14th BILETA Conference: "CYBERSPACE 1999: Crime, Criminal Justice and the Internet".

Monday, March 29th & Tuesday, March 30th, 1999.
College of Ripon & York St. John, York, England.

E-mail, The Police, and the Canadian Charter of Rights and Freedoms: Retooling Our Understanding of a Reasonable Expectation Privacy in the Cyberage

Introduction

The phenomenon of cyberspace, and its medium the Internet, recently have generated an abundance of debate in legal literature. Much of this debate has been an attempt to answer the question of whether the traditional legal doctrine is capable of dealing with the legal issues posed by this new communications medium. One area in which this debate has moved from the law school lecture hall and into the courtroom is in the area of search and seizure law. Specifically, when issues of unreasonable police searches have arisen regarding personal e-mail, the Court has been required to determine whether personal e-mail falls within the jurisdiction's understanding of what constitutes a search. In *R* v. *Weir,* the Alberta Court of Queen's Bench brought this issue forward within the context of s.8 of the *Canadian Charter of Rights and Freedoms.* It is my position that in the Court in *R* v. *Weir,* showed that traditional legal doctrine has the ability to adapt to the new medium. In determining the standard of reasonableness, however, the Court in *Weir* inappropriately applied an assumption of risk analysis in its attempt to understand the level of privacy that Canadian society affords e-mail communications.

This paper is separated into four parts. Part I lays out the facts, the Court's conclusions regarding privacy in e-mail and the risk analysis doctrine that was applied. Part II contains an analysis of general principles dealing with section 8 of the *Canadian Charter of Rights and Freedoms.* This includes a discussion of the analysis stipulated by the Supreme Court of Canada in *Hunter* v. *Southam Inc*as well as its rejection of the American assumption of risk analysis in *Duarte* v. *The Queen.* Part III will look at the decision in *Weir* in relation to the *Charter* principles advocated by the Supreme Court of Canada. Part IV will argue that the test in *Duarte* is more indicative of Canadian society's expectation of privacy in interests such as personal e-mail than is the application of the risk assumption analysis followed by the Court in *Weir.*

Part I

a) The Facts of R v. *Weir*

On June 22, 1996, a third party (hereinafter "sender") using the Internet e-mail address christed@connect.ab.ca sent an e-mail message to the defendant's personal e-mail account at dtweir@supernet.ab.ca.. This e-mail included several digital photographs, graphic images and movie attachments (jpg, gif, and avi respectively). After the defendant attempted to access his e-mail by dialing up the mailbox account at his Internet Service Provider (ISP), the defendant became aware that his mailbox file was inaccessible to him. This inaccessibility was do to the sender's large

attachment overloading the defendant's account.

At the request of the defendant, the ISP attempted to repair the overloaded mailbox file. One of the ISP's repair technicians, in the regular course of his work, noticed the contents of the attachment. The ISP found several pictures and videos that were believed to be depicting child pornography. The ISP then informed the Edmonton police and copied the material. On police instruction, the ISP allowed the material to be accessed by the accused without informing him that the police were aware of the mailbox file's contents.

Using the copy of the material provided by the ISP, the police obtained a warrant pursuant to s. 487 (1) to search the dwelling place of the accused. Although he was not present during the search, the accused spoke with the police from work and provided information about the files. The police seized the contents of the defendant's CPU along with a diskette with 190 computer files alleged to contain child pornography. The defendant was subsequently charged with one count of possessing child pornography contrary to s.163.1 (4) of the *Criminal Code.*

b) The Decision in R v. Weir.

At trial, the defence urged the Court to rule that the act of transferring a copy of the sender's attachments from the ISP to the police amounted to an unwarranted, and therefore, unreasonable seizure of Mr. Weir's e-mail. As this information was used by the police in its s.487 (1) warrant application, the defence argued that the evidence obtained from the diskette at the defendant's dwelling place should be excluded on the basis that it was obtained with a tainted warrant. The Court held that in viewing and transferring the mailbox contents to the police, the ISP had acted as an informant. Such an act did not amount to a search within the meaning of section 8 of the *Charter.* The approach and method of the Court's conclusions in this regard were neither novel nor interesting. What is of interest, however, is that for the first time in Canada, the Court, in *dicta*,looked at whether personal e-mail would afford protection pursuant to section 8 of the *Charter,* and in what context that protection be viewed in relation to other traditional communication mediums.

c) Reasonable Expectation of Privacy in E-mail

To determine whether section 8 of the *Charter* protected the defendant from the pre-warrant search of his e-mail, the Court was required first to turn its mind to whether personal e-mail carried a reasonable expectation of privacy. In making its decision on this issue, the Court looked at both the expert testimony at trial, as well as the American decision of *United States* v. *Maxwell.*

In *Maxwell,* the United States Air Force Court of Criminal Appeals (AFCCA) discussed the reasonable expectation of privacy in e-mail. Similar to the case before the Court in *Weir,* the AFCCA was faced with the issue of whether the defendant's personal e-mail was protected against unwarranted search and seizure by the Fourth Amendment. The only significant difference between *Maxwell* and *Weir* was that the defendant in *Maxwell* was sending his personal e-mail within the private America Online network system and not through a regular ISP.

In its decision, the AFCCA looked at the nature of e-mail to determine whether personal e-mail was covered by the Fourth Amendment. To determine if a reasonable expectation of privacy existed in e-mail the Court relied in part on the assumption of risk analysis set out by the U.S. Supreme Court. Pursuant to this doctrine, a person's reasonable expectation of privacy is affected directly the degree of risk that the alleged privacy interest would be disclosed to parties outside the confidential communication. The Court, after reviewing the evidence of the e-mail medium, limited the reasonable expectation of privacy in personal e-mail to situations in which the sender and receiver of the e-mail had exclusive access to the messages by way of a password and there was minimal o risk that the transmissions could be received by anyone other than the intended recipient(s). As such the

decision in *Maxwell,* by implication, did not create a reasonable expectation of privacy in e-mail during transmission over the Internet. Rather, the *Maxwell* decision is limited intentionally to the context of private, contained network systems such as America Online.

In *Weir,* the Court agreed with the conclusions leading up to the decision in *Maxwell.* The Court concluded that in 1996, unencrypted e-mail transferred over the Internet held a considerable risk of interception by both the defendant's ISP and outside third parties such as hackers or other Internet nodes along the transfer route. Further, unlike the Canada Post Corporation, ISPs in Canada are not regulated by statute. It could not be said, therefore, that there was any legislative implication that personal e-mail held a reasonable expectation of privacy in the same way as 1st class mail. On the other hand, the Court was mindful of the *Maxwell* finding that an expectation of privacy did exist in e-mail files stored within the AOL environment. The expert witnesses also confirmed that they themselves believed that their e-mail communications over the Internet would carry at least a limited level of privacy.

In agreeing with the experts' expectations as well as what it thought was the decision in *Maxwell,* the Court in *Weir* concluded that personal e-mail transmitted over the Internet held a reasonable expectation of privacy. In reality, however, the decision in *Weir* went further than the *Maxwell* decision, and expanded search and seizure protection in e-mail from exclusive networks such as AOL to the more easily accessible e-mail communications stored in regular ISPs and transferred over the Internet. It is unclear, however, whether the Court in *Weir* knew that it had expanded a reasonable expectation of privacy in e-mail beyond what the *Maxwell* decision had contemplated.

d) The Level of Privacy in E-mail - Less than First Class Mail

Unlike the court in *Maxwell*, the Court in *Weir* went on to discuss the standard of privacy that should be afforded to e-mail in relation to the already protected forms of communication. It entered into a standard of privacy analysis. The Court first looked at the academic debate surrounding the nature of personal e-mail communications. In following the analysis of Megan Connor Berton's article on privacy in personal e-mail, the Court conceded that there are significant similarities between the nature of first class mail communications and the much newer medium of personal e-mail communications. First, the Court determined that personal e-mail is very similar to first class mail within a content analysis. Further, both are relatively inexpensive forms of asynchronous communications. On close inspection, however, the analogy with first class mail broke down when the technologies of the two forms of communication were compared. Rather, the method of transmission of personal e-mail was more analogous with other forms of telecommunications, such as telephone communications. In the end, the Court's focus with regard to the nature of e-mail moved away from the content analogies of the highly protected first class mail. Instead, the Court subsumed the standard of privacy analysis within the assumption of risk analysis that it had used earlier.

In adopting the technology analogy over the content analogy, the Court applied the former within the assumption of risk analysis mentioned earlier. Specifically, the Court looked at the susceptibility of unencrypted e-mail messages to interception when transferred over the Internet. Further, unlike traditional mail, the technological nature of e-mail often requires that confidentiality be sacrificed when technical "glitches" are repaired by ISPs. These two factors led the Court to hold that the manner in which the e-mail technology is presently managed, the way in which the mailbox files are repaired by ISP's, and the relatively low degree of security present in unencrypted e-mail transmissions, combine to create a lower level of privacy than that of first class mail. As such, it was the Court's opinion that the *Criminal Code* general search warrants as well as the more intrusive wiretap warrants were reasonable authorizations within the context of seizing a person's e-mail. As will be seen below, however, the adoption of an assumption of risk analysis to reach this conclusion is not the proper analysis in light of the Supreme Court of Canada's decision in *Duarte* v. *The Queen.*

Part II

Canadian Case Law. -General Principles

Everyone in Canada has the right to be secure against unreasonable search and seizure pursuant to section 8 of the *Canadian Charter of Rights and Freedoms.* As part of the Canadian Constitution, the *Charter* proclaims the legal principles with which all state actions must comply. Within the analysis of section 8, the Supreme Court of Canada has established two specific questions that must be looked at in cases where an unreasonable search is at issue. From the Court's rulings in the seminal decision of *Hunter* v. *Southam,* these two questions can be articulated as follows:

1. Did the actions of the state constitute a Search within the meaning of section 8 of the *Charter?;* and
2. Was the State search reasonable?

As will be seen below, the Court's answers to these two questions have created an approach unique to Canada for protecting the interests of people from unreasonable search and seizure.

a) What Constitutes a Search

Similar to the position of the American Supreme Court on the Fourth Amendment, the Supreme Court of Canada in *Hunter* concluded, that section 8 of the *Charter* protects people, not property. The Court held that the defining nature of "search and seizure" protection was *not* based on the right to be free from unauthorized trespass to property. Rather the organizing principle of section 8 was that the state must not interfere with a person's reasonable expectation of privacy. In abandoning the legacy left by the landmark decision of *Entick* v. *Carrington,* the *Hunter* decision brought many privacy interests which would have failed under the traditional common law property analysis within section 8 of the *Charter*. In the years that have followed the Court's decision in *Hunter*, Canadian Courts have held that a search may occur where the police: take aerial photographs of a person's estate; commit surreptitious video surveillance of an illegal gambler's hotel room;seize personal commercial information; or intercept private cellular telephone communications. All of these constitute a search without the defendant holding a property right in the privacy interest.

The Supreme Court of Canada's early decisions seemed to indicate that it would adopt the two-part American test to determine whether a person holds a reasonable expectation of privacy. This approach requires both an objective and subjective expectation of privacy before the Court will attach Fourth Amendment protection will attach. In *R* v. *Wong,* however, the Supreme Court of Canada indicated that the analysis under section 8 of the *Charter* was not concerned with an individual's subjective expectation of privacy but rather with society's interest of being free from over-intrusive police investigations without prior judicial authorization. The proper test for the Court, therefore, is to determine objectively whether the reasonable person would expect that the investigative technique in question interfered with the particular personal privacy interest to such an extent that it would only be available with some form of judicial pre-authorization. As one academic points out, the rejection of the subjective requirement under the American test will lead Canadian courts to label police investigative techniques as a search in more circumstances than our neighbors to the South.

Along with its rejection of the two-part American test, the Supreme Court of Canada also rejected the use of the American assumption of risk analysis to determine if a defendant holds a reasonable expectation of privacy. Under an assumption of risk analysis, the defendant's reasonable expectation of privacy is determined by looking at the precautions taken by the defendant to ward off any probable interception or discovery of the privacy interest by an outside party. In following this analysis, the post-*Katz* decisions of the United States Supreme Court indicate that it is reluctant to hold that a reasonable expectation of privacy exists where the lawful use of technologically advanced

instruments creates a probable risk of the privacy interest being intercepted regardless of the reasonable efforts of the defendant.

The Supreme Court of Canada faced similar question in *Duarte.* Here, the Court rejected the argument that a risk of interception played a role in determining whether a search had occurred under section 8 of the *Charter.* In this case, the Crown argued that, as the defendant's words were communicated to an informant, the defendant's expectation of privacy in the communication was eliminated because he had subjected himself to the risk of the communications being relayed to the police. Any police recording of the communication with the consent of the informant, therefore, would not amount to a search within the meaning of section 8 of the *Charter.* The Court quickly rejected this assumption of risk analysis, stating that an adherence to this American approach would, if taken to its logical conclusion, destroy all expectations of privacy. The determination of whether a search had occurred, did not relate to the probable risk of disclosure of the communication. The proper question to ask is whether the person had reasonable grounds to believe that his privacy interest would be intercepted by the state without his consent or prior judicial authorisation.

In light of the transfer of information between the ISP and the Edmonton police in *Weir,* it is important to note that the Supreme Court of Canada has indicated a distinct test for analysing questions of informational searches. In *R* v. *Plant,* the Court was faced with a situation in which the police, by special arrangement, had acquired online computer access to the local hydro company's computer records. Through this access, the police gathered information regarding the electrical consumption of a suspected hydroponic marijuana grower. On appeal to the Supreme Court of Canada, the defendant argued that he held a reasonable expectation of privacy in the information regarding his hydro consumption. After enunciating five factors to determine the nature of the information obtained by the police, the Court determined that section 8 of the *Charter* would protect confidential information that would tend to reveal intimate details of the lifestyle and personal choices of the individual. The majority of the Court held that such information did not go to the biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state. In the aftermath of this decision, there has been little explanation by the Court of what would go to the biographical core of personal confidential information. In the case of personal e-mail, however, it has yet to be determined whether information held by an ISP about a person's e-mail accounts could be requested by the police without triggering section 8 *Charter* protection.

b) Was the Search Reasonable?

After reaching the conclusion that a reasonable expectation of privacy exists, the next step is to balance the State's need to intrude on the privacy interest. In other words, is the search itself reasonable? In *R* v. *Collins,* the Supreme Court of Canada indicated that a search will be reasonable if it is authorized by law, if the law itself is reasonable, and if the manner in which the search was carried out is reasonable. In the criminal context, warrantless searches in Canada have been held to be presumptively unreasonable. To overcome this presumption, the Crown must show that, within the context of the privacy interest, the unwarranted search was otherwise authorized by law, and that the search was conducted in a reasonable manner.

c) Searches and Seizures Authorised by Law

Though the Court has recognized limited common law authorizations for a warrantless search, in most circumstances the Court will require prior judicial authorization where such a mechanism has been created by Parliament. In 1997, Parliament passed s. 487(2.1) of the *Criminal Code,* giving police engaged in a criminal investigation the power to search and seize data found on a computer system. With the inclusion of s. 487(2.1), both the intercept warrant and the traditional search warrant are now applicable to the Internet e-mail environment. As a form of telecommunications, the e-mail transmissions are subject to modern day wiretap interceptions authorized in Part VI of the

Criminal Code. As a form of data, these communications may also be seized by the state. At present there has been no case dealing with the use of a Part VI intercept warrant in relation to Internet communications. As the police grow more certain of how crimes through this medium are being committed however, it is likely that the intercept warrant will become a valuable tool in police investigations.

The intercept warrant authorizations of Part VI and the traditional search warrants of Part VX of the *Criminal Code* authorize different degrees of privacy invasion. Though both warrants require that the State has reasonable grounds that the interception or search will provide evidence of a serious crime, in most cases an intercept warrant will intrude to a greater degree, as it is, by nature, over inclusive in its application. The stricter requirements of the intercept warrants within Part IV the *Criminal Code* indicate that Parliament understands the over-intrusive nature of the wiretap warrant. They created an onerous test for the police to overcome before judicial authorization will be granted. In theory, therefore, a person's e-mail transmissions will be protected by the strict judicial authorization requirement.

A *caveat* should be stated in relation to the onerous provisions created to protect against the more intrusive nature of the wiretap warrant. At present it remains open to discussion whether the courts have shown proper care in monitoring the use of the wiretap warrant by police. For example, between 1991 and 1995 the Attorney General of Canada applied for over 1000 normal audio intercept warrants pursuant to section 185(1) of the *Criminal Code* (see Table 1.). Not a single one of these applications was refused by the courts. It is conceded that a *Parsons* application may be brought at trial to challenge the sufficiency of the warrant's supporting Information. This does not, however, reduce the fact that at present the police are able to obtain the intercept warrant with little of the judicial governance that was contemplated in *Hunter*.

In Canada, a search will be reasonable if it is authorized either at common law or by statute. In the context the Court's decision in *Weir* there are two relevant computer-related common law warrantless search powers. These are the common law authorizations of third party

Table 1

The Number of Authorizations/ Renewals Granted

Type of Application Granted	**Year**				
	1991	**1992**	**1993**	**1994**	**1995**
Normal Audio s.185(1) *C.C.*	291	225	236	217	213
Normal Video s.487.01 (1) *C.C.*			1	16	25
Emergency Audio	7	2	2	1	1

s.188(1) *C.C.*					
Emergency Video **s.487.01(1) *C.C.***	0	0	0	0	0
Renewals **s.186(6) *C.C.***	11	6	2	2	7
Total Applications Granted	309	233	241	236	246

Table 2

The Number of Applications For

Authorizations/Renewals Refused

Type of Application	Year				
	1991	1992	1993	1994	1995
Normal Audio **s.185(1) *C.C.***	0	0	0	0	0
Normal Video **s.487.01 (1) *C.C.***	0	0	0	0	0
Emergency Audio **s.188(1) *C.C.***	0	0	0	0	0
Emergency Video **s.487.01(1) *C.C.***	0	0	0	0	0
Renewals **s.186(6) *C.C.***	0	0	0	0	0
Total Applications Refused	0	0	0	0	0

consent and the Open Field doctrine. Each of these may cause future problems in future analyses of whether a search is reasonable in the context of personal e-mail.

Third party consent will only be valid if it can be reasonably viewed as a substitute for prior judicial authorization. The fact that the third party can remove the traditional barrier of property trespass, therefore, will not likely suffice to make the search reasonable without a more substantial factor. In the context of the current trend of ISPs willingly providing to the police with evidence of illicit activity stored on their systems, the consent of the ISP may not be enough without some other support. Such support could include a user agreement by which it can be consented that the user himself was consenting to the material being disclosed to the police. The Court in *Weir* did not address this issue.

The Open Fields doctrine was established as part of Canadian law by the Supreme Court of Canada in *R* v. *Boersma.* This doctrine indicates that, if the privacy interest is in the plain sight of the police and within the public purview, the accused cannot claim that he had a reasonable expectation of privacy in the thing being searched or seized. In *R* v. *Morin,* the Court concluded that the police action of logging onto a BBS located at the accused's home was within the public purview, therefore nullifying any concept of a reasonable expectation of privacy in its contents. Though no case in Canada has yet addressed this issue with regard to personal e-mail transmitted over the Internet, it is possible that the interception of e-mail transmissions via an Internet node may not require an intercept warrant.

In balancing the privacy interests of the individual with the state's need to investigate criminal activity, Canadian Courts have often used the traditional tools of analogy in circumstances where the reasonableness of a non-warrant lawful authorization is in question. As such most newly-argued privacy interests, such as personal e-mail communications, have been looked at in comparison with existing privacy interests. It seems clear from the academic and foreign case law analyses that e-mail has many characteristics that make it analogous to first class mail. In light of this and the comparison of personal e-mail with first class mail in *Weir* the law dealing with first class mail must be determined.

In looking contextually at the reasonable expectation of privacy in 1st class mail, the law of Canada has afforded high levels of privacy to this form of communication The Newfoundland District Court's decision in *R. v. Crane* best enunciates this point. Evidence was adduced that the police had searched the defendant's mail with the help of Canada Post and without a warrant. In holding that both co-defendants' section 8 *Charter* rights have been violated, the Court discussed the long-standing principle that privacy in one's first class mail was an important and highly-protected element of Canadian society. In reaching this conclusion, the Court found that the privacy interest in first class mail is established by the *Canada Post Corporations Act.* The Court held that within the *CPCA* Parliament implicitly states an intention to promote the security of one's mail beyond that which would exist at common law.

Interestingly, in light of the technology argument put forward by the Court in *Weir,* the decision in *Crane* does not look at the susceptibility of the technology used to keep 1st class mail confidential. Rather, the Court reached its conclusion by looking at Parliament's prohibitions against state interception of first class mail. The Court held that such prohibitions indicated an intention to protect the privacy of mail communications absent a judicial warrant. Though no Canadian case has enunciated the principle, it appears that because of the obvious temptation to read the mail of suspected citizens, sealed, private letters are afforded special protection from search and seizure. Looking at personal e-mail communications in the context of the privacy rights afforded first class mail without advocating a similar legislative pronouncement on privacy in e-mail, therefore, is not a proper strategy. At present, no such pronouncement by Parliament exists in Canada.

Part III

The decision in *Weir* indicates that Canadian courts are willing to afford privacy to e-mail communications made in cyberspace. Further, the Court's conclusions, in *dicta*, indicates that the

traditional legal doctrine is capable of accommodating privacy interests in this new medium. As in most cases, however, the problem is not usually the ability of the legal framework to deal with a new issue but rather how the legal framework is used in reaching the court's conclusions. This is what happened in *Weir.*

Though the Court correctly followed the principle of whether a reasonable expectation of privacy existed in personal e-mail, it erred in the application of the test to establish the standard of privacy within personal e-mail. This is most apparent in the Court's use of an assumption of risk analysis and the application of technology's role in constructing the level of privacy in personal e-mail. In particular, when the Court inquired whether encryption programs could better protect a person's expectation of privacy in personal e-mail, it incorrectly addressed the question that was to be answered under the section 8 analysis. As was indicated in *Duarte,* the question of whether it is a reasonable conclusion that a third party could intercept personal e-mail communications is not congruent with the principles of section 8 of the *Charter.* Rather, the question is whether the reasonable person would believe that the police could make the interception without prior judicial authorization. This question was neither asked nor answered within the analysis of *Weir*.

The Court's failure to understand the way in which society perceives the security risks in e-mail will, if followed, erode the privacy rights of persons suspected of unlawful conduct. By ruling that the *Criminal Code* intercept warrant authorizations apply to private e-mail communications,the Court has sanctioned an incredibly wide and intrusive means by which the police can compile information against a suspect. Think of the varied number of communications that the typical e-mail user gets in one day. In comparison with first class mail communications, the totality of the personal e-mail communications would be caught within the intercept warrant. At present, however, the conclusion in *Weir* is likely to be followed by future court as the contextual comparison with first class mail is non-determinative. Unlike e-mail, the privacy afforded to first class mail in Canada is a construction of Parliament. Any equal protection of personal e-mail in this regard will have to come by way of legislation. Until that time the Court will be hard pressed to hold that personal e-mail communications carry a greater protection than is presently afforded to telephone communications.

An important area not required to be answered on the facts in *Weir* was what role the decision in *Plant* will play regarding the actions of police agents actively seeking information from ISP's regarding suspects. It remains uncertain, however, whether information relayed by an ISP to the police contains confidential information. In future cases, the Court will have to determine the issue of whether it is willing to allow close relationships between the ISP carrier and the police. As is argued by Scott Hutchinson in *Computer Crime in Canada,* a court's decision on this issue likely will depend on whether it can be shown that the contract between the defendant and the ISP indicated any confidential arrangement. On the construction of many new ISP agreements it seems that the contracts do not contain any such agreement.

Though it is agreed that the Court properly extended the reasonable expectation of privacy in personal e-mail during Internet transmissions, it is uncertain how these issues will be brought forward in future criminal proceedings. As with the comments in the last paragraph, the facts in *Weir* did not lend themselves to an in depth analysis in this area. It is likely, however, that future decisions will be argued within the context of the Open Fields doctrine and Third party consent. Under both concepts the level of privacy in *Weir* may be drastically reduced. In these cases, however, the Court must be aware that the exceptions to warrantless searches being presumptively unreasonable must be determined within the overall principles of section 8. As such, the decision in *Weir* and the Court's statements in *Duarte* must be looked at to shape any further rulings in this area.

In concluding that the defendant in *Weir* held a reasonable expectation of privacy in e-mail, the Court followed the existing principles as set out in *Hunter.* The application of these principles, however, was not congruent with the Court's decision in *Duarte.* Rather, the approach taken by the Court was one that, while correct in result with regard to the applicability of both the Part VI

intercept warrant and Part XV general search warrant authorizations, is troublesome in the level of privacy it erodes. Further, though the facts of *Weir* did not provide the proper forum in which to address other issues regarding search and seizure, it has opened up the dialogue in which these issues may be addressed. Specifically, it likely will come to bear that informational privacy, the open field doctrine, and third party consent will be considered in light of the *Weir* decision. Any problems, such as the Court's application of the assumption of risk analysis, could be resolved if the courts approach the traditional method of analogy along formal content constructions and not along parallels in technology. This will result if the Canadian Courts are careful not to follow the analysis in *Weir* and instead follow the path set out by the Supreme Court of Canada in *Duarte.*

Part IV

The decision in *Weir* creates an interesting dilemma for persons who wish to use e-mail for personal communications. If they want to keep their private and personal e-mail communications private to the same extent as their first class mail they must use an encryption system to do so. At present, e-mail encryption systems are bulky, inherently complicated, and difficult to use. They sabotage the very incentive that has drawn people to use the e-mail communications medium. In effect, encryption systems hinder the user-friendly environment and slow the medium's ability to send quick asynchronous communications. Technology, it seems, is the advantage of the communication medium, while being at the same time the bane of privacy in personal e-mail communications. The purpose of the discussion here is to argue that the Court in *Weir* failed to understand that e-mail communications in cyberspace are redefining the role of technology in our understanding of what is a reasonable expectation of privacy in Canadian society. The Court failed to understand the relationship between section 8 rights and the other rights enshrined in the *Charter.*

The application of the assumption of risk analysis, to determine the reasonable expectation of privacy in Internet communications is rejected by a growing number of legal academics. They argue that technological security in a privacy interest does not relate directly to the expectation of privacy within the cyberspace environment. Unlike traditional forms of communications, e-mail often defies the correlation between the actual susceptibility of risk in a medium's technology and our understanding of privacy in our use of that medium. Rather the reasonable person in the cyberage links privacy in e-mail transmitted over the Internet with the socially-constructed risk of having the communication brought into the public forum. In applying this perception to the e-mail environment, people may understand how to use e-mail, but at present at least, most do not fully understand how e-mail works on a mechanical level. It is unlikely, therefore, that people understand the actual technical security risks of unencrypted e-mail as well as they relate to the socially constructed risks. If this is the case, then the courts may be affording a level of privacy in personal e-mail that does not mirror our current need or expectations of privacy in the medium.

By accepting the assumption of risk analysis in determining the level of constitutional protection of a particular privacy interest, the courts will create a fixed zone of privacy under the *Charter.* As people move from traditional forms of protected communication to newer forms of computer-driven communication systems, however, the content of the communication faced an increased risk of interception by third parties. As Frederick Schauer comments, the technology of the Internet is analogous to a device that would enable a passerby to look through the seemingly solid walls of a dwelling place. Subject to legislation, the risk assumption analysis would reduce the reasonable expectation of privacy in the house. It might seem inconceivable that the courts would allow such a reduction in privacy in one's dwelling place. But this is exactly what will result if the Court uses the assumption of risk analysis to reduce the level of privacy in e-mail from that afforded to communications that are less susceptible to technological surveillance.

In the communications environment the reasonable expectation of privacy secured by section 8 often is a mechanism for protecting a person's Constitutional protected freedom of expression. Within the context of the argument made above, it must be considered that the level of privacy afforded to

personal e-mail will affect not our right to control the public dissemination of personal information, but also the right to express our views without fear of having them used against us. Any reduction of privacy protection under the assumption of risk analysis will, therefore, effect our right to communicate within a free and democratic society. In *Weir,* we see the possibility that the low level of privacy in personal e-mail could erode not only our section 8 *Charter* protection, but also our section 2(b) freedom of speech protection. The *Duarte* test, however, is far less limiting to the court's ability to protect our freedom of expression in the context of unreasonable search and seizure. Asking whether the reasonable person would concede to such state interference without a warrant is a superior means of ensuring the protection *Charter* rights than the assumption of risk analysis.

If our understanding of technology in e-mail is based on socially-constructed lines that are not linked to the actual risk of third party interception, then the rejection of the risk analysis doctrine by the Supreme Court of Canada in *Duarte* is of great significance. By accepting that section 8 of the *Charter* protects a person's ability to decide *when* and *how* private information shall be disclosed to the public, the Court rejects a determinative mechanism that does not correlate to our perceived understanding of risk within cyberspace. This is not the approach adopted in *Weir.* It is the approach, however, that will best protect privacy rights in e-mail in Canada. It is likely that future Canadian decisions will afford a more accurate representation of *Charter* principles if they limit the application of technology within the analysis of the level of section 8 protection to be afforded to personal e-mail.