider. However, the employer had common authority over the computer which attenuated Ziegler's privacy interests. Company policy on computer use was very relevant to the Court's decision.
R. v. Cole 2012 SCC 53	Cole was a public school teacher. He was provided a laptop computer from his employer. While accessing a student's e-mail account (as part of his duties), he located nude photos of another student and copied them to the computer's hard drive.	**Privacy Rights:** Cole had a reasonable expectation of privacy in his work computer. Ownership of property is a relevant consideration. Workplace policies are also relevant, but not determinative. One must consider the "totality of the circumstances."

	A school technician located a hidden folder on Cole's hard drive during routine monitoring, and inside located images that he believed constituted child pornography. The school's principal instructed him to make a copy of the materials and handed the copy over to the police. The police seized the computer and searched the hard drive without a warrant.	**Requirement of a Warrant:** The police required a warrant to search the computer and the CD (although they could seize them temporarily to safeguard their contents.) They are not relieved from obtaining a warrant simply because they are provided with evidence lawfully obtained beforehand by another state actor (i.e. the school principal.) **Third party consent?** It does not apply The school board could not waive the privacy interests of Cole without his consent. **School Officials:** The principal's actions did not violate section 8 of the Charter. Principals have a statutory duty to maintain a safe school environment and by necessary implication, a reasonable power to seize and search a school-board issued laptop if the principal believed on reasonable grounds that it contained compromising pictures of a student.
R. v. Ballendine 2011 BCCA 221	A man was arrested in Italy for producing and distributing (via the internet) child pornography. His business records disclosed Ballendine (who lived in Victoria, B.C.) had ordered DVDs containing CP by e-mail. The Victoria Police Department obtained a search warrant for Ballendine's residence, his computers, and "devices capable of storing data, such as hard-drives…" A	**Overbroad?** The court ruled that while the warrant had no parameters on the types of files that could be accessed or on the relevant time frame within which the police were entitled to examine the dated files on the computer, those were not fatal because the warrant's other terms qualified the extent of the search to *specific types of evidence* (relating to the particular fraud investigation). Thus it was not too broad. (Data parameters were not "particularly pertinent" to that inquiry).

	forensic examination of the hard-drive of a computer located CP videos. Ballendine challenged the search warrant's validity at trial.	
R. v. Jones 2011 ONCA 632	In 2005, Jones was under investigation for fraud allegedly perpetrated through the use of a computer. Officers obtained a search warrant to seize his computer and search it for *evidence of fraud*. While viewing the computer's contents, the police noted images that appeared to constitute child pornography. The police determined the rest of the computer could be searched for more evidence of child pornography without a second warrant. A full examination of the computer then yielded multiple images and videos of child pornography.	**Was the search of the computers and cell phone lawful in the absence of a secondary warrant?** Yes. The BCCA held that the authority to search for "documentation" extends to electronically-stored information. Furthermore, the authority to search computers and similar device need not be expressly stated on the face of a warrant. "When the police, in the course of executing a warrant, locate a device that can reasonably be expected to contain an electronically-stored version of a thing they have been authorized to search for, they can examine that device for the purpose of determining whether it contains that thing (i.e. information), but only to the extent necessary to make that determination." The Court noted that had the police conducted a more thorough examination of the computer and cell phone, different considerations would have presented themselves – but those were not argued on appeal.

R. v. Vu 2011 BCCA 536 (On appeal to the SCC)	The police obtained a search warrant to investigate theft of electricity at a residence. The warrant authorized them to search for equipment used to divert electricity but also "documentation identifying ownership and/or occupancy" of the residence. Inside the home the police found two computers and cell phone. The warrant did not explicitly authorize the search of computers or cell phones. The police nevertheless searched these items without a secondary warrant. Evidence located within them tied Vu to the residence. Specifically, both MSN messenger and Facebook were running on the computer when it was examined by the police. The officer had merely to click on the respective icons to see certain information that was already loaded onto the computer. It does not appear a full, forensic examination of the computer or cell phone occurred.	**Requirement of (Secondary) Warrants:** 1. The residential search warrant authorized seizing "media capable of storing data." The digital memory card met this standard. But the warrant did not explicitly specify what *type* of data was being searched for on the storage media. The court held that warrant was *not overbroad*, because the broad, unrestricted terms in the warrant were qualified by *further items* which served to limit the *types of evidence* that the police were entitled to look for. 2. With respect to the Hitachi hard-drive, the court held that the search warrant itself did not list child pornography as something to be searched for. Furthermore, searching for the *types of information* set out in the warrant would *not involve a search of video files.* Even evidence of Rafferty's internet usage history was inadmissible as it was not specified in the original search warrant. 3. The Crown conceded the police had no warrant to search the laptop and Blackberry located in the Honda civic and this constituted a violation of Rafferty's section 8 rights. The court agreed, citing *R. v. Little* [2009] O.J. no. 3278 (SCJ).

R. v. Rafferty 2012 ONSC 703 (S.C.J.)	Police obtained a search warrant to seize a Honda Civic owned by Rafferty. Inside the car they located a laptop computer and Blackberry. Police also obtained a search warrant for Rafferty's residence. Inside they located a 20 gigabyte Hitachi hard drive and a digital memory card from a camera. The warrant authorized seizing computer systems, peripherals, and media capable of storing data. But the warrant also stated the target of the search included documents showing a relationship between Rafferty, McClintic and the victim and her family. The Hitachi hard drive was examined and it was determined in 2005-6 the Applicant had downloaded child pornography using LimeWire. When the laptop was examined, the police found data fragments from which it could be inferred he had also used Limewire in the moths leading up to the offence to access child pornography. The defence argued: 1. The warrants did not allow for a subsequent sufficiently tailored search of the items' contents;	**Overly Broad warrant?** No. The warrant that was issued was therefore not overly broad because it was anchored in the specific conditions of the LTSO. The computer would only reasonably yield information about some of these conditions.

	2. If they did pass facial validity, they were nevertheless overbroad; and 3. The police required secondary warrants to search the items found in the Honda Civic.	
R. v. Bourdon 2013 ONCA 86	The accused was subject to a LTSO. One of the conditions prohibited him from accessing the internet or possessing any computer that had internet capability. The parole authorities sought a warrant to search for breaches of the LTSO, and attached that certificate to the ITO.	**Application Denied.** The government's reliance on an IP address associated to emails sent and received from the presumed "target computer" lends itself to potential pitfalls. The person(s) sending the emails in question may have used "spoofing" software to disguise their true IP address, and therefore the installation of the Trojan software could target innocent computer users and their computers. The computer in question could also be in a public space such as a café or library. Installation of the spyware would potentially capture many innocent persons utilizing the computer for innocent purposes. The government's application would also permit real-time video surveillance via the computer's webcam. As such, the government must apply for a wiretap authorization, not a warrant. Future applications must address the court's concerns before a warrant would issue.

In Re Warrant To Search A Target Computer at Premises Unknown (*United States District Court Southern District of Texas, Houston Division*) Case # H-13-234M April 22, 2013 Smith J.	Federal law enforcement officers applied for a search and seizure warrant targeting a computer allegedly used to commit various crimes, including bank fraud and identity theft. The computer's exact physical location was not exactly known, but it could be accessed via the internet. The requested warrant would have authorized the police to *surreptitiously install* software designed to not only extra certain stored electronic records but also to generate information over a 30 day period *going forward*. That information would include utilizing the computer's "webcam" to take photos of the user without his or her knowledge, to transmit latitude and longitude coordinates for the computer's location, and to record what applications were being run. It was, in effect, a request to install a Trojan spyware program. (*The rule utilized in this case seems to be roughly analogous to the "general warrant" provisions under s. 487.01 of the Criminal Code of Canada.*)	**Did use of the "Stringray" violate the accused's reasonable expectation of privacy?** No. Campbell J. held that the suspect could not "credibly argue that he had a legitimate expectation of privacy" because he had allegedly rented his apartment and purchased his computer fraudulently using false identities. As the accused had *obtained all the items in question through fraud* (including the aircard), there was no objectively reasonable expectation of privacy in the items. The judge also added that the use of the Stingray did not constitute a "severe intrusion." The device mimicked a cell tower and sent signals to, and received signals from the aircard. While the FBI did not disclose in its initial warrant application to utilize Stingray that the mobile tracking device would capture signals from *other cell phones and aircards in the area* (i.e. from innocent third parties), this was a "detail of execution which need not be specified."
United States of America v. Rigmaiden District Court of Arizona, Campbell J. (May 8, 2013)	The accused was alleged to have partaken in an elaborate scheme to file fraudulent tax returns to the government in the names of deceased persons and third parties. The government was able to track and locate an "aircard" connected to a laptop	

	computer allegedly used in the scheme. When the fraudulent tax returns were filed online, an IP address was left behind. That IP address came back to the aircard in question. It was a mobile device, however. As part of its investigation, the authorities utilized a clandestine tracking device called the “Stingray.” The Stingray is a transceiver used by the FBI to locate suspects. It sends out a signal that tricks phones within a targeted area into hopping onto a fake network. This in turn generates information the authorities can utilize to pinpoint its exact geographical location. Armed with that information, the authorities located and arrested the accused, his computer, and the aircard.	

Third Party Consent to Searches

R. v. Cole 2012 SCC 53	The school board essentially provided the computer to the police and consented to its contents being searched. [Please see the prior discussion of the facts in this case for more detailed information.]	**Third Party Consent to a Search:** Cole's employer could *not* consent to a search of the computer by the police. The doctrine of third party consent does not apply in Canada. The school board could not waive the privacy interests of Cole without his own informed consent.
City of Ontario v. Quon 529 F. 3d 892 (2010) (Supreme Court of the United States)	Quon was a police sergeant. He and other officers had utilized a government alphanumeric pager system for personal messages. The employer's position on personal use was somewhat fluid – personal messages were not entirely forbidden. Quon exceeded his billing limits and an investigation began. Many messages were personal and some were sexually explicit, sent by the married Quon to his girlfriend at work. In one month as few as 8% of Quon's texts had been work-related Quon and others sued for violations of their privacy rights.	**Reasonable Expectation of Privacy in A Work "Personal Electronic Device"?** The majority opinion decided the case purely on the reasonableness of the pager audit, explicitly refusing to consider "far-reaching issues" it raised on the grounds that modern communications technology and *its role in society was still evolving*. The majority did assume (implicitly) that police officers did have a reasonable expectation of privacy in their pager communications and that "employer policies concerning communications will of course shape the reasonable expectations of their employees, especially to the extent that such policies are clearly communicated."

United States v. Stabile 633 F. 3d 219 (3rd Circuit Court of Appeals, 2011)	Stabile shared a residence with his spouse. Authorities arrived when he was not home to investigate counterfeit cheques. His spouse was present and consented to the authorities searching the house. Several hard drives were seized and searched. Images of child pornography were located.	**Spouse's Consent Sufficient?** Stabile's spouse could legally consent to the seizure of the computers. Where multiple people may use the same computer and store information on the same hard drive, factors such as the identity of the users, whether password protection is used, and the location of the computer in the house will help determine *who may grant consent.*
U.S. v. Ziegler 474 F.3d 1184 (9th Circuit Court of Appeals, 2007)	Ziegler was employed by a corporation as a Director of Operations. He kept his work computer in a private office with a lock. Access to his computer required a password. Routine monitoring of the company network located child pornography on Ziegler's computer. The employer contacted the FBI and consented to a search of the computer. No search warrant was obtained.	**Work Computers and 3rd Party Consent:** Ziegler maintained a reasonable expectation of privacy in the work computer. But the employer had common authority over it and *could consent to the search*. Company policy on computer use was very relevant to the Court's decision.

Plain View Doctrine

R. v. Jones 2011 ONCA 632 (Ontario Court of Appeal)	In 2005, Jones was under investigation for fraud allegedly perpetrated through the use of a computer. Officers obtained a search warrant to seize his computer and search it for *evidence of fraud.* While viewing the computer's contents, the police noted images that appeared to constitute child pornography. The police determined the rest of the computer could be searched for more evidence of child pornography without a second warrant. A full examination of the computer then yielded multiple images and videos of child pornography.	**Plain View?** Noting that a "computer search pursuant to a warrant must be related to the legitimate targets respecting which the police have established reasonable and probable grounds", the court dismissed the notion that once a computer is lawfully seized its entire contents may be pored over by state authorities without restraint. It is not merely an "indivisible object." The police may examine any file or folder on a computer to *reasonably accomplish the authorized search*, but only in a "cursory fashion, in order to determine whether they are likely to contain *evidence* of the type they are seeking." The plain view doctrine's contours must continue to be respected in the realm of digital evidence. While it authorized the police to *seize* those files which were lawfully examined in a *"cursory manner"* and which themselves revealed evidence of a criminal offence, it did not authorize the police to continue *searching* for further evidence of unrelated crimes to those targeted by the initial warrant. In Jones' case, child pornography video files sought out by the police had nothing to do with the original scope of the search warrant and were therefore clearly unlawfully seized.

United States v. Stabile 633 F. 3d 219 (3rd Circuit Court of Appeals, 2011)	A police officer began searching the computer for evidence of financial crimes, pursuant to a warrant. He came upon a folder labelled "Kazvid", opened it, and located file names suggestive of child pornography. The files were viewed to confirm they were child pornography, without another warrant.	**Plain View?** While criminals can "hide, mislabel or manipulate files to conceal criminal activity"… granting state authorities "carte blanche" to search every file "impermissibly transforms a limited search into a general one." Concerns about "overbroad" searches remain serious ones. However, in this case, the file *names* were in plain view. Thus, the doctrine applied (at least, initially.) The plain view doctrine should be updated to a digital era by allowing its "contours… to develop incrementally through the normal course of fact-based adjudication."
United States v. Comprehensive Drug Testing Inc. 621 F.3d 1162 (9th Circuit Court of Appeals, 2010)	The federal government was conducting an investigation into the use of steroids by professional baseball players. Ten players tested positive. The government obtained warrants to obtain information from private entities that had collected the samples and information. CDT was one of those entities. The government seized and reviewed the drug testing records of hundreds of players, not just the ten the warrant specified.	**Plain View?** The government attempted to rely on the plain view doctrine to justify the discovery of the additional files. The Court viewed this claim sceptically. It noted that "by necessity, government efforts to locate particular files will require examining a great many other files to exclude the possibility that the sought-after data are concealed there. Once a file is examined, however, the government may claim… that is contents are in plain view and, if incriminating, the government can keep it." Such a search could in theory be virtually limitless.

Cell Phones and "Smart" Phones, Incl. Text Messages

R. v. Polius [2009] O.J. No. 3074 (Ont. Sup. Ct.)	Polius' cell phone was seized when he was arrested for counselling murder. When examined without a warrant, it disclosed his cell phone number. This the police used to obtain his cell phone records which were tendered into evidence at trial. Justice Trafford of the Ontario Superior Court found that the officer who seized and examined the cell phone without a warrant did not have a reasonable basis for his belief that it may contain evidence of the alleged offence; as a result, its seizure was not lawful.	**Search Incident to Arrest?** A search warrant was required to examine an item *beyond the cursory inspection* permitted in certain situations. "The power to SITA [search incident to arrest] includes a power to conduct a cursory inspection of an item to determine whether there is a reasonable basis to believe it may be evidence of the crime for which the arrest was made. However, any examination of an item beyond a cursory examination of it is not within the scope of the power to SITA. Using other words, the evidentiary value of the item must be reasonably apparent on its face, in the context of all of the information known by the arresting officer. Where the purpose of a SITA is to find evidence of the crime, the standard governing the manner and scope of the search is a "... reasonable prospect of securing evidence ...". See *R. v. Caslake*, *supra*, at para 21. The police "... must be in a position to assess the circumstances of the case so as to determine whether a search meets the underlying objectives ..." of the SITA. See *Cloutier v. Langlois*, *supra*, at paras. 60-62. [Emphasis added]."

R. v. Manley 2011 ONCA 128	After his arrest on lawful grounds, police officers located a cell phone on Manley and investigated it to determine the rightful owner. When examining its stored data they found a photograph of Manley holding a sawed-off shotgun. The police then obtained a warrant to search the remaining contents of the phone.	**Reasonable Search?** It was reasonable for the police to conduct a "*cursory search"* of the phone to determine its ownership, as the police had credible evidence Manley possessed stolen cell phones in the past. But the Court cautioned that its decision rested on an agreement that the police did not search the stored data in the cell phone for any other purpose. Had the police been able to satisfy themselves as to its ownership without reviewing its electronic contents, such a search would have been unlawful. **Privacy Rights?** "Cell phones and other similar handheld communication devices in common use have the capacity to store vast amounts of highly sensitive personal, private and confidential information – all manner of private voice, text and e-mail communications, detailed personal contact lists, agendas, diaries and personal photographs. An open-ended power to search without a warrant all the stored data in any cell phone found in the possession of any arrested person clearly raises the spectre of a serious and significant invasion of the *Charter*-protected privacy interests of arrested persons. If the police have reasonable grounds to believe that the search of a cell phone seized upon arrest would yield evidence of the offence, the *prudent course is for them to obtain a warrant authorizing the search.*"

R. v. Fearon 2013 ONCA 106	The appellant was arrested for robbery while armed with a firearm. Upon arrest, a police officer conducted a pat down search and located a cell phone. The officer examined the contents of the phone and found photographs of a gun and cash, as well as an incriminating text message. The appellant was brought to the station, where there was a further search of the cell phone over the course of the next two days, as well as periodically prior to the obtaining of a warrant several months later. However, the subsequent searches did not produce any evidence that was relied on at trial beyond what was found during the initial search incident to arrest. On appeal, the appellant argued the search of the contents of the cell phone went beyond the permissible limits of a search incident to arrest. The officers testified that their belief the phone could have been used in the commission of the offence was premised on their own investigative experience – to wit, that when multiple suspects are involved in a robbery, they often communicate with each other via calls or text messages. The officers also testified that suspects often take pictures of their loot and store it on their phones.	**Search Incident to Arrest?** Yes. The Court considered whether to carve out a cell phone exception to the common law doctrine of search incident to arrest. The Court stated that creating such an exception would be a significant departure from the existing state of the law, and that the record in this case did not suggest it was necessary. While ultimately concluding "If it ain't broke, don't fix it", the Court did note the following: (a) the contents of a cell phone can be highly personal and sensitive in nature, attracting a high expectation of privacy; (b) it was significant that the cell phone was not password protected or otherwise "locked" to users other than the appellant when it was seized; (c) the police had a reasonable belief that the cell phone would contain relevant evidence (*based on their own prior investigative experiences)*; (d) the police were within the limits of *Caslake* to examine the contents of the cell phone in a cursory fashion to ascertain if it contained ***evidence*** relevant to the alleged crime (*and note that a "cursory search" involved manipulating the phone*

		and locating pictures and text messages NOT in plain view); (e) if a cursory examination did not reveal any such evidence, then at that point the search incident to arrest should have ceased; (f) there was no suggestion in this case that this particular cell phone functioned as a "mini-computer" nor that its contents were not "immediately visible to the eye". The Court stated that if the cell phone had been password protected or otherwise "locked" to users other than the appellant, it would not have been appropriate to take steps to open the cell phone and examine its contents without first obtaining a search warrant.
R. v. Hiscoe [2013] N.S.J. No. 188 Nova Scotia Court of Appeal	Accused was charged with possession of cocaine for the purpose of trafficking. Upon arrest, police seized the accused's smartphone, which was on the seat of his car. At the arrest scene, an officer opened the phone and reviewed a number of text messages. The officer reviewed the messages again later that evening and transcribed them. Almost a month later, police downloaded the entire contents of the accused's smartphone.	**Search Incident to Arrest v. Full Search of the Phone's Contents:** The rights enshrined in s. 8 must remain aligned with technological developments. The period between arrest and search is a legitimate factor for consideration in deciding whether a search incident to arrest is lawful. Here, the *initial* search of the phone was incidental to arrest and was lawful. But the accused's rights under s. 8 had been violated by reason of the *full content*

	The judge described Mr. Hiscoe's cell phone as a "regular smart phone, a Blackberry sort of phone" and observed that such phones could store dozens of gigabytes of data not unlike personal or home computers, for which there is a high level of privacy. The seizure of his cell phone was lawful under the search incident to arrest power, because it was on the driver's seat at the time of the respondent's arrest and Cst. Foley had a reasonable basis to believe that it contained text messages relating to the apparent drug meeting with the driver of the second car.	*download* of the respondent's smartphone a month later (without a warrant.) The trial judge's inferences regarding heightened expectations in privacy in such sophisticated technological devices that often contained an individual's entire personal information library were accepted. **On Passwords:** While the presence or absence of a password or lock may be another relevant factor in determining whether a search incident to arrest is lawful or within its proper parameters, it should not be determinative. Whether such a security feature exists or is turned on is not substantively helpful in determining the privacy interests of the accused in the contents of his cell phone, nor the propriety of a police search. Just because a password is not on at the very moment the police seize a cell phone cannot mean that the state is welcome and free to roam through its contents.
R. v. Little [2009] O.J. No. 3278 (S.C.J.)	A smartphone is lawfully seized by the police pursuant to s. 489(1)(c) of the *Code* during a search of the residence of the accused. The smartphone was not specifically identified in the search warrant.	**Can the police search this smartphone, even if lawfully seized, with a second warrant?** Fuerst J. held that it was permissible to analyze the phone to determine its telephone number, and to forensically analyze blood spatter on it.

	The police conduct a full examination of the smartphone's contents.	BUT, the police needed a second warrant to examine the information stored in it. There was no urgency to do so, and no other circumstances that made it impracticable to obtain judicial authorization for the search.
R. v. S.M. [2012] O.J. No. 2833 (S.C.J.)	S.M. is charged with being a party to a murder, On the cell phone of a co-accused, seized pursuant to a warrant, his nickname appears on the contact list with his phone number. This, among other items, become crucial evidence against him and key to the furtherance of the investigation that leads to his arrest at a later date.	**Can a person claim a privacy interest in the contents of another person's cell phone?** Yes and No. S.M. had no standing re: certain forms of information. S.M. had an insufficient privacy interest in the **contact list** in the co-accused's cell phone. Information contained in a contact list will involve private information belonging to each contact (nickname, phone number). But any privacy interest the contact has in that information is significantly reduced once that person communicates that information to other persons knowing that those persons may record it and/or share it with others. Also, one does not have any privacy interest in: (1) **photos**; or (2) **recordings** if they were contained within another's cell phone and created by or on behalf of the owner of the cell phone.

		However, a non-owner of a cell phone does have an ongoing and important privacy interest in other information that might be obtained from another person's cell phone. This includes **text messages** contained in a cell phone or that can be obtained from the records of the carrier for that cell phone, if they were sent to that one person and intended solely for that person to view. That the recipient might show others the message matters not.
R. v. Liew [2012] O.J. No. 1365 (Ont. S.C.J.)	Liew and another male were arrested in Markham as they unloaded a shipment (they expected to be drugs) from a tractor trailer. Liew was carrying a cell phone. The arresting officer seized the phone and immediately conducted what he called a "cursory search" of it. He checked the call history feature of the phone and wrote down the five phone numbers listed in it. The officer said he wanted to know about other possible suspects - people who might be coming to meet up with Liew - or people whom they were going to deliver the drugs to. He also didn't want evidence to be lost. He said it's his understanding that someone can send a "kill signal"	**Was the "cursory" search justified on the facts of this case?** The Court held that the seizure of the phone was justifiable as the police had reasonable grounds to believe Liew was receiving a shipment of cocaine and may have been contacting others about the arrival of the shipment. However, the Court also held that in the absence of exigent circumstances, searching the contents of the phone without a warrant was unlawful. Even a "cursory search" was unjustified. *Manley* can be distinguished as in that case there were concerns as to whether or not Manley was the lawful owner of the phone (he wasn't.) No such concerns existed for Liew.

	remotely to a phone to wipe out its contents. Later, at the police division, and still without a warrant, officers conducted an extensive search of the phone's contents.	As a general rule, the police must obtain a warrant to search the cell phone's contents.
U.S. v. Skinner 6th Circuit Court of Appeals August 14, 2012 Case No. 09-6497	The accused was a drug mule. He was given a "pay as you go" cell phone by other drug suppliers. He used the phone during his drug-transporting. There was no subscriber agreement for the phone in his own name. The phone had GPS technology that was active when Skinner was using it. The police discovered someone named "Big Foot" was involved in the drug trade and without a warrant, found the location of the phone via "ping"ing it (with the phone company's assistance.) The cell phone company told the police where the phone was at various times. Ultimately, the police found Skinner with his phone, and 1000 lbs of marijuana in a mobile home.	**A Reasonable Expectation of Privacy in the GPS coordinates?** The challenge in the US courts was based on the warrantless "search" of the cell phone's GPS data (which lead to everything else.) The majority of the 6th circuit held that the accused "had no reasonable expectation of privacy in the phone's GPS data or the location of his cell phone." The fact that accused was not aware the GPS signal was active thus informed his subjective beliefs did not constitute an objectively founded reasonable expectation of privacy. Furthermore, it is worth nothing the Court began its decision by noting that "[w]hen criminals use modern technological devices to carry out criminal acts and to reduce the possibility of detection, they can hardly complain when the police take advantage of the inherent characteristics of those very devices to catch them."

R. v. Mahmood 2011 ONCA 693	After an armed robbery of a jewellery store, the police had few leads. They obtained a standard search warrant for the records of four major cell phone companies for all subscriber accounts that utilized the closest tower to the scene of the robbery on the relevant date and time. This was a "tower dump" warrant. After some further investigation, the police supplement this information with new information to obtain the records of some specific suspects via another standard warrant. This was a "subscriber warrant." As a result of the first two warrants, the police are able to obtain a standard search warrant for the residences of the accused parties.	**A reasonable expectation of privacy in cell phone records?** YES – even though they are held by the cell phone company and reveal little personal information about the subscriber. But the expectation of privacy is "significantly reduced", accordingly. However, the police can obtain these records on the less rigorous standard contained in section 492.2(2), rather than the standard "credibly based probability" requirement in section 487. Section 492.2(2) requires "reasonable grounds to suspect that an offence… has been committed ad that information that would assist in the investigation of the offence could be obtained through the use of a number recorder…"
R. v. Burnett [2012] O.J. No. 6350 (S.C.J.)	Accused was charged with importing firearms. A Canadian studying in the United States, accused entered Canada by car and was connected by his name with an investigation from the day before of a man who had been refused entry to the U.S. A sniffer dog detected contraband inside his vehicle. As a result of the positive indication and the other indicators known to the officers at that point, a Border Services officer detained the accused and read him his	**The border matters:** The Court denied the application to exclude the text messages. It was important to make a finding of fact that at the point in time when Border Services officer first viewed photos and text messages on the cell phone, he was aware of strong indicators that the accused was violating Canada's laws of entry.

	rights to counsel and caution. He was then frisk searched by another officer and the currency he was carrying was counted. At this point an officer examined the cell phone that the accused brought into the country with him. This took no more than five minutes, during which time the officer observed suspicious text messages with respect to possible crimes.	
Quon v. Arch Wireless Operating Company 529 F. 3d 892 (Ninth Circuit Court of Appeals, 2008)	Quon was a police sergeant. He and other officers had utilized a government alphanumeric pager system for personal messages. The employer's position on personal use was somewhat fluid – personal messages were not entirely forbidden. Quon exceeded his billing limits and an investigation began. Many messages were personal and some were sexually explicit, sent by the married Quon to his girlfriend at work. In one month as few as 8% of Quon's texts had been work-related. He was subject to disciplinary proceedings. Quon and others sued for violations of their privacy rights.	**A reasonable expectation of privacy in text messages stored on the service provider's network?** Yes. Users of text messaging services ordinarily have a Fourth Amendment reasonable expectation of privacy in the contents of the text messages stored on the service provider's network. The *content* of the messages should be viewed differently than the addressing information associated with them. Both text messages and email messages are sent from user to user via a service provider that stores the messages on its servers, but user do have a reasonable expectation of privacy in the content of their text messages (as do the authors and recipients of email messages.)

R. v. Telus Communications 2013 SCC 16	The police in this case obtained a general warrant and related assistance order under ss. 487.01 and 487.02 of the *Criminal Code* requiring Telus to provide the police with copies of any stored **text messages** sent or received by two Telus subscribers. The relevant part of the warrant required Telus to produce any messages sent or received during a two-week period on a daily basis. Telus applied to quash the general warrant arguing that the prospective, daily acquisition of text messages from their computer database constitutes an interception of private communications and therefore requires authorization under the wiretap authorization provisions in Part VI of the *Code*.	**A split judgment:** The court split 3-2-2. Abella J. wrote for three judges, and Moldaver J. concurring in the result for two judges. Cromwell J. wrote the dissent for himself and McLachlin C.J. Abella J. decided the case by interpreting "intercept a private communication" under Part VI. Moldaver J. declined to interpret the meaning of "intercept" and instead found that the search in question was the functional equivalent of a Part VI intercept. **Abella J. on privacy rights in text messaging:** Despite technological differences, text messaging bears several hallmarks of traditional voice communication: it is intended to be conversational, transmission is generally instantaneous, and there is an expectation of privacy in the communication. [1] Text messaging is, in essence, an electronic conversation. The only practical difference between text messaging and the traditional voice communications is the transmission process. This distinction should not take text messages outside the protection of private communications to which they are entitled in Part VI. Technical differences inherent in new technology should not determine the scope of protection afforded to private communications. [5] **On 3rd party conduit:** The communication process used by a third-party service

		provider should not defeat Parliament's intended protection for private communications. Telecommunications service providers act merely as a third-party "conduit" for the transmission of private communications and ought to be able to provide services without having a legal effect on the nature (or, in this case, the protection) of these communications: see *Society of Composers, Authors and Music Publishers of Canada v. Canadian Assn. of Internet Providers*, 2004 SCC 45, [2004] 2 S.C.R. 427, at paras. 100-101) [41]
R. v. Desrosier and Peppler 2013 BCPC 41545-1	Defence brought a Charter motion to exclude from evidence text messages retrieved from a Blackberry located inside a safe. The police had a valid search warrant, but not a Part VI authorization. The defence argued that the Supreme Court's decision in *R. v. Telus Communications Co.* required the police to obtain a part VI authorization before they could seize the stored text messages.	**Application denied.** *Telus Communication Co.* was directed at the *prospective* retrieval of text messages from a third party service provider. It does not apply to the seizure of text messages already stored on a user's personal device.

E-Mail Messages and IP Addresses

United States v. Warshak 631 F.3d 266 (6th Circuit Court of Appeals, 2010)	Warshak was charged with defrauding customers. The government obtained thousands of e-mails from Warshak's Internet Service Provider without a warrant.	**Privacy Rights?** A "subscriber enjoys a reasonable expectation of privacy in the content of e-mails stored, sent or received through a commercial ISP." A warrant is required to compel an ISP to turn over the contents of a subscriber's e-mails. **Keeping Pace with Change:** "The Fourth Amendment must keep pace with the inexorable march of technological progress, or its guarantees will wither and perish." **Email:** "Since the advent of e-mail, the telephone call and the letter have waned in importance, and an explosion of Internet-based communication has taken place. People are now able to send sensitive and intimate information, instantaneously, to friends, family, and colleagues half a world away. Lovers exchange sweet nothings, and businessmen swap ambitious plans, all with the click of a mouse button. Commerce has also taken hold in e-mail. Online purchases are often documented in e-mail accounts, and email is frequently used to remind patients and clients of imminent appointments. In short, "account" is an apt word for the conglomeration of stored messages that comprises an e-mail account, as it provides an account of its owner's life. By obtaining access to someone's e-mail, government agents gain the ability to peer deeply into his activities."

United States v. Forrester 512 F.3d 500, 510 (9th Circuit Court of Appeals, 2008)	During an investigation of the accused parties' ecstasy manufacturing operation, the government employed various computer surveillance techniques to monitor their email and internet activity. A court order authorized the installation of a "mirror port" on the co-conspirator's account with his ISP. This allowed the government to learn the "to/from" addresses from email messages, the IP addresses of the websites visited, and the total volume of information sent to or from the account.	**A reasonable expectation of privacy?** No. Email and internet users have no reasonable expectation of privacy in the "to/from" addresses of their messages or in IP addresses of websites visited. The Court rested its decision largely on the fact this routing information passes through and may be held by a third-party conduit, i.e. the ISP, for the purposes of ensuring the communication reaches its desired address or location. (*Query: Would this analysis hold up in Canada? The involvement of a "third-party" conduit that has access to the information in question seems to be of less significance, generally.*)
Quon v. Arch Wireless Operating Company 529 F. 3d 892 (Ninth Circuit Court of Appeals, 2008)	Quon was a police sergeant. He and other officers had utilized a government alphanumeric pager system for personal messages. The employer's position on personal use was somewhat fluid – personal messages were not entirely forbidden. Quon exceeded his billing limits and an investigation began. Many messages were personal and some were sexually explicit, sent by the married Quon to his girlfriend at work. In one month as few as 8% of Quon's texts had been work-related. He was subject to disciplinary proceedings.	**A reasonable expectation of privacy in the content of e-mail messages stored on the service provider's network?** Yes. In *Forrester* the Court did not rule on whether persons have a reasonable expectation of privacy in the content of e-mails. The Court did conclude however that "[t]he privacy interests in these two forms of communication [letters and e-mails] are identical," and that, while "[t]he contents may deserve Fourth Amendment protection . . . the address and size of the package do not."

Peer-To-Peer (P2P) Networks / Internet Subscriber Information

R. v. Ward 2012 ONCA 660	A German investigation revealed persons had been accessing child pornography via a website. Some of the access came via a Canadian ISP, Bell-Sympatico. The Canadian police received information from their German counterparts that some specific IP addresses on specific dates and times had accessed child pornography files. The RCMP sent a "letter of request" to Bell for subscriber information relating to the IP addresses in question. This letter referenced *PIPEDA*. Bell complied. The police then obtained a warrant for Ward's home and computer. They located child pornography files.	**Reasonable Expectation of Privacy?** *PIPEDA* acknowledges that disclosure of personal information by a private sector business – even without the consent of the individual in question – may lawfully occur. Section 7(3) authorizes this disclosure, but does not mandate it. *PIPEDA* does not create any police search and seizure powers. The terms of *PIPEDA* inform one's reasonable expectation of privacy under section 8 of the *Charter*. Similarly s. 487.014(1) of the *Code* authorizes the police to request information that may be disclosed under *PIPEDA*. It does not create a search and seizure power. While the relationship with Bell was relevant information, the fact that one allows a third party into one's "zone" of personal privacy does not vitiate one's rights under the *Charter*. The "risk analysis" doctrine in the US is rejected. Ward did NOT have a reasonable expectation of privacy in his subscriber information held by Bell-Sympatico.

R. v. Trapp 2011 SKCA 143 ***R. v. Spencer*** 2011 SKCA 144 (Sask. Court of Appeal) **(On appeal to the Supreme Court of Canada; due to be heard October 2013)**	***Trapp*****:** A member of the Saskatoon Police Service logged onto the Gnutella network on July 24, 2007. She browsed the network for the purpose of determining whether anyone in Saskatchewan had files containing child pornography available for sharing on the network. While browsing a shared file folder she discovered they contained child pornography files. She downloaded these files to confirm their status as child pornography. The IP address for the computer sharing these files was publicly available. The officer then sent a letter of request to the ISP in question (SaskTel) for "any information" relating to this IP address. SaskTel confirmed the IP address belonged to Trapp. Officers executed a search warrant on his personal computer in his home and located child pornography files.	**A "Search"?** The majority in *Trapp* held that the offender did maintain a reasonable expectation of privacy in his subscriber information held by the ISP, notwithstanding his access and use of a file sharing network. They held, "[w]hen one subscribes for Internet access service, one does not surrender one's expectation of privacy regarding what one chooses to access on the Internet." However, the majority also held that the search was a reasonable one and thus no violation of section 8 of the *Charter* occurred. The latter conclusion was derived primarily through a combination of section 487.014(1) of the *Criminal Code* and section 29 of *The Freedom of Information and Protection of Privacy Act* (a provincial statute). The combination of these two acts justified the police "letter of request" for SaskTel to provide subscriber information, and SaskTel's decision to provide that information voluntarily. As such, the search was authorized by law, the law was reasonable and the manner in which the search was conducted was reasonable. **In dissent**, Ottenbreit J.A. held that "[w]ith the advent of crimes involving the internet, the letter [of request] was a reasonable way for police to determine the identity of someone allegedly committing prohibited acts using a file-sharing network on the internet." He concluded that Trapp had no reasonable

	***Spencer*:** Similar to the offender in *Trapp*, Spencer obtained a number of files containing child pornography over the internet through the file-sharing program LimeWire. He retained the files in a shared folder on his personal computer and others were able to view and download the child pornography. An officer with the Saskatoon Police Service logged onto the LimeWire network on August 31, 2007 and located the child pornography in the shared folder. The IP address associated with the computer hosting the shared folder was publicly available. The officer then sent a letter of request for the "customer identifying information" surrounding that subscription account to Shaw Communications (the ISP.) Shaw complied and a warrant was obtained to search the residence in question. The IP address was registered to Spencer's sister. However, Spencer also resided there. Spencer's computer was seized and searched and child pornography was located on its hard-drive.	expectation of privacy in his name, address and phone number respecting his IP address. **The "Majority" – A Search?** Two judges – Caldwell J.A. and Ottenbreit J.A. – hold the accused had no reasonable expectation of privacy in the internet subscriber information in question. Among other considerations, the majority examined the contractual agreement with Shaw Communications which explicitly contemplated disclosure to the authorities upon request. Furthermore, the combination of section 487.014(1) of the *Code* and section 7(3) of *PIPEDA* (which applies to private businesses) allowed for the police letter of request in question. 7(3)(c.1) of *PIPEDA* in particular authorized the voluntary disclosure of "an individual's personal information to the police by a third party without the individual's knowledge or consent", if the disclosure was "made to a government institution…" "for the purpose of administering any law of Canada." This factor militated against finding a reasonable expectation of privacy in the subscriber information. **In partial dissent**, while agreeing with the result, Cameron J.A. (who authored the majority decision in *Trapp*), noted that he was "doubtful" the offender held no reasonable expectation of privacy in the disputed information.

United States v. Perrine 518 F. 3d 1196, 1204 (10th Circuit Court of Appeals, 2008)	An unknown person was in an online Yahoo! chat room in September 2005 using the alias "stevedragonslayer." He invited a civilian to view his webcam which showed a young female child engaged in sexual activity. The civilian reported this to law enforcement. With this information, the police were able to determine from Yahoo! and a local ISP the personal subscriber information (including a real name and residential address) behind the account "stevedragonslayer."	**A reasonable expectation of privacy in your personal subscriber information held by your ISP?** No. The identifying information (including name, address, etc) was voluntarily transmitted to the third-party ISPs. The accused was also using peer-to-peer file sharing software on his computer, thereby giving anyone with internet access the ability to gain entrance to his computer. Subscriber information provided to an ISP is not protected by the Fourth Amendment's privacy expectation.
United States v. Borowy 595 F. 3d 1045 (9th Circuit Court of Appeals, 2010)	In 2007 an FBI special agent logged onto the LimeWire P2P service for routine monitoring of child pornography tracking. The agent identified several files on Borowy's computer that were known to contain child pornography. The agent subsequently downloaded the files from the P2P service and was able to confirm the illegal nature of the contents. Borowy claimed that he installed a version of LimeWire that prohibits other P2P users from downloading or viewing files on his computer. At the time, Borowy believed that this feature was engaged, therefore providing him with "a reasonable expectation of privacy in the files."	**Reasonable Expectation of Privacy?** The Appeals Court, based on precedent, noted in its opinion that an illegal government search is executed "only if it violates a reasonable expectation of privacy." The Court rejected Borowy's claim of privacy. Borowy's "subjective intention not to share his files did not create an objectively reasonable expectation of privacy in the face of such widespread public access." Absent this expectation, the Court ruled that the FBI's search for and downloading of the files on the P2P site did not violate the Fourth Amendment.

	The FBI determined no such feature was employed, and the FBI agent was able to download and view the files through the P2P service, which led to a subsequent search warrant for Borowy's home, including his laptop computer. This search uncovered better than 600 images of child porn, in addition to 75 videos.	
United States v. Ganoe 538 F.3d 1117 (9th Circuit Court of Appeals, 2008) *Cert. denied*, 129 S.Ct. 2037 (2009)	In January 2004 an Immigration and Customs Enforcement Special Agent was using LimeWire to locate persons trading in online child pornography. The agent accessed Ganoe's computer and observed a file depicting child pornography. Additional files were then downloaded which also constituted child pornography. The IP address on the computer was traced back to the offender's residence. A search warrant executed at his residence on his personal computer about two months later revealed more child pornography.	**Reasonable Expectation of Privacy?** The defendant's expectation of privacy in his personal computer could not "survive [his] decision to install and use file-sharing software, thereby opening his computer to anyone else with the same freely available program." "To argue that Ganoe lacked the technical savvy or good sense to configure LimeWire to prevent access to his pornography files is like saying that he did not know enough to close his drapes. Having failed to demonstrate an expectation of privacy that society is prepared to accept as reasonable…"
R. v. Caza 2012 BCSC 525	GigaTribe was a somewhat unique P2P network, as when one becomes a user one may only share or transfer information with people who have accepted them as a contact. If you have a GigaTribe account, and it is open, any of the users on our contact list, using their account, can see the things you are offering to share. One can	**Is a reasonable expectation of privacy present because GigaTribe users have a "contact" list?** The defence the police surreptitiously conducted a warrantless search of the suspect's computer. But the court held that a GigaTribe user has no reasonable expectation of privacy in the

	also send messages to one's contacts via GigaTribe. Users do not have to share personal information. They add each other as contacts not knowing who is truly behind the other account, or if it is shared or used by an individual alone. GigaTribe is typically utilized for sharing child pornography. Toronto Police used a Gigatribe account surreptitiously and sent messages to another account suspected of harbouring child pornography files. That account responded and later allowed the police officer to download child pornography files. Toronto police found the IP address of the computer associated to the suspect account. The ISP confirmed the residential address of the account as being in Kamloops, B.C – without a warrant. A search warrant was executed at a residence and a hard drive containing child pornography was located.	messages he sends to another user – they are akin to putting letters in the mail. It did not matter the accused thought he was sending the messages to a "contact" only, and not to anyone else (including the police). That was not a reasonable expectation of privacy. Once the messages were sent, the sender had given up all control over them. Furthermore, a user knows they cannot be assured of who lies behind the recipient's username. They choose to share with another user and assume any inherent risk. *There is a hope for, but no objectively realistic expectation of privacy.*

Wireless Networks

R. v. Spencer 2011 SKCA 144 (Sask. Court of Appeal)	In addition to the facts reviewed in the preceding section, it is important to note that Spencer accessed the internet via a wireless connection. His sister was the paid internet subscriber, although they both resided in the same household and his computer was located inside the residence.	**Reasonable Expectation of Privacy?** The Crown could not argue that Spencer had no reasonable privacy interests in his connection to the Wi-Fi network merely because the paid subscription agreement was in his sister's name. Both he and his sister resided in the home and both utilized the Wi-Fi network. *R. v. Edwards* [1996] 1 S.C.R. 128 does not "preclude an individual from challenging a search pursuant to s. 8 of the *Charter*" in such circumstances. Where "home Wi-Fi networks are commonplace, a reasonable and informed person concerned about the protection of privacy would not expect to surrender his or her privacy rights simply by reason that the internet service which they used in their own home was registered in another resident's name." However, Spencer could also not claim a higher expectation of privacy in this case simply because he did not personally sign the service agreement with the ISP. To allow one through "reckless disregard or wilfull blindness" to the terms of an internet service agreement to maintain a high privacy expectation would not be reasonable. Rather, Spencer, for the purposes of his privacy rights, was deemed to be a "derivate party" to

		the service agreement in question. A reasonable and informed person concerned about the protection of privacy would "expect to take the benefit of and to be required to comply with the terms of the agreement governing the provisions of those internet services."
United States v. Ahrndt (US District Court, District of Oregon) Fed. District Oregon, January 2010	In February 2007, an Oregon resident identified as JH was using her personal computer when it automatically picked up a nearby wireless network, to which she connected. JH began using Apple's iTunes software, which allows users to share media files such as digital photos and music over computer networks, and noticed that another user's files were available to her over the wireless network in a subdirectory entitled, "Dad's Limewire Tunes." After reading the names of some of these files, JH realized that they contained child pornography and contacted the authorities. Further police investigation revealed that the files indeed contained child pornography and that the network and the files were those of Ahrndt. Search warrants executed on Ahrndt's home and computer revealed child pornography.	**Reasonable Expectation of Privacy?** The District Court found that Ahrndt did not demonstrate a subjective expectation of privacy, and that even if he had, such an expectation was unreasonable because he had left his wireless network unencrypted and his iTunes settings openly shared his files with that network. The court noted Ahrndt was "using his iTunes software, and its preferences were set to actively share his music, movies, and pictures with anyone who had access to the same wireless network." The court further found that using iTunes to share files on an: "unsecured wireless network is not like a private conversation behind an unlocked door. Nor are files shared by LimeWire like an announcement in a public forum, because users do not actively send files to anyone. Rather, LimeWire users search each other's computers for files that interest them and, if one user finds a file of interest on another user's computer, they can . . . download the file. . . . When a person shares files on LimeWire, it is like leaving one's documents in a box marked

		`free’ on a busy city street. When a person shares files on iTunes over an unsecured wireless network, it is like leaving one's documents in a box marked `take a look’ at the end of a cul-de-sac. I conclude that iTunes' lesser reach and limit on file distribution does not render it unlike LimeWire in terms of its user's reasonable expectation of privacy.”

Social Networking Websites (Facebook, Twitter, etc.)

Leduc v. Roman 2009 CanLII 6838 (S.C.J.)	Justice Brown of the Ontario Superior Court of Justice reviewed a master's decision to deny a defendant's application for the production of the plaintiff's ostensibly private Facebook pages in a case involving injuries sustained in a car accident.	Justice Brown noted that "Canadian popular culture has embraced www.facebook.com" and that it was "beyond controversy" that a person's Facebook pages may contain relevant documents to litigation. Furthermore, this information should be accessible to all the relevant parties regardless of whether or not the profile was set with certain privacy settings in mind. The Court stated pithily that Facebook's primary purpose, as a social networking website, was to "enable people to share information about how they lead their social lives." To deny parties to litigation access to this information "risks depriving [them] of access to material that may be relevant to ensuring a fair trial."
R. v. Sonne 2012 ONSC 1741 (S.C.J.)	Sonne was arrested as part of the G20 protests in Toronto in 2010. He ultimately gave statements to the police. The defence challenged the admissibility of these statements during a blended *Charter* s. 10(b) / voluntariness *voir dire*.	**What can be inferred from "tweets'?** The evidence put forward by the Crown to demonstrate that Mr. Sonne was well aware of his legal rights prior to giving the statements included copies of documents that were obtained through links on Mr. Sonne's Twitter account. On June 21, he Tweeted "read EVERY PDF on this page and know your rights" and posted a link to "movementdefence.org", a website with materials created specifically for the G20,

		including a “Legal Guide for Activists” and a brochure entitled “What to do if the police come knockin’.” After reviewing these documents, Justice Spies found that the legal guide “is intended to provide the person who reads it with an overview of their rights when dealing with the police. It also deals with what a person should do if arrested by police. This includes asserting the right to silence.” While Mr. Sonne *did not testify* in regards to his understanding of these documents, Justice Spies concluded that *“it is reasonable to infer that Mr. Sonne had read these documents and was generally familiar with their contents.”* She further concluded that, combined with the fact that Mr. Sonne had actively challenged the police during his interrogation, it was reasonable to conclude that he had sufficient knowledge of his legal rights during one interrogation in particular.
R. v. Rafferty 2012 ONSC 742 (S.C.J.)	The Crown obtained a “Neoprint printout” of the Facebook profile of the accused (from the corporate HQ of Facebook in California). On April 8, 2009, at 10:01 am EST, Rafferty posted a status updated as “everything good is comming my way.” The victim disappeared later that same day.	**Relevant? Probative vs Prejudicial?** The posting is circumstantial evidence of the state of mind of the accused and is highly relevant evidence. The message posted represented the entire thought that Rafferty wished to convey at that point in time. There is no missing context.

	The defence argued without the proper context surrounding the message it was more prejudicial than probative and thus should be excluded.	
U.S. v. Meregildo 11 Cr. 576 United States District Court Southern District of New York August 10, 2012	Federal prosecutors obtained a warrant to search the contents of the accused's Facebook account. The information to obtain the warrant was based on a "friend" of the accused's voluntarily giving access to the accused's Facebook page to the FBI. The accused challenged the legitimacy of this tactic on the basis that he held a reasonable expectation of privacy in his Facebook content and that his "friend" could not simply hand this over the FBI to be used against him in a criminal investigation.	**Reasonable online expectations of privacy?** The Court held: "Facebook-and social media generally-present novel questions regarding their users' expectations of privacy. Facebook users may decide to keep their profiles completely private, share them only with "friends" or more expansively with "friends of friends," or disseminate them to the public at large. Whether the Fourth Amendment precludes the Government from viewing a Facebook user's profile absent a showing of probable cause depends, inter alia, on the user's privacy settings. When a social media user disseminates his postings and information to the public, they are not protected by the Fourth Amendment. However, postings using more secure privacy settings reflect the user's intent to preserve information as private and may be constitutionally protected. The Government viewed Colon's Facebook profile through the Facebook account of one of Colon's "friends" who was a cooperating witness…. *Where Facebook privacy settings allow*

		viewership of postings by "friends", the Government may access them through a cooperating witness who is a "friend" without violating the Fourth Amendment… Colon's legitimate expectation of privacy ended when he disseminated posts to his "friends" because those "friends" were free to use the information however they wanted-including sharing it with the Government.

Evolving Societal Expectations of Privacy?

United States v. Jones 565 U.S. _____ (2012); 132 S. Ct. 945 (Supreme Court of the United States, 2012)	In 2004, a joint FBI and Metropolitan Police Department task force began investigating Jones and Maynard for narcotics violations. During the course of the investigation a Global positioning system (GPS) device was installed on Jones's Jeep Grand Cherokee without a valid warrant. This device tracked his movements 24 hours a day for four weeks. The GPS data was crucial to securing Jones' convictions.	**A Reasonable Expectation of Privacy?** The government said Federal Bureau of Investigation agents use GPS tracking devices in thousands of investigations each year. It argued that attaching the tiny tracking device to a car's undercarriage was too trivial a violation of property rights to matter, and that no one who drove in public streets could expect his movements to go unmonitored. Police were free to employ the tactic for any reason without showing probable cause to a magistrate and getting a search warrant. The Supreme Court ruled unanimously that police erred by not obtaining an extended search warrant before attaching a tracking device to Jones' car. But the justices split 5-4 on the reasoning. **Alito J. (Dissent):** The Fourth Amendment protects a reasonable person's "well-developed and stable set of privacy expectations. But *technology can change those expectations.…* *Short-term* monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable… But the use of *longer-term GPS monitoring.…* impinges on expectations of privacy." **Sotomayor J.'s Concurring Opinion:** While agreeing with the majority's approach, the

		following observations were made: "Technological advances… will also affect the *Katz* test by shaping the *evolution of societal privacy expectations*." "Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity if susceptible to abuse." Certain technologies – such as GPS tracking – may "[a]lter the relationship between citizen and government in a way that is inimical to democratic society." **On Disclosure to Third Parties:** "More fundamentally, it may be necessary to *reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties*. This approach is ill-suited to the digital age."
R.v. Telus Communications Co. 2013 SCC 16	The Supreme Court addressed whether a general warrant, or a Part VI authorization, was necessary for state agents to seize the prospective daily production of text messages.	**Does technology changes our societal expectations of what constitutes reasonable privacy?** Citing the earlier case of *R. v. Wong*, Abella J. held that "the broad and general right to be secure from unreasonable search and seizure guaranteed by s. 8 [of the *Charter*] is meant to keep pace with technological development[.]"

American Civil Liberties Union of Illinois v. Alvarez Seventh Circuit Court of Appeals May 8, 2012 Case No. 11-1286	Illinois had an "eavesdropping" law that prohibited the recording of any conversation between two or more parties – in any setting, even a public one – without all party consent. In certain circumstances, violating this law could result in a mandatory minimum of four years' incarceration. The ACLU brought an application to have an injunction issued against enforcement of the law. They wanted to set up a "police accountability program" which included a plan to openly make audio-visual recordings of police officers performing their duties in public places and speaking at a volume audible to bystanders.	**The law violates the 1st Amendment:** Audio and audiovisual recording are media of expression commonly used for the preservation and dissemination of information and ideas and thus are "included within the free speech and free press guarantee of the First and Fourteenth Amendments." The act of making an audio or audiovisual recording is necessarily included within the First Amendment's guarantee of speech and press rights. **On the importance of audio and audiovisual recordings in a free society – *when utilized by civilians*:** Audio and audiovisual recording are uniquely reliable and powerful methods of preserving and disseminating news and information about events that occur in public. Their self-authenticating character makes it highly unlikely that other methods could be considered reasonably adequate substitutes. As the ACLU is proposing to record *openly* – that is, to effectively provide notice to the affected parties – and only those conversations that are not private, its proposed "police accountability program" is entitled to First Amendment protection. **Commentary:** *I have included this case because it puts the traditional analysis of audiovisual recording in criminal cases on its head – here, it is the state trying to prevent the*

		recording of its agents, by civilians, rather than a civilian attempting to block the state from recording him or her. The analysis is thus very different. How one views state agents recording citizens in public versus how one views civilians recording state agents' actions in public is at the core of the analysis. Society has different expectations depending on who holds the camera/microphone, and why.