

PERSONAL RELATIONSHIPS OF
DEPENDENCE AND INTERDEPENDENCE IN
LAW:

CHAPTER 4: PERSONAL RELATIONSHIPS IN THE
YEAR 2000: ME AND MY ISP

IAN KERR

THE GATEKEEPERS

Aquacool_2000 loves to talk business. Unfortunately, not everything that he says is golden. For example, in reference to three members of the management team of a publicly traded corporation known as AnswerThink Consulting Group Inc., Aquacool_2000 stated the following: "One of them is an arrested adolescent whose favourite word is 'turd.' One is so dull that a 5-watt bulb gives him a run for his money. And the third believes that the faster you go in your car, the smarter you get." These remarks were never spoken. But they were posted to an online message board available to all 125 million subscribers of Yahoo!, perhaps the largest portal on the World Wide Web.¹ Recognizing that its advertising revenue and stock valuations rest mainly in the invisible hand of corporate America, Yahoo! had invited its subscribers to "discuss the future prospects of the company and share information about it with others."² In fact, Yahoo! had set up similar message boards for every publicly traded corporation listed on the New York exchange.

Clearly, Yahoo! had envisioned a frank exchange of information on its message boards. One might even say that Yahoo! had abetted such exchanges. By constructing an architecture that encouraged message board participants to select a nom de plume and thereby communicate pseudonymously, Yahoo! ensured an online discussion that has been described as "colloquial in tone, opinionated, speculative, and frequently caustic and derogatory."³

As the story goes — and as one might imagine — AnswerThink did not think too highly of Aquacool_2000's remarks and answered with a threat of legal action. Capitulating to the pressure exerted by AnswerThink, Yahoo! decided to disclose personal information about Aquacool_2000⁴ without even telling him that it had done so. Had Yahoo! notified Aquacool_2000 of its decision to disclose the requested information to

AnswerThink, he would have had the opportunity to seek a protective order to enforce his constitutionally protected right to speak anonymously.⁵ His inability to do so resulted not only in a (potentially frivolous) defamation suit against him, it also resulted in the immediate termination of his employment. As it turns out, Aquacool_2000 was an AnswerThink employee.

Before proceeding further, it is important to have a sense of the means by which Internet service providers collect personal information about people like you, me, and Aquacool_2000. There are a number of ways for a service provider to collect such information. First, it can ask users to fill out an information form. Often, this information is the *quid pro quo* given in exchange for the service. The level of invasiveness in the questionnaire usually correlates with the perceived importance of the services rendered. For example, if a user wishes to do something simple such as view certain content on a Web page designed by Macromedia, it will need to use a special plug-in.⁶ In order to obtain the plug-in, the user will be asked to fill out an information form. Given the relative insignificance of the plug-in, the Macromedia form makes it optional for a user to include his first or last name. But every user is required to supply his email address. If the user is willing to provide this basic information, he will then be able to download the plug-in and view the desired content in an optimal manner. Other online services demand more extensive information in return for their more extensive products. For example, to avail themselves of Yahoo! email and Web page services, Yahoo! users must fill out a form that not only requires disclosure of their names and email addresses, but also their street addresses, interests, and hobbies, etc. Information collected from forms such as these are combined into massive databases owned by the respective service providers.

A somewhat more subtle method by which service providers are able to gather information is through the use of cookies, also known as "persistent client-side hypertext transfer protocol files."⁷ These are small files that are downloaded from the service provider's host computer to an individual user's computer and stored there. When the user returns to the service provider's site, the cookie is retrieved from the user's computer, allowing the service provider to maintain details on the movements of the user within its site. Some Internet service providers have set up wide-ranging networks of cookie senders and collectors, in the form of banners that appear on Web sites of all types and descriptions. The pro-gram associated with those banners pumps the cookie information into a single depot. Online advertising giant Doubleclick is one such company.⁸ It develops and maintains individual user profiles that can

then be sold to direct advertisers to better target their advertising audiences. The method by which cookies are stored and maintained may also be employed in a corrupt manner, allowing a service provider's computer to mine and manipulate all of the cookies gathered by a user and thus develop a very highly detailed profile of where the user has been and when they were there.⁹

Internet public discussion groups such as Usenet and Listserv can also operate as a source of information about Internet users. When a user posts opinions on one of these forums, that information is often archived in a permanent database. If a user's email address or user name remains constant over the years, it becomes a simple matter to write an automated software routine that will scan those archives, and collate and analyze the opinions of that user.

As a final example, service providers supplying access to the Internet are in a unique position to gather and store information pertaining to individual users. The Internet is a global network of large servers (nodes) sharing information in a way that allows data to be efficiently routed to particular host computers. Internet access providers are the gatekeepers, standing between individual users and the World Wide Web. Access providers send and receive information to and from users and route it through to larger Internet nodes. Billing and other information needed to carry on the service provider-user relationship is stored by the access provider. In addition, the access provider can obtain and record accurate information detailing the exact location of particular users at a particular time and compile lists of all of their points of destination while online. In some cases, this allows access providers to learn the habits and preferences of their users. By linking the real-life identity of the user to his online activities, the access provider can build a highly personal profile of the user.

Returning to our narrative, Yahoo! collects personal information. In order to subscribe to any of Yahoo!'s services, a user must provide, inter alia, his zip or postal code, gender, occupation, industry, and interests. In addition to this information, which is "voluntarily"¹⁰ disclosed by those who wish to be subscribers, Yahoo! also collects other kinds of information about its subscribers without their knowledge. For example, Yahoo! gathers information that would allow an interested party to trace the source of each and every comment posted on each and every one of its message boards. Yahoo! does this by saving a log of Internet Protocol (IP) addresses¹¹ for every person that posts a message to one of its message boards. These IP logs are kept by Yahoo! for years and could potentially be cross-referenced to private emails sent or received by its

subscribers, which are also stored on Yahoo! servers. The only way for users to ensure that Yahoo! does not have access to private communications is to encrypt their messages.¹²

Encryption may be divided into two types: symmetrical encryption and asymmetric encryption. The former works by creating a single key that is used in the calculations to convert the file into the ciphertext. That same key must then be used to decrypt that same file. The latter involves two related keys, one of which only the owner knows (the "private key") and the other which anyone can know (the "public key"). The message is encrypted using the private key and may then be decrypted by using the public key. In doing so, the decrypting party may satisfy himself that the message received is accurate in content and that the party sending the message is, in fact, who he purports to be.¹³

Given its incredible technical means to gather, copy, store, and manipulate personal information, it is no surprise that Yahoo! had exactly the information that AnswerThink was looking for. And this was likely not the first time that a high-powered corporation like AnswerThink had instituted legal proceedings merely to intimidate and silence its online critics.¹⁴ Is it any less surprising that Yahoo! decided to disclose to AnswerThink personal information about Aquacool_2000?

Don't decide yet — there are additional facts. The relationship between Yahoo! and its users is said to be governed by the "Terms of Service" promulgated on the Yahoo! Web site. The "Terms of Service" incorporate by reference Yahoo!'s "Privacy Policy."¹⁵ The first sentence of its "Privacy Policy" proclaims that "Yahoo! is committed to safeguarding your privacy online." It further states that:

This Privacy Policy will let you know: what personally identifiable information is being collected about you; how your information is used; who is collecting your information; with whom your information may be shared; what choices are available to you regarding collection, use, and distribution of your information.¹⁶

The policy also provides that subscribers will be notified "at the time of data collection or transfer if your data will be shared with a third party and you will have the option of not permitting the transfer."¹⁷ However, according to the policy, Yahoo! will only disclose a member's personal information when it believes in good faith that such disclosure is required by law.¹⁸

At the bottom of its "Privacy Policy" and throughout its Web site, Yahoo! displays the TRUSTe certificate,¹⁹ a logo that is familiar to many Internet users. By featuring the TRUSTe seal throughout its Web site, Yahoo! represents to its users that it complies with strict privacy policies and procedures and that it will not disclose personal information to third parties without prior permission or some other legal justification.

Notwithstanding its explicit "Terms of Service" and detailed "Privacy Policy," Yahoo! handed over to AnswerThink all of the information that it had requested. Apparently, Yahoo! receives hundreds of similar requests for personal information every year and has granted several such requests without ever notifying the subscriber that his personal information and private communications were about to be disclosed.²⁰ By failing to notify its subscribers, Yahoo! precludes people like Aquacool_2000 from mounting any sort of defence until it is too late. Once Aquacool_2000's personal information became known to AnswerThink, there was no turning back.

Aquacool_2000 is not alone in his plight. In fact, the US Federal Trade Commission has been investigating the actions of Yahoo!'s GeoCities²¹ since the fall of 1998. The FTC has charged GeoCities with misleading subscribers by advertising that its policy was to not release personal information while, in fact, GeoCities was selling that information to direct marketers. The information was then used to contact subscribers with unsolicited, unwanted advertisements.²² More disturbingly, Geocities has also been accused of using a children's version of its Web site to collect personal information from unwitting minors. Information-gathering techniques have included requesting information about parents' mutual funds and their income-earning capacities in exchange for various prizes or rewards. The FTC has taken a special interest in discovering the extent of such activity, its ramifications, and possible solutions to this unacceptable practice.²³

Of course, Yahoo! is not the only Internet service provider known to have disclosed personal information to a third party upon request. Consider the case of Timothy McVeigh, a retired officer of the US Navy, who faced discharge from his position on a US submarine after a member of the Navy's judge advocate general, acting on an anonymous tip, asked a paralegal to contact America Online (AOL) to find out personal information about him. Without a warrant or court order, AOL released personal information to the paralegal about McVeigh's sexual orientation. On this basis, McVeigh was dismissed from the Navy — his conduct ruled as being against its policies on homosexuality. This decision was ultimately overturned and the conduct of the naval investigation was found

to be questionable. Initially, AOL denied that it had released the information at all but eventually issued a full apology for contravening its own standards of privacy and confidentiality.²⁴

American service providers are not the only ones to disclose personal user information to third parties without their knowledge or consent. Canadian providers have done the same. Imagine the following. Some-one sends you an email with the subject header, "TRY THIS!" You aren't even aware that this particular email has been sent to you. Because your inbox is overloaded with messages, the "TRY THIS!" message causes you to exceed your available disk quota. Consequently, access to your email is disabled. So you phone your Internet service provider, Supernet, to complain that you are unable to access your email. You are told that a technician will look into the matter. In an attempt to free up some memory and thereby enable your email account, the technician searches for files with large attachments that can be deleted. After opening the message with the subject header, "TRY THIS!," the technician notices attachments with suspicious filenames. Suspecting that the large attachments are child pornography, the technician opens a file. Sure enough, the message that has been sent to you without your knowledge or consent contains images depicting young children engaged in sexual activity. The technician informs her supervisor, who in turn contacts the police. The police request an electronic copy of the file. Supernet decides to cooperate. Consequently, Supernet forwards several of your messages to the police without telling you.

It is worth pausing to underscore the fact that, because your account has been disabled, the illicit "TRY THIS!" file (the existence of which remains unknown to you) has not yet been delivered to you. Knowing this, the police instruct your Internet service provider to resend the pornographic email to you so that it will be in *your* possession. On this basis, the police will then be able to obtain a search warrant, seize your computer, and arrest you.

Believe it or not, this actually happened in Alberta.²⁵ Perhaps even more surprising was the decision that was rendered by the Alberta Court of Queen's Bench. Smith J. held that Supernet's search of the user's inbox, its decision to open the user's email without his consent, the police's instruction to copy and then forward them his mail without telling him, and the police's instruction to resend the illicit file to the user did not unjustly interfere with the user's reasonable expectation of privacy.²⁶

After pausing for dramatic effect, I must now confess that, in my previous narrative, I sugarcoated the facts. In the actual Alberta case, Dale Weir, the recipient of the "TRY THIS!" email, was not an innocent

person who was framed by the sender of the email. On the facts set out in *R. v. Weir*, the addressee of the message was a consumer of child pornography. Though this revelation certainly makes it more difficult to sympathize with Weir about the fact that his personal information was ultimately disclosed, the manner in which Weir's private communications were discovered and disclosed should be troubling to every-one. There was no subpoena, no search warrant — no prior judicial authorization of any sort. Supernet simply made a unilateral decision to sift through Weir's private account and then disclose its finding with-out notice or any other form of due process.

The narratives considered above illustrate the incredible power that Internet service providers (ISPs) hold over their users. ISPs are by default the gatekeepers of informational privacy on the Internet. By providing online services such as email, Web site space, or portals to various online consortiums, an ISP gains access to and control over a plethora of personal information and private communications belonging to each of its many users. Each user is therefore dependent on those who provide them with Internet services, not only for the proper storage, maintenance, and management of their personal information and private communications, but also for determining whether and when their personal information may be disclosed to third parties. In other words, the safeguarding of user information is largely dependent on the benevolence and good judgment of ISPs. As illustrated by the above narratives, this is sometimes cause for concern.

In Canada, the newly enacted *Personal Information Protection and Electronic Documents Act*²⁷ prescribes a number of rules that are sure to have an impact on many of the informational transactions between ISPs and third parties. But as Canada's federal privacy commissioner has recently stated, "Bill C-6 is far from the end of the process of protecting privacy in this country. There remain enormous gaps in the protection of individuals from inappropriate intrusions, be they brought about by dealings with personal information or by other forms of surveillance."²⁸ The aim of this chapter is to fill in one of those gaps. Despite the growing body of literature on privacy in the information age, there is a paucity of research focusing squarely on the nature of the legal relationship between Internet user and service provider.

The object of this study is to examine that relationship as a special instance of a relationship of dependence. There are several valuable reasons for doing so. First, a clearer understanding of this relationship might assist law reformers in determining whether special obligations ought to flow from it. Given the future importance of access to

information and informational privacy, it is essential to know whether the relationship between Internet user and service provider is or ought to be governed by anything other than the contractual arrangements between the parties or the minimal requirements of recently enacted privacy legislation. Second, an examination of ISP-user relationships in this context will have the reciprocal effect of deepening our understanding of the notion of a "relationship of dependence." By casting its focus on the *informational imbalance* between the parties rather than the more familiar types of power imbalances (e.g., inequalities based on economics, social status, physical strength, and expertise), this study seeks to provide a more robust understanding of what it is that makes a relationship one of dependence. As such, this chapter will ultimately contribute to a broader understanding of the law of obligations.

THE CONTRACTUAL UNDERPINNINGS OF ISP-USER RELATIONSHIPS

The logarithmic proliferation of available Internet services defies comprehensive quantification or classification. However, it is useful to categorize Internet services according to the nature of the exchange between ISP and user. For present purposes, it is sufficient to consider three kinds of basic exchanges: (1) services in exchange for cash, (2) services in ex-change for personal information, and (3) services in exchange for tolerated advertising.²⁹

Internet access is almost always exchanged for cash. Service providers of this sort act as the direct intermediary between the user's individual computer and the Internet. Usually, access is gained through local land phone lines that connect the user to the access provider's host computer. Access providers often provide a range of services on a cash-for-service basis. Among these are: email accounts (with arrangements made to download the email to the user's computer), multiple email addresses, access to various databases, access to mailing lists of users with similar interests, and hosting for user Web pages. Other services offered in exchange for cash include the use of remailers and other technologies that allow users to gain anonymous access to databases in libraries, government departments, and other data collection services, as well as anonymous access to certain entertainment sites.

The second category provides various services in exchange for a user's personal information rather than money. These often include portal services, i.e., personalized launch pads to various zones of the Internet tailored to each user's specific interests. Yahoo! is an example. In ex-change for the user's name, address, and other personal information about his habits and preferences, the user can get stock quotes,

subscribe to a personalized news compilation service, be apprised of the local weather conditions, etc. Web site hosting (e.g., GeoCities) is also available in exchange for personal information.

In the third category, personal information is not required. Services are "free" to users (except for the annoyance costs generated by distracting advertisements). Services in this category range from the strange and whimsical to the obvious gateway to paid services. An example near the former end of the spectrum is an online purity test that allows users to rate their purity against the scores collected about others.³⁰ Apparently, the information collected for the purity test is not logged. At another point on the spectrum, users encounter a slew of cartoons generally dealing with the death and dismemberment of small fuzzy creatures.³¹ The other end of the spectrum is exemplified by a site that offers a free mortgage calculator in the hopes that the user will then be tempted to make use of the paid services of that same Web site.³²

There is a common thread stitching together this motley collection of service providers. Whether in exchange for remuneration, information, graft, or graffiti, the vast majority of online service providers do not merely create a public thoroughfare for virtual voyeurs. Rather, they attempt to establish some sort of relationship with those who show interest in their services. Stripped down to their most basic form, almost all of these relationships can be understood as contractual in nature. Something of value is offered by one person to another in exchange for an online service.

Much has been written on the subject of contract formation online.³³ Recently, various jurisdictions have begun to propose and enact electronic commerce legislation, one of the aims of which is to ensure that traditional doctrinal defects associated with the formation of online contracts are cured through the use of functional equivalents.³⁴ For example, contracts that traditionally required a signature can now be achieved through a series of mouse clicks on a computer. In this instance, the functional equivalent of a signature is simply the manifestation of assent through some identifiable means.³⁵ So long as the online transaction demonstrates the communication of an offer, its acceptance, and the exchange of valuable consideration, a contract will be created.³⁶ The medium of communication is relevant only insofar as it might affect the place where the contract was purportedly made, or the time at which the contract was said to have come into existence, should such determinations be in dispute.

For the purposes of this study, the analysis of ISP-user agreements will be limited to situations in which service providers clearly intend to enter into contractual relationships and therefore require users to

manifest their assent to a prominently displayed "Terms of Service" document via some functional equivalent of a signed document. For the sake of simplicity, it will be assumed that the typical problems associated with contracts of adhesion (*viz.* reasonable notice as to onerous or unusual terms) have been adequately dealt with through the careful design and delivery of the particular Web-wrap agreement in question.³⁷

Limiting the investigation of ISP-user relationships to situations where the ISP provides explicit "Terms of Service" that are manifestly assented to by the user, a relatively extensive survey of more than forty such agreements³⁸ governing a variety of services in various jurisdictions³⁹ ultimately revealed a range of different obligations undertaken by ISPs with respect to the disclosure of personal user information. The results of the survey indicate that ISP-user relationships can be understood as falling into one or more of five categories:⁴⁰ (1) Confidential; (2) Confidential within the Limits of the Law; (3) Disclosure when Illegality Is Suspected; (4) Disclosure to Protect ISP or in Extraordinary Circumstances; and (5) Voluntary Disclosure and Active Monitoring.

CONFIDENTIAL

Though this form of contractual undertaking is indeed quite rare, some ISPs have actually promised to keep their users' personal information confidential in spite of any and all requests for disclosure. A relatively well-known example of this was an anonymous remailer service known as anon.penet.fi. By stripping email messages of the identities and digital addresses of the original sender and then remailing them to the locations specified, the anon.penet.fi. remailer service allowed individuals who might not otherwise have participated in certain socially beneficial discussions to have a voice, without fear of reprisal.⁴¹ Given his allegiance to the cause of anonymous speech, this particular service provider, Johan Helsingius, had evinced a "strong commitment to preserving anonymity in all cases," indicating that he would not waiver even in the face of a court order.⁴² However, when push came to shove, after a Finnish court required him to divulge the email address belonging to one of his users who was suspected of distributing child pornography, Helsingius caved. Shortly thereafter, he decided to shut down his remailer.⁴³

ISPs are generally unwilling to promise absolute confidentiality to their users because of recently proposed and enacted legislation in various jurisdictions that require ISPs to comply with law enforcement, failing which the ISP will be strictly liable, either criminally or civilly, for the conduct of its users. For example, the recently proposed Bill

C-231, the *Internet Child Pornography Prevention Act*,⁴⁴ requires ISPs to "advise the Minister of the identity of [the user], the nature of the material and the means whereby it may be accessed by others."⁴⁵ According to this bill, an ISP that fails to do so will itself be guilty of an offence and could lose its licence or be subject to more serious criminal sanctions.⁴⁶

Provisions such as this have become known as *safe harbours*.⁴⁷ In the present context, a safe harbour aims to encourage responsible online behaviour by providing a statutory limitation on the liability of service providers. As one American author put it:

Legal accountability in cyberspace hinges critically on establishing, and fairly defining, the liability of [service providers]. Such liability is appropriate when the [ISP] provides the tools for the underlying offenses, and further aids the responsible party by concealing the user's identity. However, an opportunity should also be provided for [ISPs] to avoid liability when they are willing to cooperate with authorities. Such an incentive can be provided through a safe harbor provision guaranteeing the [ISP] protection from civil and criminal liability when the administrator (1) has acted in good faith, and (2) voluntarily discloses to the authorities the identity of a user engaging in illegal activities.⁴⁸

Notice the strategy here. Rather than involving government directly in the policing of online conduct, regulation is left in the hands of ISPs and users. A safe harbour allows an ISP to avoid liability for illegal conduct that takes place on their sites or as a result of their services. ISPs can protect themselves by taking affirmative action (e.g., removing the offending materials) and in some instances by disclosing information about their users.⁴⁹

While this strategy circumvents problems typically associated with a top-down governmental approach to regulation, it has its own draw-backs. As Sopinka J. astutely pointed out a few years ago:

A determination of the scope of liability of network operators will surely have ramifications on freedom of speech. If computer operators are held liable for the expression of their subscribers it would place a duty on them ... The result would likely lead to an increase in screening of private messages. It would potentially result in censorship, as companies would wish to protect themselves from possible civil or criminal liability. *This would put network administrators in the unenviable position of deciding what is acceptable speech and what is not.*⁵⁰

Though it does not, strictly speaking, contain a safe harbour provision, section 7 of the recently enacted *Personal Information Protection and Electronic Documents Act*⁵¹ has a similar effect.⁵² Assuming that ISPs are governed by the *Act*,⁵³ it will encourage ISPs to disclose personal information to third parties without the users' knowledge or consent whenever an ISP "has reasonable grounds to believe [that the users' personal information] could be useful in the investigation of a contravention of the laws of Canada, a province or a foreign jurisdiction that has been, is being or is about to be committed, and the information is used for the purpose of investigating that contravention."⁵⁴ To restate the point made by Sopinka J. in a slightly different way, legislative initiatives such as these put an ISP in an unenviable relationship with its users. While ISPs clearly owe certain duties to protect the confidentiality of their users, keeping quiet will sometimes conflict with their own interests. As a result of the safe harbour approach, it will sometimes be in an ISP's interest to disclose personal information in a manner that undermines the interests of its users.

Given that most ISPs recognize this cruel fact of online life, the "Terms of Service" agreements almost never promise confidentiality in regard to any and all requests for disclosure.

CONFIDENTIAL WITHIN THE LIMITS OF THE LAW

Many "Terms of Service" agreements promise that the ISP will take steps to ensure the confidentiality of a user's communications and will only release personal information in circumstances where the ISP is legally compelled to disclose. For example, the University of Calgary's "Computing and Networks Policy" promises that, "if a user is suspected of using university computers for illegal purposes, access to files, directories or other user information may be granted to persons outside the university only by appropriate order of a competent court."⁵⁵ ISPs who adopt this approach will generally request that the user remove the illicit material, failing which it will take matters into its own hands. A sample from Demon Internet's "Acceptable Use Policy" illustrates this approach:

Demon Internet's relationship with other networks, and ultimately its connectivity to the rest of the Internet depends largely upon proper behaviour by its customers. Demon Internet cannot tolerate any behaviour by customers which negatively impacts upon its own equipment or network, or upon the use by other customers of the Internet, or which damages Demon Internet's standing in the wider community.

Demon Internet will therefore enforce appropriate sanctions against any of its customers who are responsible for serious abuse of the Internet. Such sanctions include, but are not limited to, a formal warning, suspension of one or more of the customer's services, suspension of all Internet access through Demon Internet or termination of the customer's account(s).⁵⁶

ISPs who have opted for internal sanctioning of their users do not generally disclose information to law enforcement authorities unless they are explicitly directed to do so. Nor do they monitor online conduct or communications unless they have been notified of a user's illicit activity. An example of this approach can be found in America Online's "Rules of User Conduct":

America Online generally does not pre-screen, monitor, or edit the content posted by users of communications services, chat rooms, message boards, newsgroups, software libraries, or other interactive services that may be available on or through this site. However, America Online and its agents have the right at their sole discretion to remove any content that, in America Online's judgment, does not comply with Rules of User Conduct or is otherwise harmful, objectionable, or inaccurate. America Online is not responsible for any failure or delay in removing such content.⁵⁷

DISCLOSURE WHEN ILLEGALITY IS SUSPECTED

A good number of ISPs are disinclined to treat their users' personal information as confidential. They are therefore willing to disclose information whenever suspicion arises or a legally motivated request has been made. As we have seen, this is the practice adopted by Yahoo!.⁵⁸ ISPs who fall into this category tend to view cooperation with investigations as a more important goal than safeguarding their users' personal information. Recall that this latter approach was adopted by Supernet in its decision to forward Dale Weir's emails to the police merely on the basis of a request to do so. Unlike Yahoo!, the actions of Supernet comport with its current "Acceptable Use Policy and Liability Disclaimer," which provides that Supernet "will report to law enforcement authorities *any actions which may be considered illegal*, as well as any reports it receives of such conduct. When requested, [Supernet] will fully cooperate with law enforcement agencies in any investigation of alleged illegal activity on the Internet."⁵⁹ Presumably, notices such as these will make

it difficult for users to argue that they reasonably held a high expectation of privacy.

DISCLOSURE TO PROTECT ISP OR IN EXTRAORDINARY CIRCUMSTANCES

Some ISPs leave open the possibility that they might disclose personal user information for reasons other than law enforcement. Typically, these include the release of information where it is used for the purposes of acting in respect of an emergency that might threaten the life, health, or security of an individual.⁶⁰ Many commercial ISPs draft the exclusions to their privacy policies even more broadly. An example of one such provision is found in Microsoft's Hotmail "Terms of Service":

Microsoft will not monitor, edit, or disclose any personal information about you or your use of the Service, including its contents, without your prior permission unless Microsoft has a good faith belief that such action is necessary to: (1) conform to legal requirements or comply with legal process; (2) protect and defend the rights or property of Microsoft; (3) enforce the TOS; or (4) act to protect the interests of its members or others.⁶¹

By including the right to disclose personal information in order to protect and defend its rights or property as well as to protect the interests of others, Microsoft makes it quite clear that it has less interest in safe-guarding its users' personal information than ISPs falling into the other categories enumerated above. Still, ISPs in this category do promise that their default position is to not disclose personal information unless there is at least some reason for doing so. This can be contrasted with ISPs in the final category who make no such promises.

VOLUNTARY DISCLOSURE AND ACTIVE MONITORING

The final category consists of ISPs who are unwilling to make any assurances as to the confidentiality of their users' personal information. Of-ten, these ISPs make it clear to their users that they should have a low expectation of privacy. For example, Verio's "Acceptable Use Policy" spells out to its users that:

In general, the Internet is neither more nor less secure than other means of communication, including mail, facsimile, and voice telephone service, all of which can be intercepted and otherwise compromised. As a matter of prudence, however, Verio urges its subscribers to assume that

all of their on-line communications are insecure. Verio cannot take any responsibility for the security of information transmitted over Verio's facilities.⁶¹

Similarly, Muskoka.com informs users that it "does not guarantee privacy of your files and email. If you want complete privacy, encryption software is freely available."⁶²

Some ISPs go so far as to provide notice that they are actively monitoring user accounts and that they will voluntarily disclose user information and communications in a variety of circumstances. This is often the case with employers who provide Internet services to their employees, since employers generally have a greater duty to control the conduct of their employees. Consider the following typical employer policy:

The company's telephone, voice mail, computer storage and e-mail systems are the property of the company and are to be used for company authorized purposes only. All information transmitted or stored using the company telephone, voice mail, computer system and e-mail system is the confidential and proprietary information of the company, except for publicly available information.

All messages recorded or saved on voice mail or e-mail and all files stored on company computers are considered to be company records and may have to be delivered by the company in connection with litigation or to comply with a requirement.

Employees should not expect that any matter created, received, stored or sent on the telephone, voice mail, computer or e-mail systems will be confidential or private from company management, except for attorney client privileges benefiting the company. The company reserves and employees must protect and not waive rights of attorney client privilege as the right of the company. In addition, the company re-serves all trade secret protection and all rights to prohibit other parties from accessing such matters.

Except as provided in this Policy, company management reserves the right to access any voice mail, e-mail message, or any computer file created, sent, stored or received by any employee at any time and with-out notice.⁶³

Similar policies have been adopted by a number of service providers who offer online forums for real time chat. For example, ICQ indicates in its "Terms of Service" that it may:

(c) nominate any person who may not be an ICQ employee to monitor, using his own discretion, any channel or chatroom and to allow him to deny or terminate access granted to you or any other user, without notice, at anytime, including while you are chatting or delivering or sending information. ICQ may cancel such nomination, at any time for any reason or no reason.⁶⁴

To summarize the contractual underpinnings of ISP-user relationships — and this should come as no great empirical surprise — it appears that Internet service providers have adopted quite a broad range of relationships with their users viz. the treatment of their personal information. At one end of the spectrum, some ISPs hold themselves out as the guardians of informational privacy. At the other end of the spectrum are ISPs who do not view it as part of their role to safeguard the privacy interests or, for that matter, *any* interests of their users.

So far, we have only considered contractual approaches to various ISP-user relationships. Underlying the contractual understanding of the relationship is the idea that the parties to the agreement are otherwise unrelated and each of them is acting in a self-interested manner. Although the law of contract governs relationships voluntarily entered into by parties at arm's length, not all contractual relationships are considered to be relationships at arm's length.⁶⁵ The question that must ultimately be addressed is whether the relationship between ISP and user — though it is at its core contractual in nature — is *always* to be understood as a relationship at arm's length.

RELATIONSHIPS OF DEPENDENCE AND INTERDEPENDENCE

Social Exchange Theory

Contract lawyers are not the only ones to conceive of relationships as founded on the idea of an exchange. Social psychologists have, for many years, used the exchange model as a means of understanding human interaction. According to social exchange theory, participants in a social interaction jointly determine the rewards and costs that they achieve from it.⁶⁶ By understanding social interaction in this way, those who form relationships with each other may come to depend on one another. According to social exchange theory, the notion of *dependence*

describes the degree to which one of the two interacting parties needs their relationship.⁶⁷ One can gauge the level of a person's needs by determining the extent to which that person's well-being rests on involvement in the relationship. Dependence is thought to be greater to the degree that a relationship provides good outcomes and to the degree that the outcomes available in alternative relationships are poor.⁶⁸

Some social exchange theorists have recognized that dependence in a relationship affects the power held by each of the parties. This is so because one individual's power over another derives from the other party's being dependent on him.⁶⁹ Not straying too far from Weber's classic definition of power, social exchange theorists define power as the potential for one actor to obtain favourable outcomes in an ex-change episode at another's expense.⁷⁰ Accordingly, power is fundamentally rooted in the dependence actors have on one another.⁷¹

Thus in order to determine whether a particular relationship is a relationship of dependence, one must determine whether one party holds power over the other. Social psychologists who subscribe to *interdependence theory* have for some time held that the measure of one person's power in a relationship is the extent to which, by varying his behaviour, he can affect the quality of another's outcomes. According to Thibaut and Kelly, power can manifest itself in two forms: *fate control* and *behaviour control*.⁷² When X has fate control over Y, he can affect Y's outcomes regardless of what Y does. It is therefore possible for X to employ his fate control over Y as a means of controlling Y's behaviour. However, when X merely has behaviour control over Y, it remains possible for Y to reduce the variations to his outcomes by adjusting his behaviour in response to X. In the context of behaviour control, the effect of X changing his behaviour will sometimes make it desirable for Y to change his own behaviour accordingly.

Since the nature of a social exchange is dyadic, it is usually the case that *both* parties involved in a personal relationship are to some extent dependent on their relationship. The notion of *interdependence* in a relationship describes the extent to which the well-being of both parties is dependent upon the existence of the relationship.⁷³ Usually, this means that each party has some power over the other. Thus, as the level of interdependence increases in a relationship, each party becomes restricted in terms of the power that can be exerted upon the other with impunity. Increasing interdependence ultimately results in an equilibrium in terms of the power structure underlying the relationship.

So far, the notion of dependence has been characterized as a function of the extent to which a relationship can satisfy the needs of the party

and the extent to which the quality of alternative relationships is poor. Other interdependence theorists have extended these basic ideas. One recent extension known as the *investment model*" adds two further dimensions. First, it suggests that dependence increases to the degree that the dependent party makes an *investment* into the relationship. Here, investment refers to the resources that a person has devoted to the relationship, either directly or indirectly.⁷⁵ Understood quite broadly in this context, resources include anything that can be transmitted from one person to another. Thus one invests in a relationship by devoting such things as goods, services, love, status, or information to the relationship.⁷⁶ The more that one invests into the relationship, the more he becomes dependent on it.

Those who subscribe to the investment model suggest that dependence in a relationship also produces the psychological experience of *commitment*.

Commitment includes conative, cognitive, and affective components. The conative component of commitment is *intent to persist* - John feels intrinsically motivated to continue his relationship with Mary. The cognitive component is *long term orientation* - John envisions himself in the relationship for the foreseeable future and considers the implications of current action for future outcomes. The affective component is *psychological attachment* - John experiences life in dyadic terms, such that his emotional well-being is influenced by Mary and their relationship.⁷⁷

It is important to differentiate between dependence and commitment. Dependence describes the structural aspect of the relationship between two parties, whereas commitment characterizes one party's subjective experiences concerning the relationship. Dependence is a structural state describing the degree to which an individual needs a relationship to increase the quality of his outcomes. Individuals may or may not be aware of their dependence:

At critical moments, John may actively contemplate his dependence on Mary, consciously reviewing the extent of his satisfaction, alternatives and investment. At other times, however, John's dependence may remain largely implicit - he may not consciously consider the extent of his need. In contrast commitment is the *subjective state* that dependent individuals experience on a daily basis. In this sense, commitment can usefully be construed as the subjective sense of allegiance that is established with regard to the source of one's structural dependence.

Because John is dependent on his relationship, he develops intentions to persist with Mary, he foresees long term involvement with Mary, and he feels affectively linked to Mary and their relationship. It is the psychological experience of commitment, rather than the structural state of dependence, that is argued to influence everyday behavior in relationships.⁷⁸

Though commitment is what influences a party's behaviour in a relationship, it is the level of that person's dependence that affects the actual power held by each of the parties in the relationship. This is an important distinction to keep in mind when applying social exchange theory to an examination of ISP-user relationships.

Dependence and Interdependence in ISP-User Relationships

Social exchange theory provides a deeper understanding of the relationship between Internet service provider and user than the more straightforward contractual approach contemplated earlier in this chapter ("The Contractual Underpinnings of ISP-User Relationships"). This theory can be utilized to explicate the degree to which users come to depend on Internet service providers.

Internet User Dependence

Internet users are dependent on service providers in a number of different ways. Given the vast range of services available, it is neither possible nor desirable to compile a comprehensive list. A few examples will suffice. Perhaps the most basic need of Internet users that requires the establishment of a relationship with an ISP is the need to gain access to the Internet.⁷⁹ An inability to obtain the services of an access provider will decrease the quality of a person's outcomes. In a networked world, it will leave individuals completely disconnected from the many new forms of social interaction that take place online. That is, a relationship with an ISP is necessary for the development of other personal relationships. While the question of universal access to online services may seem unimportant to some,⁸⁰ the issues surrounding access will become more pressing as government and private sector organizations begin to disseminate information and do business exclusively in the online setting. This possibility is not farfetched. For example, the Ministry of the Attorney General of Ontario is about to launch its Integrated Justice Project.⁸¹ The project aims to integrate information flowing from a number of its justice partners, including: law enforcement agencies, the Crown Attorney's office, court services, the judiciary, and correctional

services. The integration process and the delivery of vital information will gradually move away from the paper-based world to the online setting and aims eventually to disseminate all court-related documents and to discharge all Crown disclosure obligations by exclusively electronic means. Without establishing a relationship with an ISP, individuals will be unable to obtain information necessary to the administration of justice. The same will soon be true for many other kinds of government and private sector information and informational services.

As an American author recently put it, "in an age where the key wealth-creating activity ... concerns the production, distribution and manipulation of information, the Internet is destined for a prominent role."⁸² With a continued social migration into digital environments, the well-being of individuals will come to depend on their relationships with ISPs. Some services, such as access, are widely available. For now, this means that people are not necessarily dependent on the relationships they have with particular access providers since they could achieve virtually identical outcomes through an alternative service provider. This is generally true for those users who have the necessary resources (i.e., cash or credit). Others, who rely on a local FreeNet and other no-charge service providers, are more dependent on the relationship they have with their access providers.⁸³

In addition to a user's dependence on an ISP to gain access to important information services and to establish and continue online relationships with others, we have seen that ISPs are by default the guardians of informational privacy on the Internet. By providing online services such as email, Web site space, or portals to various online consortiums, an ISP gains access to personal and private information belonging to each of its many users. Each user is therefore dependent on those who provide him with Internet services, not only for the proper storage, maintenance, and management of his personal information, but also for ensuring that his private communications are secure from intrusion and kept confidential. Once user information is in the care and control of a service provider, the ISP is usually in a position to assert power over its users.

Applying interdependence theory to this scenario, an ISP has fate control over its users. That is, by being in a position to employ a user's private information to various ends,⁸⁴ an ISP can affect the user's out-comes, regardless of what the user does. To continue with an earlier example, Yahoo!'s decision to disclose the identity of Aquacool_2000 to AnswerThink (in order to avoid its own legal battle with the powerful corporate entity) resulted in the dismissal of Aquacool_2000 from his

place of employment. Because of Yahoo!'s practice — which was to disclose personal information without notice whenever such information was being sought for the purposes of litigation — the quality of Aquacool_2000's outcomes was diminished. As soon as his personal information was disclosed, there was nothing that Aquacool_2000 could have done to alter his fate. Recall from above that fate control can be used by the power-holder in a relationship as a means of controlling the dependent party's behaviour. Thus an ISP's ability to disclose a user's personal information or private communications *with impunity* can be used as a means of regulating the user's conduct online. In fact, this is precisely the strategy that underlies the legal use of safe harbour provisions discussed earlier (in "The Contractual Underpinnings of ISP User Relationships").

One might argue that, given the availability of alternative service providers, the power that can be asserted by any given ISP is in fact limited to behaviour control. Those who espouse this position would say that an ISP does not have the power to control its users' fate, since users are not in fact bound to remain in that relationship.⁸⁵ If a user does not like the privacy policy of a particular ISP, he can simply change his behaviour; i.e., surf the Net and sign on with a different provider whose privacy policy would result in more favourable outcomes. If nothing else, the Internet has created a multiplicity of alternatives.

While it is true that, for many Internet services, a user might easily establish an alternative relationship that would result in better outcomes, it is crucial to recognize that, if the user has previously entered into a relationship with a different service provider, he may have made a very special sort of investment in the first relationship. He may have *reposed confidence in the relationship* by voluntarily allowing the service provider access to personal information or private communications on the faith of the service provider's promise that no such information would be disclosed to a third party without his knowledge and consent.

Reposing confidence in a relationship where both parties have invested love is risky enough. Fortunately for those who are in a close personal relationship, with love usually comes commitment, which, in the context of interdependence theory, means that both parties intend the relationship to persist, feel a long-term orientation towards it, and have a psychological attachment towards each other. Since there is no love lost between them, the same cannot be said of ISP-user relationships. Though one consequence of many ISP-user relationships is that the ISP becomes privy to all sorts of personal information and private communications belonging to the user, most ISP-user

relationships are not close personal relationships. Since an ISP does not generally feel a sense of commitment to its users, the unique kind of informational investment made by a user leaves him or her in a state of dependence.

ISP-User Interdependence

Interdependence theory asserts that, for most dyadic relationships, the well-being of each party is to an extent dependent on the well-being of their relationship.⁸⁶ Notice that this is *not so* in the case of ISP-user relationships. Though ISPs are commercially dependent on the existence of users in general,⁸⁷ they are not usually dependent on particular users. This creates a serious imbalance in most ISP-user relationships. From the perspective of an ISP, the user is but an (IP) number. Unlike when a husband or wife is confided in and is later pressured with a request to disclose personal or private information to a third party, the ISP is not *psychologically committed* to the relationship. Given the lack of interdependence in their relationship, the ISP will be inclined to give greater weight to furthering its own interests than it would to furthering the well-being of the user (or to furthering its relationship with the user). Since each individual user is in essence dispensable, the power structure of most ISP-user relationships will never reach a state of equilibrium. Consequently, the ISP will not usually be inclined to protect the user's interests as against its own or others. This puts ISPs in a position similar to banks and other commercial institutions that have care and control of their customers' personal information or private communications. The difference is one of degree. Given that ISPs often store and manage users' private communications on an unlimited number of subjects (not just financial information), the personal hold that an ISP may have over its users could make users even more dependent on the confidentiality of ISP-user relationships than would be the case with other commercial customers in their relationships with financial institutions.

As we have seen, Internet users are often forced to depend on the benevolence and good judgment of an ISP. But sometimes ISPs who have been reposed of trust or confidence on the basis of an undertaking not to disclose personal information do not carry out those undertakings. In such cases, an interesting question arises: when an ISP discloses a user's personal information or private communications, is this merely a breach of contract, or is it a breach of trust or confidence? The answer to this question requires a determination as to whether the relationship between Internet service provider and user is *merely a* relationship at arm's length.

RELATIONSHIPS OF TRUST AND CONFIDENCE

For several centuries, the law has recognized that the preservation of society requires a vigilant protection of the trusting relationship.⁸⁸ "No part of the jurisdiction of the Court is more useful than that which it exercises in watching and controlling transactions between persons standing in a relation of confidence to one another."⁸⁹ To use the succinct words of one commentator, "the mischief to which the policy is directed is clear. Trusted parties may serve their own ends rather than those of the trusting party."⁹⁰ In order to avoid such mischief, the law of fiduciaries will sometimes protect those who have come to depend on others.

Through its willingness to impose duties on fiduciaries and its recognition that traditional categories of fiduciary relationships are not closed,⁹¹ the law has been said to facilitate the development of inter-dependent relationships. In his well-known work on the fiduciary obligation, E.J. Weinrib characterized the fiduciary obligation as the law's realization of the economic importance of fostering incentive by protecting relationships of interdependence — relationships that he refers to as "the entrepreneur's business apparatus": "A sophisticated industrial and commercial society requires that its members be integrated rather than autonomously self-sufficient, and through the concepts of commercial and property law provides mechanisms of *interaction and interdependence*. The fiduciary obligation ... constitutes a means by which those mechanisms are protected."⁹² According to Weinrib, the basic policy underlying the fiduciary obligation is the desire to preserve and promote the integrity of socially valuable relationships that arise as a result of human interdependence.⁹³ An interactive and interdependent society mandates the monitoring of trusting relationships in order to avoid their potential for abuse. Without a public policy that prohibits the abuse of another's trust, individuals would be less inclined to place themselves in relationships of dependence.

Although the policy underlying the law of fiduciaries is relatively uncontroversial, its definition and scope are less so. As one Supreme Court of Canada judge admitted in the midst of one of Canada's most important decisions on the subject, "there are few legal concepts more frequently invoked but less conceptually certain than that of the fiduciary relationship."⁹⁴ Taking these remarks as a kind of judicial cue, it is beyond the scope of the present study to try to articulate a comprehensive explication of the fiduciary concept. The aim here is much more mod-est. It is restricted to a determination of whether any of the core notions underlying the fiduciary concept might plausibly be ascribed to ISP-user relationships.

The Fiduciary Concept

In the *Law of Trusts in Canada*,⁹⁵ D.W.M. Waters endorses the notion that fiduciary status is most often associated with trusts and "trust-like" relationships in which conflicts of interest and duty tend to arise. Within a trusting relationship, the trusted party is given discretion to affect the principal's interests. As a result, the principal is dependent on the trusted party. As Weinrib describes it, "the leeway afforded to the fiduciary to affect the legal position of the principal in effect puts the latter at the mercy of the former, and necessitates the existence of a legal device which will induce the fiduciary to use his power beneficially."⁹⁶ The reposing of trust and the resulting discretion places the trusting party in a state of dependency. After all, the trusted party may act indifferently or without care or diligence on behalf of the trusting party, or the trusted party may intentionally divert value away from the trusting party.⁹⁷ As we have seen, these mischievous possibilities are to be discouraged. To that end, the courts will impose a fiduciary obligation on the trusted party and control the use of his or her discretion.

If the relationship is not one in which trust or discretion arises, then there appears to be no reason for imposing fiduciary obligations. As noted by Weinrib, discretion and obligation are correlative concepts. "Accordingly, the hallmark of a fiduciary relation is that the relative legal positions are such that one party is at the mercy of the other's discretion."⁹⁸ R. Flannigan suggests that a fiduciary's discretion can usually be understood as part of a wider category of power held by the trusted party that includes any access that he might have to the trusting party's assets.

"Discretion," by itself, is not the significant fact. In this context we are concerned with the abuse of the relationship. For this purpose discretion merely indicates that the trusted party has access to assets and, hence, the opportunity to abuse ... Trust which leads to the trusted party gaining "access" to assets will attract the fiduciary obligation. The presence of "discretion" is merely an indication in a particular case that such trust exists. It is the potential for the abuse of that trust which requires the obligation.⁹⁹

Status-Based Fiduciary Relationships

The law of fiduciaries was originally premised on the principle of *uberrimae fidei* — a duty of utmost good faith. Traditionally, a duty of loyalty was imposed upon individuals who fell within a recognized list of categories of relationships. On this approach, when the nature of a

particular relationship was in dispute, the judicial analysis usually consisted of listing the traditional categories of relationships that attracted a fiduciary obligation, followed by an attempt to determine if the relationship in question fell within the scope of one of the listed categories. As one recent commentator has described it, "the nature of the particular relationship itself or the interaction of the parties involved in it was a secondary matter."¹⁰⁰

The most commonly cited examples of traditional fiduciary relationships include: trustee-beneficiary, solicitor-client, principal-agent, director-corporation, partner-partner, employer-employee, guardian-ward, doctor-patient, parent-child, and confessor-penitent.¹⁰¹ The traditional fiduciaries are sometimes described as "status-based" fiduciary relationships. Once a party is able to establish that the relationship in question falls within the scope of one of the recognized status relationships, then certain facts no longer need to be proven. So long as the relationship is of the appropriate status, there is no requirement to prove that the fiduciary is in a position of trust or is in a position to unilaterally exercise a discretion; the relationship will be deemed fiduciary in nature upon proof of its status.

The hallmark of all traditional fiduciary relationships is that one party is dependent on the other. This accords with the concepts of trust and loyalty, which stand at the heart of the fiduciary obligation. The word "trust" connotes a state of dependence and the correlative duty of loyalty arises from the level of trust and dependence that is evident in the relationship. The type of disclosure that routinely occurs in these kinds of relationships results in the trusted party's acquiring influence that is equivalent to a discretion or power to affect the trusting party's legal or practical interests.

Many of the categories enumerated above consist of relationships wherein the trusting party has sought the advice of the trusted party. Courts exercising equitable jurisdiction have repeatedly affirmed that clients in a professional advisory relationship have a right to expect that their professional advisors will act in their best interests, to the exclusion of all other interests, unless the contrary is disclosed. A person receiving advice should not need to protect himself from the abuse of power by his independent professional advisor when the very basis of the advisory contract is that the advisor will use his special skills on behalf of the advisee. As B. Welling puts it: "Imposing fiduciary obligations on the traditional licensed pillars of the community — doctors, lawyers, bankers, corporate directors — required them to dispense advice with due regard for the fact they were not dealing with customers of

equal bargaining power, but with trusting souls who were dazzled by their credentials and hung on their every word."¹⁰²

Fact-Based Fiduciary Relationships

Although the use of traditional categories to determine fiduciary relationships was originally quite effective as an abbreviation of a difficult legal concept, some commentators subsequently recognized that this approach is subject to a hardening of the categories. As Weinrib writes: "The existence of a list of nominate relations dulls the mind's sensitivity to the purposes for which the list has evolved and tempts the court to regard the list as exhaustive and to refuse admittance to new relations which have been created as a matter of business exigency."¹⁰³

On this basis, some courts have come to recognize that a variety of other relationships are also constructed on the same foundation of trust and loyalty as were the traditional status-based fiduciary relationships. In recognition of the inherent danger of unduly restricting fiduciary doctrine — especially given the fact that the fiduciary doctrine aims to protect, preserve, and encourage a number of socially and commercially valuable relationships — courts have not limited the fiduciary obligation to the fixed category of status-based fiduciary relationships.

The Supreme Court of Canada has declared that the categories of fiduciary relationships are not closed.¹⁰⁴ As Dickson J. held in *Guerin v. R.*: "It is sometimes said that the nature of fiduciary relationships is both established and exhausted by the standard categories of agent, trustee, partner, director and the like. I do not agree. It is the nature of the relationship, not the specific category of actor involved that gives rise to the fiduciary duty. The categories of fiduciary ... should not be considered closed."¹⁰⁵ As a result, fiduciary doctrine has expanded to cover other fact-based fiduciary relationships. More recently, writing for the majority of the Supreme Court of Canada, LaForest J. stated: "In summary, the precise, legal or equitable duties the law will enforce in any given relationship are tailored to the legal and practical incidents of a particular relationship. To repeat a phrase used by Lord Scarman, ' [t] here is no substitute in this branch of the law for a meticulous examination of the facts': see *National Westminster Bank Plc. v. Morgan*, [1985] 1 All E.R. 821 (H.L.) at p. 831."¹⁰⁶ The identification of fact-based fiduciary relationships requires that the judiciary undertake, in addition to a status-based analysis, a fact-based analysis. As a result of the Supreme Court's adoption of this approach, other Canadian courts and legal scholars have since endeavoured to define the policies and principles that underlie the fiduciary relationship with the aim of identifying its constituent

elements. Over the last quarter century, the Supreme Court of Canada has spent a great deal of time wrestling with the principles, policies, and essential ingredients underlying the fiduciary relationship.¹⁰⁷

The Constituent Elements of Fact-Based Fiduciary Relationships

Ever since the Supreme Court of Canada's decision in *Lac Minerals Ltd. v. International Corona Resources Ltd.*,¹⁰⁸ most fact-based fiduciary inquiries begin with an acknowledgment of the approach adopted by Wilson J. in *Frame v. Smith*:

There are common features discernible in the contexts in which fiduciary duties have been found to exist and these common features do provide a rough and ready guide to whether the imposition of a fiduciary obligation on a new relationship would be appropriate and consistent.

Relationships in which a fiduciary obligation have been imposed seem to possess three general characteristics:

- 1 The fiduciary has scope for the exercise of some discretion or power.
- 2 The fiduciary can unilaterally exercise that power or discretion so as to affect the beneficiary's legal or practical interests.
- 3 The beneficiary is peculiarly vulnerable to or at the mercy of the fiduciary holding the discretion or power.

It is possible for a fiduciary relationship to be found although not all these characteristics are present ... [however] the presence of conduct that incurs the censure of a court of equity ... cannot itself create the duty.¹⁰⁹

Sopinka J. also identified "depending or vulnerability" as the one characteristic that was indispensable to the existence of a fiduciary relationship. LaForest J. dissented on the issue of vulnerability, finding that vulnerability, though often present in fiduciary relationships, is not a necessary ingredient. The indispensability of depending or vulnerability remained unchallenged until the Supreme Court of Canada's decision in *Hodgkinson v. Simms*.¹¹⁰

In his majority judgment in *Hodgkinson v. Simms*, LaForest J. restated and reasserted his earlier position from *Lac Minerals* that vulnerability is not a requisite part of every fiduciary relationship, stating that "the concept of vulnerability is not the hallmark of fiduciary relationship though it is an important indicia of its existence. Vulnerability is

common to many relationships in which the law will intervene to protect one of the parties ... while the doctrine of unconscionability is triggered by abuse of a pre-existing inequality in bargaining power between the parties, such an inequality is no more a necessary element in a fiduciary relationship than factors such as trust and loyalty are necessary conditions for a claim of unconscionability." After reviewing *Guerin v. R.* and *Frame v. Smith*, LaForest J. concluded that a fact-based fiduciary relationship exists where "there is evidence of a mutual understanding that one party has relinquished its own self-interest and agreed to act solely on behalf of the other party."¹¹² He reiterated that the oft-quoted dicta of Wilson J. is merely "a rough and ready guide in identifying new categories of fiduciary relationships,"¹¹³ describing her three general characteristics as "indicia that help recognize a fiduciary relationship rather than ingredients that define it."¹¹⁴ According to LaForest J., "the question to ask is whether, given all the surrounding circumstances, *one party could reasonably have expected that the other party would act in the former's best interests with respect to the subject-matter at issue.* Discretion, influence, vulnerability and trust [are] non-exhaustive examples of evidential factors to be considered in making this determination."¹¹⁵ Similar remarks have been made by legal scholars. For example, P.D. Finn has argued that:

What must be shown is that the actual circumstances of a relationship are such that *one party is entitled to expect that the other will act in his interests and for the purposes of the relationship.* Ascendancy, influence, vulnerability, trust, confidence or dependence doubtless will be of importance in making this out. But they will be important only to the extent that they evidence a relationship suggesting that entitlement. It must so align him with the protection or advancement of that other's interests that foundation exists for *the fiduciary expectation.*¹¹⁶

The requirement of a fiduciary expectation might be understood as a kind of judicial roadblock. It is meant to preclude a court from imposing fiduciary relationships *solely* on the basis that one party is vulnerable or dependent on another. As one judge readily acknowledged:

The word "fiduciary" is flung around now as if it applied to all breaches of duty by solicitors, directors of corporations and so forth. But "fiduciary" comes from the Latin "*fiducia*" meaning "trust." Thus, the adjective "fiduciary" means of or pertaining to a trustee or trusteeship. That a lawyer can commit a breach of the special duty of a trustee, eg ... by

entering into a contract with the client without full disclosure ... is clear. But to say that simple carelessness in giving advice is such a breach is a perversion of words.¹¹⁷

Other critics also share this point of view. Welling, for example, has suggested that "the time has come to rein in runaway fiduciary duties."¹¹⁸ As Welling has argued: "Kidnappers don't owe fiduciary obligations merely because they can physically overpower their trussed up captives. A fiduciary is someone in a position of *legally* condoned power who can affect the legal position of someone else by *legal* means and who, *for those reasons*, is obliged to consider the best interests of that other person before doing so."¹¹⁹ Through a judicial recognition that the basis for establishing a fiduciary relationship is more than just proving a relationship of dependence, Welling trusts that the court "has man-aged to stop the trendy nonsense by which every bit of corporate or professional nastiness became labeled a breach of fiduciary obligation."¹²⁰

Those who share this point of view believe that "equity's blunt tool must be reserved for situations that are truly in need of the special protection that equity affords."¹²¹ On this basis, some courts have been reluctant to find a fiduciary duty within an arm's length commercial transaction. Where the parties have had an adequate opportunity to prescribe their own mutual obligations, it is usually thought that contractual remedies will suffice.¹²² This point has been recognized in a number of cases. As articulated by Dawson J. in *Hospital Products Ltd. v. United States Surgical Corp.*:

The undesirability of extending fiduciary duties to commercial relationships and the anomaly of imposing those duties where the parties are at arm's length from one another was referred to in *Weinberger v. Kendrick* (1892) 34 Fed Rules Serv. (2d) 450. And in *Barnes v. Addy* (1874) 9 Ch. App. 244 at 251, Lord Selborne LC said: "It is equally important to maintain the doctrine of trusts which is established in this court, and not to strain it by unreasonable construction beyond its due and proper limits. There would be no better mode of undermining the sound doctrines of equity than to make unreasonable and inequitable applications of them."¹²³

To quickly recap, it would seem that a proper judicial inquiry into the existence of a fact-based fiduciary obligation will include a number of constituent elements. First, the inquiry will consider all of the traditional hallmarks, including: whether the trusted party was in a position

to unilaterally exercise a power or discretion; whether the trusted party was thereby able to affect the trusting party's legal interests; and whether, as a result, the trusting party was at the mercy of the trusted party. Second, recognizing dependency as a necessary though not a sufficient condition, a proper inquiry will determine whether the trusting party is entitled to expect that the trusted party will act in his interests and for the purposes of the relationship. Presumably, this would require a demonstration that the relationship between the parties exists primarily for the benefit of the trusting party. On this basis, Canadian courts are far less likely to impose a fiduciary obligation in the case of a commercial transaction at arm's length.

ISP-USER RELATIONSHIPS

Is the relationship between Internet service provider and user *merely a* relationship at arm's length? Or is it a relationship the nature of which might lead a court to impose special duties of loyalty on the part of the service provider? It should by now be evident that the manner in which these two questions have been posed is problematic. Since ISP-user relationships obviously are not within the traditional categories of fiduciary relationships, the answer will hang entirely on the specific facts underlying the parties' particular interaction. Given the inexhaustible range of available Internet services, the majority of which are governed by the private orderings of the parties, there will never be a single generalizable answer.

The better question is whether an ISP could *ever* be said to be a fiduciary. Without a doubt, a number of the constituent elements are present in many ISP-user relationships. As we have seen, Internet users are very often in a relationship of dependence on their service providers. The current architectures of the networked world allow ISPs access to their users' personal information and private communications in a manner unparalleled by even the most powerful financial institutions or arms of government. Access to these assets allows ISPs to exercise power to the benefit or detriment of their users. As we have seen, not only does this allow ISPs to control user behaviour, in some cases, it allows them to hold control over the destiny of their users. To paraphrase Weinrib, there are times when an ISP has the leeway to affect the legal position of its user, putting the latter at the mercy of the former. An ISP acting *male fides* has access and therefore could: convert a user's private communications to its own or to another's advantage; disclose confidential information to a competitor; or turn over otherwise privileged evidence in the course of criminal or private litigation, etc.

At the same time, it is not clear that the services offered by most ISPs are ever undertaken with a view towards acting primarily to the benefit of their users, let alone to their exclusive benefit. To take an extreme example, an employer who provides Internet services does not generally undertake to do so exclusively for the benefit of its employees. Offering such services to employees is but a means to the corporation's own ends. Even the most benevolent employer (whose policy permits employees to utilize its Internet services for personal use) does not offer such services for the exclusive benefit of the employees. If an employee uses those services to illicit ends or in any other manner that is not in the best interests of the corporation, how could it possibly be said that the employer is obligated to use the evidence that it has gathered to serve the employee's benefit, rather than serving the best interests of the corporation? In what meaningful sense can the employee be said to have expected a duty of loyalty from his employer that would trump its own corporate interests?

Similar arguments could be made in a number of other circumstances contemplated earlier in this chapter ("The Contractual Underpinnings of ISP-User Relationships"). Such circumstances will arise whenever an ISP has given clear notice that its allegiances are *not always* with its users. According to the broad categories of ISP contractual undertakings outlined earlier, this could occur when an ISP states in its contract that it will: (1) disclose whenever illegality is suspected; (2) disclose to protect the ISP or in extraordinary circumstances; or (3) volunteer disclosure and actively monitor.

These three categories of contractual undertakings are contemplated to be at arm's length. The case of *Weir*¹²⁴ discussed earlier ("The Gate-keepers") furnishes a useful illustration. Recall that Supernet's "Accept-able Use Policy and Liability Disclaimer" provided that it "will report to law enforcement authorities *any actions which may be considered illegal*, as well as any reports it receives of such conduct. When requested, [Supernet] will fully cooperate with law enforcement agencies in any investigation of alleged illegal activity on the Internet."¹²⁵ On the basis of signing this agreement, which explicitly stated that Supernet's loyalty was limited whenever illegality is suspected, is there any credible basis for Weir to assert that he believed his relationship with Supernet to be one in which he was entitled to expect that Supernet would act in his interests and for the purposes of the relationship? Could he possibly have thought that his ISP would remain loyal to him once it had in-advertently discovered that he was a regular consumer and distributor of child pornography?

The conclusion to be drawn from the above examples is not that ISP-user relationships are *always* at arm's length. In fact, other cases like *Aquacool_2000 v. Yahoo! Inc.*¹²⁶ raise interesting possibilities. What happens when a service provider holds itself out as "committed to safe-guarding your privacy online" and explicitly undertakes to notify you "at the time of data collection or transfer if your data will be shared with a third party," promising all the while that "you will have the option of not permitting the transfer," backing up each of these promises with certification representing that the service provider complies with the highest standards of trust and confidence on the Internet?¹²⁷ Further, what if the ISP is contemplating the transfer of your personal information, not for the purposes of legitimate law enforcement, but because of some corporate inducement to assist another corporation in its private crusade against its critics? In such a case, should the alleged facts prove to be true, there is an argument to be made that all of the constituent elements of a fiduciary relationship are present. In addition to the ISP's access to the user's personal information and private communications and its leeway to exercise discretion and thereby transfer user assets to the user's detriment, the alleged facts also support a characterization of a relationship that entitles the user to expect that his service provider will treat his personal information and private communications in a manner that comports with his interests.

If this is correct, then the idea that some ISPs might be held to owe their users a duty of loyalty with respect to the care and control of user information is an increasingly important consideration. In fact, the idea of ISP-as-fiduciary might become even more plausible as network technology (NT) becomes more advanced. Some Internet visionaries predict a networked world in which virtually all information is stored on Internet servers, manipulated through personal information management applications, and accessed through Internet appliances.¹²⁸ For example,

Larry Ellison, CEO of Oracle Corporation believes that soon, personal computers will be replaced by new devices that rely almost exclusively on fast networks and have very little intelligence inside. "Fast, cheap networks mean computers will cost \$500, not \$5,000." He dubbed the new devices network computers, or NCs, as opposed to today's personal computers. Network computers and similar devices, such as the interactive video set-top box, contain almost no software, just a basic input/output system, and download a complete operating system when switched on. This whole process takes only seconds to complete ... In a world full of cheap, almost disposable, network computers, users will

be able to carry a smart card to allow access to the network. Because all programs are downloaded from the network, and because everyone's personal data files and backups are stored on servers connected to the system it will be possible to slide a card into any NC and instantly begin work, as if the user were at home using their own machine.¹²⁹

As Ellison himself described it, "network computers will not replace PCs, just as PCs didn't replace mainframes. But network computers will be the center of the world."¹³⁰

If something like Ellison's vision becomes reality, the centre of the world will be wherever the leaders of NT choose to build it. Wherever that turns out to be, the end result is the same: the storage and management of all information will take place far away from the user. In a world where people have little or no control over the flow of their own information, users will be completely dependent on information service providers. Information service providers and information managers will become the stewards of personal information and private communications. In such a world, it would seem only reasonable to expect that the management of such information would be carried out in the best interests of the users. Thus, in a fully networked world, the relationships between information service providers and their users bear a much greater resemblance to a fiduciary relationship than they do to a relationship at arm's length.

CONCLUSION

ISPs are our gatekeepers. More and more, we come to rely on ISPs, not only to provide quality information services, but also to manage our information. By controlling an asset that is characterized more and more as the new currency of the so-called *knowledge economy*,¹³¹ users depend on ISPs to safeguard their personal information and private communications. This gives ISPs power over their users: power to control their behaviour; power to alter their outcomes.

Currently, relationships between ISP and user are governed primarily by the law of contract. Given the increasing extent to which users re-pose trust and confidence in their ISPs, it is unclear whether the legal duties owed by ISPs to their users are also subject to the equitable principles governing the law of fiduciaries. It has been suggested here that this possibility is an increasingly important consideration. While it would be wrongheaded to conclude that ISPs are *always* fiduciaries — as if we could somehow generalize about a motley collection of private orderings — it would be equally misguided to conclude that ISPs are *never*

fiduciaries. The conclusion offered here is more modest than either of these. It is simply that *some* ISP-user relationships display all of the constituent elements of a fiduciary relationship.

ACKNOWLEDGEMENTS

I would like to thank the Canadian Association of Law Teachers, the Canadian Law and Society Association, the Canadian Council of Law Deans, and the Law Commission of Canada for their generous contribution to the funding of this project. I would also like to convey my deepest gratitude to David Arntfield, Marcus Bronfreund, John Hoben, Karen G. McCulloch, and Bernard Sandler for all of their extraordinary efforts and for the high quality of research assistance that they provided.

NOTES

1 Yahoo!'s global audience is said to have grown to more than 145 million unique users worldwide, including 14 million users in Japan. Yahoo!'s global registration base has grown to more than 125 million cumulative registrations for Yahoo! member services. The company's traffic increased to a record 625 million page views per day on average during March 2000, online: Yahoo! <<http://docs.yahoo.com/docs/pr/lg00pr.html>> (last modified: 5 April 2000); see also G. Fontaine, "Internet Portals" online: idate <<http://www.idate.fr/maj/multi/lpi/lpi.pdf>> (last modified: 1 February 2000). This 1999 study revealed, inter alia, that Yahoo! was, at that time, the second largest portal, AOL being the largest. <<http://vwww.internetwk.com/newsO199/newsO12299-9.htm>>.

2 See recently filed *Aquacool_2000 v. Yahoo! Inc.* at United States District Court Central District of California (Plaintiff's complaint at para. 6) [hereinafter *Aquacool_2000*], online: Electronic Privacy Information Centre <http://www.epic.org/anonymity/aquacool_complaint.pdf> (last modified: 20 May 2000).

3 *Ibid.* at para. 7.97.

4 In order to subscribe to Yahoo!, a user must provide, inter alia, his zip code, gender, occupation, industry, and interests.

5 The US Supreme Court has firmly held that the First Amendment protects anonymous speech. See *McIntyre v. Ohio Elections Commission* (1995), 514 U.S. 334.

6 Macromedia is a graphics design company that specializes in dynamic web content. Plug-ins are computer applications that enhance a base program. In this case, the plug-in is used to enhance the user's web browser to allow it to view specialized content. See online: Macromedia <<http://www.macromedia.com/>> (date accessed: 21 May 2000).

7 See "What's in Them Cookies? Web Site Is Finding Out." *Privacy Times* (15 February 1999) at 1. online: *Privacy Times* <<http://www.privacytimes.com>>.

8 See online: DoubleClick <<http://www.doubleclick.net>> (date accessed: 21 May 2000).

9 *Ibid.*

10 Single quotation marks are used to indicate a qualified sense of the word voluntary. The architecture of the subscription routine in fact requires the disclosure of the requested information. It is, in the truest sense, a contract of adhesion. The failure to provide the relevant information will block the user's access to the

service portal. The only possible way that an individual could gain access to Yahoo! services without providing the information sought is to fraudulently enter false information into the Yahoo! system.

11 An IP address is the unique number assigned to an individual's computer by that user's ISP. It allows other computers to communicate with that computer directly, bypassing some of the delay of more tortuous routing. It can be set to change each time the user logs on to the ISP or remain constant throughout the user's dealings with the ISP. See Matisse Enzer, "Glossary of Internet Terms" (1996 - 2000), online: Matisse <<http://www.matisse.net/files/glossary.html>> (last modified: 4 May 2000); J.R. Levine and C. Baroudi, *The Internet for Dummies* (San Mateo, Calif.: IDG Books, 1994).

12 Cryptography is the means by which messages may be hidden or disguised in files such that they may not be accessed by the general public or may be con-firmed as to have come from a particular source. "It works by mathematically transforming a plaintext (or cleartext) message or file into a disguised ciphertext, a process known as encryption. Decryption involves turning the ciphertext back into plaintext." See online: PC Guardian <http://www.pcgardian.com/software/encryption_faq.htm> (last modified: 9 May 2000).

13 Of course, encryption would be pointless for those, like Aquacool_2000, who wish to make pseudonymous public commentary. See e.g. G. Greenleaf and Roger Clarke, "Privacy Implications of Digital Signatures" (IBC Conference on Digital Signatures, Sydney, Australia, 12 March 1997), online: Privacy Implications of Digital Signatures <<http://www.anu.edu.au/people/Roger.Clarke/DV/DigSig.html>> (last modified: 10 March 1997). See also Pretty Good Privacy, online: PGP Security <<http://www.pgp.com/>> (date accessed: 17 May 2000).

14 *Aquacool_2001*, *supra* note 2 at para. 26.

15 See online: Yahoo! Privacy Policy <<http://docs.yahoo.com/info/privacy>> (last modified: 15 April 1994).

16 *Ibid.*

17 *Ibid.*

18 *Ibid.*

19 TRUSTe is an independent, nonprofit privacy initiative dedicated to building users' trust and confidence in the Internet and accelerating growth of the Internet industry. TRUSTe has developed a third-party oversight "seal" program that alleviates users' concerns about online privacy, while meeting the specific business needs of each of its licensed Web sites. Were Yahoo! to breach its privacy commitments, it would lose its certification. Thus far, it remains certified. See particular verification for Yahoo! online: Truste Validation Page <<http://www.truste.org/validate/361>> (date accessed: 17 May 2000). See also online: Truste <<http://www.truste.org/>> (last modified: 24 April 2000).

20 *Aquacool_2001*, *supra* note 2 at para. 23.

21 Geocities is a Web hosting company that purports to build communities of interest. Their site is divided into various "neighbourhoods." A user can choose the location of his individualized site and communicate with like-minded others in the neighbourhood. Geocities also maintains mailing lists known as "clubs." These forums, moderated by other Geocities members, exist to enhance the community feel of Geocities. Geocities is currently owned by Yahoo! and is located online: Yahoo! Geocities <<http://www.geocities.com>> (last modified: 21 May 2000).

22 "FTC Takes Action on Privacy Enforcement" *McBride Baker & Coles: ITEC LAW ALERT* 8:5 (October 1998), online: ITEC Law Alert <<http://www.mbc.com/newsletters/itec/newsin85.html>> (last modified: 21 December 1999).

23 D. Radcliff, "Companies Struggle with Privacy on the Web" *CNN* (20 May 1999), online: CNN <<http://cnn.com/TECH/computing/9905/20/privacy.idg>> (last modified: 21 May 2000).

24 For a more detailed account of this case, see D.M. McTigue, "Marginalizing Individual Privacy on the Internet" (1999) 5 B.U. J. SCI. & TECH. L. 5 at para. 6-16.

25 See *R. v. Weir* (1998), 213 A.R. 285 (Q.B.), leave to appeal to Alta. C.A. granted [1999] Alta. C.A. 275.

26 *Canadian Charter of Rights and Freedoms*, s. 8, Part I of the *Constitution Act*, 1982, being Schedule B to the *Canada Act 1982 (U.K.)*, 1982, c. 11.

27 Bill C-6, *Personal Information and Electronic Documents Act*, 2d Sess., 36th Parl., 1999, (assented to 13 April 2000, R.S.C. 2000, c. 5) [hereinafter *Bill C-6*]. See online: <http://www.parl.gc.ca/36/2/parbus/chambus/house/bills/government/C-6/C-6_4/C-6TOCE.html> (date accessed: 14 May 2000).

28 Bruce Phillips, "The Evolution of Canada's Privacy Laws" (Canadian Bar Association – Ontario Institute, Toronto, Ontario, 28 January 2000), online: Privacy Commission of Canada <http://www.privcom.gc.ca/english/02_05_a_000128_e.htm> (last modified: 18 April 2000).

29 Of course, these categories are neither mutually exclusive nor jointly exhaustive.

30 See online: The Spark.com Purity Test <<http://test.thespark.com/puritytest>> (last modified: 9 April 2000).

31 See online: The Joe Cartoon Co. <<http://www.joecartoon.com>> (last modified: 17 May 2000).

32 See online: Mortgage Analyzer Calculator <<http://www.themortgage.com/quickcalc.html>> (last modified: 18 April 2000).

33 See I.R. Kerr, "Spirits in the Material World: Intelligent Agents as Intermediaries in Electronic Commerce" (1999) 22 Dal. L. J. 1; S. Segal et al., "The Validity and Enforceability of Web-Wrap Agreements and Assessing the Need for Legislation" (Uniform Law Conference of Canada, May 1999), online: Uniform Law Conference <<http://www.law.ualberta.ca/alri/ulc>> (last modified: 7 June 1999); F.M. Buono and J.A. Friedman, "Maximizing the Enforceability of Click-Wrap Agreements" (1999) 43 J. Tech. L. & Pol'y 3; J.C. Lin et al., "Electronic Commerce: Using Clickwrap Agreements" (1998) 15 Computer Law 10; J.S. Gale, "Service Over the 'Net': Principles of Contract Law in Conflict" (1999) 49 Case W. Res. L. Rev. 567; D. Mirchin, "Online Contracts" (1999) 563 PLI/Pat. 351.; T.J. Smedinghoff, "Electronic Contracts and Digital Signatures: An Overview of Law and Legislation" (1999) PLI/Pat 125.

34 See Lin et al., *supra* note 33; R.C. Balough, "Drafting Contract Provisions for E-s Commerce Sites" (2000) 88 Ill. B.J. 40.; Mirchin, *supra* note 33; Gale, *supra* note 33; Smedinghoff, *supra* note 33.

35 See T.J. Smedinghoff, ed., *Online Law* (USA: A-W Developers Press, 1996) at para. 6.2; R.T. Nimmer, "UCITA: A Modern Contract Law for a Modern Information Economy" (1999) 574 PLI/Pat 221; US, National Conference of Commissioners on Uniform State Laws, *Uniform Computer Information Transactions Act* (draft approved 30 July 1999) [hereinafter *UCITA*], online: Uniform Law Commissioners <<http://law.upenn.edu/bl/ulc/ucita/cita10st.htm>> (last modified: 25 October 1999); US, National Conference of Commissioners of Uniform State Laws,

Uniform Electronic Transactions Act (draft approved 30 July 1999) at s.9 [hereinafter *UETA*], online: Uniform Law Commissioners <<http://www.law.upenn.edu/bll/ulc/uecicta/uetast84.htm>> (last modified: 26 October 1999); Canada, Uniform Law Conference of Canada, *Part 3: Uniform Electronic Commerce Act* (draft August 1999) at art. 20-23 [hereinafter *UECA*], online: Uniform Law Conference of Canada <<http://www.law.ualberta.ca/alri/ulc/current/euecafa.htm>> (last modified: 23 November 1999); *Uncitral Model Law on Electronic Commerce*, GA Res. 51/162, UN GAOR, 51st Sess., UN Doc. A/51/628, (1997) at IA6, online: UNCITRAL <<http://www.uncitral.org/english/texts/electcom/mlec.htm>> (last modified: 29 January 1999).

36 See Segal, *supra* note 33; Smedinghoff, *supra* note 35. See also *UCITA*, *ibid.* at s. 107.

37 Anyone who has conducted even the briefest appraisal of online user agreements will immediately recognize this assumption to be false. Most graphical interfaces for ISP "Terms of Service" are poorly designed and would probably be unenforceable according to *ratio* in *Tilden Rent-A-Car v. Clendenning* (1978), 18 O.R. (2d) 601 (Ont. C.A.). According to the court, an onerous or unusual clause is unenforceable in spite of a signature if the party seeking to enforce the clause fails to provide the other party with reasonable notice of its incorporation.

38 The list of ISP "Terms of Service" considered in this study included: online: Athome.com and Atnetwork.com <<http://www.athome.com>> (last modified: 28 April 2000); online: Acadia University <<http://www.acadiau.ca/cs/pubdocs/policies.html>> (last modified: 8 April 1998); online: Alberta Supernet <<http://www.supernet.ab.ca>> (last modified: 25 March 2000); online: AOL <<http://www.aol.com/copyright.html>> (last modified: 20 January 2000); online: AT&T Business <<http://www.attbusiness.net/terms/index.html>> (last modified: 15 March 2000); online: AT&T Canada <<http://www.attcanada.ca/about/ncterms.html>> (last modified: 16 May 2000); online: Bluelight.com <<http://bluelight.com/company.privacy.shtml>> (date accessed: 22 May 2000); online: Canada.com <<http://www.canada.com/members/register.asp?/home>> (date accessed: 22 May 2000); online: Concentric <http://www.concentric.com/privacy_policy.html> (last modified: 27 March 2000); online: Cyberlink <http://webservices.cyberlink.be.ca/acceptable_use_policy.html> (last modified: 27 February 2000); online: Demon <<http://www.demon.net/info/helpdesk/aup/access.shtml>> (date accessed: 22 May 2000); online: DeVRY <<http://www.devry.ca/index.htm>> (last modified: 22 December 1999); online: DirecPC <<http://www.direcpc.com>> (last modified: 19 May 2000); online: Geomail <<http://www.geocities.com/svcagreement.htm>> (date accessed: 22 May 2000); online: Globix <<http://www.globix.com/support/aup.html>> (last modified: 14 April 2000); online: Imaginet <<http://www.express.ca>> (last modified: 15 May 2000); online: Inforoute (English) <<http://www.inforoute.net/terms.html>> or (Francais) <<http://www.inforoute.net/francais/terms.html>> (last modified: 19 December 1999); online: Interlog <<http://www.interlog.com/terms.html>> (date accessed: 22 May 2000); online: iPrimus <<http://www.iprimus.ca/personal/terms/acceptable.htm>> (last modified: 23 March 2000); online: Magma <<http://www10.magma.ca/services/corporate/hosting/faq/acceptable%SFfaq.html>> <<http://www.magma.ca>> (last modified: 2 March 2000); online: Mindspring <<http://www.mindspring.com/aboutms/aup.html>> (last modified: 28 March 2000); online: MSN Hotmail <<http://www.hotmail.msn.com>> (date accessed: 22 May 2000); online:

Muskoka.com <<http://www.muskoka.com/conditions.html>> (last modified: 8 May 1999); online: NBTe1 (NBNet) <<http://www.nbnet.nb.ca/connect/accuse.shtml>> (last modified: 20 January 1999); online: Nipissing University <<http://kenm.unipissing.ca/uts/pollan.htm>> (last modified: 29 September 1999); online: Pangea <<http://www.pangea.ca/policy.html>> (last modified: 13 March 2000); online: Sprint Canada <www.sprintcanada.ca/English/Terms.asp?Section=FORHOME> (last modified: 7 December 1999); online: Sympatico <<http://wwwl.sympatico.ca/help/About/serviceagree.html>> (date accessed: 22 May 2000); online: Telus (a subsidiary of BCTel) <<http://www.telus.com>> (last modified: 17 October 1999); online: Toronto Free-Net <<http://freenet.toronto.on.ca>> (last modified: 15 May 2000); online: University of Alberta <<http://www.ualberta.ca/CNS/POLICY/Conditions.html>> (last modified: 15 January 1998); online: University of Toronto <<http://www.utoronto.ca/welcome.html/utordist/general/utormail.html#eligible>> (last modified: 17 January 2000); online: UWO <<http://www.uwo.ca/its/ftp/nic/security/AUP.html>> (last modified: 10 October 1997); online: Verio <<http://home.verio.com/company/aup.cfm>> (date accessed: 22 May 2000); online: Yahoo! <<http://docs.yahoo.com/info/terms>> (date accessed: 22 May 2000).

39 The survey included international service providers (who offer their services worldwide through the use of local/national dial-up numbers into their international backbone); American service providers (who operate in Canada through either a North American backbone or through independent subsidiary providers in each country); Canadian national service providers (who offer nationwide services over a national backbone); Canadian provincial service providers (many of which are more accurately described as "regional providers"); and Canadian noncommercial/ institutional service providers (including various "Free-Nets," and government and university service providers); and workplace service providers (who may use any of the above service providers).

40 Of course, these categories are neither mutually exclusive nor jointly exhaustive.

41 See generally, N. Levine, "Establishing Legal Accountability for Anonymous Communication in Cyberspace" (1996) 96 Colum. L. Rev. 1526.

42 L. Detweiler, "Anonymity on the Internet" (13 May 1993) at 1.1, online: Electronic Frontier Foundation <<http://www.eff.org/pub/privacy/Anonymity/netanonymity.faq>> (last modified: 11 May 1994).

43 See J. Quittner, "Requiem for a Go-Between" *Time* (16 September 1996) 75; Levine, *supra* note 41 at 1532.

44 Bill C-231, *Internet Child Pornography Prevention Act*, 2d Sess., 36th Parl., 1999, (1st reading 18 October 1999).

45 *Ibid.* at s. 6 (3)(c).

46 *Supra* note 44.

47 See Levine, *supra* note 41 at 1563. See also US, International Trade Administration Electronic Commerce Task Force, *International Safe Harbour Privacy Principles* (19 April 1999), online: US, International Trade Administration <<http://www.ita.doc.gov/td/ecom/shprin.html>> (last modified: 2 December 1999).

48 Levine, *ibid.*

49 American legislators have taken a similar tack. See e.g. the *Digital Millennium Copyright Act*, Pub. L. No. 105-304, 112 Stat. 2860 (1998), specifically Title II: Online Copyright Infringement Liability Limitation.

50 J. Sopinka, "Freedom of Speech and Privacy in the Information Age" (1997) 13 *The Information Society* 171 at 178-79 (emphasis added).

51 *Bill C-6*, *supra* note 27.

52 *Ibid.* at s. 7 permits an ISP to disclose without liability, which is different from requiring it to disclose *in order to avoid liability*.

53 It is unclear whether this federally enacted statute applies to Internet service providers. *Ibid.* at s. 4(1) provides that the *Act* "applies to every organization in respect of personal information that ... the organization collects, uses or discloses in the course of commercial activities." Though the *Act* is silent on whether it is meant to apply to Internet service providers, the Canadian Industrial Relations Board has recently ruled that the ISP division of Island Tel operated much like a telephone company and is therefore a federally regulated business: *Re Island Telecom Inc.* (2000), C.I.R.B.D. No. 12 (CIRBD Decision No. 59) [hereinafter *Island Tel*]. If the *Island Tel* ruling is adhered to, then *Bill C-6* will likely apply to ISPs.

54 *Supra* note 27 at s. 7(2)(a).

55 See online: University of Calgary Computing and Networks Policy <<http://www.ucalgary.ca/ucs>> (last modified: 7 September 1999).

56 See online: Demon Internet Access <<http://www.demon.net/info/helpdesk/aup/access.shtml>> (date accessed: 23 May 2000).

57 See online: America Online Rules of User Conduct <<http://www.aol.com/copyright/rules.html>> (last modified: 20 January 2000).

58 What makes the *Aquacool_2000* case controversial is the fact that Yahoo! represented its approach much differently in its "Terms of Service" document. According to its "Terms of Service," Yahoo! promised an approach more closely aligned with the category "Confidential within the Limits of the Law."

59 See online: Alberta Supernet <<http://www.supernet.ab.ca>> (last modified: 25 March 2000) (emphasis added). See also Sprint Canada's "General Terms of Service," which state that Sprint will provide "disclosure pursuant to a requirement or request of a government agency, subpoena or other legal proceeding, or disclosure required by law." See online: Sprint Canada <<http://www.sprintcanada.ca/English/Terms.asp?Section=FORHOME>> (date accessed: 23 May 2000).

60 Pursuant to s. 7(2)(b) of *Bill C-6*, *supra* note 27, disclosure of personal information for these sorts of reasons is also permitted.

61 See online: Verio Acceptable Use Policy <<http://home.verio.com/company/aup.cfm>> (date accessed: 23 May 2000).

62 See online: Muskoka.com Terms and Conditions <<http://www.muskoka.com/conditions.html>> (last modified: 8 May 1999).

63 J.C. McWhinnie, "The Internet and the Law" (10 January 2000), see online: <http://www.hawaiilawyer.com/articles/internetlaw_article_jcm.htm> (last modified: 8 May 2000).

64 See online: ICQ's Terms of Service <<http://www.icq.com/legal/ircqnet.html>> (date accessed: 23 May 2000).

65 E.g. the relationship between a commercial agent and principal or the relationship between solicitor and client.

66 L.A. Penner, "Interdependent Social Behavior," in *Social Psychology: Concepts and Applications* (St. Paul: West Publishing, 1986) 514.

67 See generally J.W. Thibaut and H.H. Kelley, *Interpersonal Relations: A Theory of Interdependence* (New York: Wiley-Interscience, 1978).

68 C.R. Agnew, P.A.M. Van Lange, C.E. Rusbult, and C.A. Langston, "Cognitive Inter-dependence: Commitment and the Mental Representation of Close Relationships" (1998) 74 *Journal of Personality and Social Psychology* 939 at 940.

69 J.W. Thibaut and H.H. Kelley, *The Social Psychology of Groups* (New York: Wiley-Interscience, 1978) at 124.

70 R.M. Emerson, "Power-Dependence Relations" (1962) 27 *American Sociological Review* 31.

71 See also K.S. Crook and M.R. Gillmore, "Power, Dependence and Coalitions," in E.J. Lawler and B. Markovsky, eds., *Social Psychology of Groups: A Reader* (Greenwich: JAI Press, 1993) 127.

72 Thibaut and Kelley, *supra* note 69 at 124.

73 *Ibid.*

74 C.E. Rusbult, "A Longitudinal Test of the Investment Model: The Development (and Deterioration) of Satisfaction and Commitment in Heterosexual Involvements" (1983) 45 *Journal of Personality and Social Psychology* 101.

75 Agnew et al., *supra* note 68 at 940.

76 Penner, *supra* note 66 at 515.

77 Agnew et al., *supra* note 68 at 940 (emphasis in the original). For an interesting application of the concept of commitment to the information technology setting, see S. Yoon, "User Commitment as an Indicator of Information Technology Use" (Association for Information Systems - Americas Conference, Phoenix, Arizona, 16 August 1996) [unpublished], online: Association for Information Systems - Americas Conference <<http://hsb.baylor.edu/ramsower/ais.ac.96/papers/yoon.htm>> (last modified: 27 September 1997).

78 Agnew et al., *ibid.*

79 Strictly speaking, not all Internet users are dependent on ISPs for access. Users with sufficient resources (i.e., cash and know-how) can purchase equipment that would give them access to the Internet without the need for developing a relationship with an ISP.

80 Especially when one considers some of the Internet services that are currently popular; e.g., cybersex forums, chat rooms, and online auctions.

81 See online: Integrated Justice Project <<http://www.integratedjustice.gov.on.ca/>> (last modified: 16 May 2000); See also G.J. Cohen, "Ontario's Integrated Justice Project" *Canadian Lawyer* (January 1999) at 19.

82 P.M. Schwartz, "Privacy and Democracy in Cyberspace" (1999) 52 *Vanderbilt Law Review* 1609 at 1619.

83 See e.g. online: Toronto Free-Net <<http://www.freenet.toronto.on.ca>> (last modified: 15 May 2000).

84 Including, as we shall see below (in Relationships of Dependence and Interdependence), promoting its own interests at the expense of the user's interests.

85 Even though some users *may perceive* themselves as *committed* to a particular service provider.

86 For an interesting application of interdependence in the context of group rights, see D.M. Johnston, "Native Rights as Collective Rights: A Question of Group Self-Preservation" (1989) 2 *Can. J. Law & Jur.* 19.

87 Schwartz, *supra* note 82 at 1620: "Network externalities are found in any product whose value depends on how many others make use of it; the more people who send and receive e-mail, for example, the more valuable it becomes for others to utilize this technology."

88 See e.g. *Welles v. Middleton* (1784), 1 Cox 112 at 124-25; *Parker v. McKenna* (1874), L.R. 10 Ch. 96 at 125.

89 *Billage v. Southee* (1852), 9 Hare 534 at 540.

90 R. Flannigan, "The Fiduciary Obligation" (1989) 9 Oxford J. Leg. St. 285 at 322.

91 See e.g. *Goldex Mines Ltd. v. Reville* (1974), 7 O.R. (2d) 216 at 224, 54 D.L.R. 672 (Ont. C.A.); *Guerin v. R.* (1984), 13 D.L.R. (4th) 321 at 340-341 (S.C.C.) [herein-after *Guerin*].

92 E.J. Weinrib, "The Fiduciary Obligation" (1975) 25 U.T.L.J. 1 at 11 (emphasis added).

93 See also L.I. Rotman, "Fiduciary Doctrine: A Concept in Need of Understanding" (1996) 34 Alta. L. R. 821 at 826.

94 Per LaForest J. in *Lac Minerals Ltd. v. International Corona Resources Ltd.* (1989), 61 D.L.R. (4th) 14 (S.C.C.).

95 D.W.M. Waters, *Law of Trusts in Canada*, 2d ed. (Toronto: Carswell, 1984) at 710-15.

96 Weinrib, *supra* note 92 at 4-5.

97 Flannigan, *supra* note 90 at 287.

98 Weinrib, *supra* note 92 at 7.

99 Flannigan, *supra* note 90 at 308.

100 Rotman, *supra* note 93 at 825.

101 See e.g. Flannigan, *supra* note 90 at 294.

102 B. Welling, "Former Corporate Managers" (1990) 31 Les Cahiers de Droit 1075 at 1097.

103 Weinrib, *supra* note 92 at 5.

104 *Guerin*, *supra* note 91; see also *Frame v. Smith* (1987), 42 D.L.R. (4th) 81 at 97 (S.C.C.).

105 *Guerin*, *ibid.* at 341.

106 *Hodgkinson v. Simms* (1994), 117 D.L.R. (4th) 161 at 179-180 (S.C.C.).

107 See e.g. *Canadian Aero Service Ltd. v. O'Malley* (1973), 40 D.L.R. (3d) 371 (S.C.C.) (senior corporate officers/directors to corporation); *Jima Ltd. v. Mister Donut of Canada Ltd.* (1973), 40 D.L.R. (3d) 303 (S.C.C.) (franchiser to franchisee); *Guerin*, *supra* note 91 (federal government to Indian band); *Frame v. Smith*, *supra* note 104 (custodial parent to noncustodial parent); *Molchan v. Omega Oil & Gas Ltd.* (1988), 47 D.L.R. (4th) 481 (S.C.C.) (partner to partner); *Lac Minerals Ltd. v. International Corona Resources Ltd.*, *supra* note 95 (senior mining company to junior mining company); *Canson Enterprises Ltd. v. Boughton & Co.* (1991), 85 D.L.R. (4th) 129 (S.C.C.) (solicitor to client); *Norberg v. Wynrib* (1992), 92 D.L.R. (4th) 449 (S.C.C.) (doctor to patient); *M.(K.) v. M.(H.)* (1992), 96 D.L.R. (4th) 289 (S.C.C.) (parent to child); and *Hodgkinson v. Simms*, *supra* note 106 (investment advisor to client).

108 *Supra* note 94 at 627-9.

109 *Frame v. Smith*, *supra* note 104.

110 *Supra* note 106.

111 *Ibid.* at 173.

112 *Ibid.* at 176-7.

113 *Ibid.*

114 *Ibid.*

115 *Ibid.* (emphasis added). Given the current composition of the Court, it is perhaps useful to note that McLachlin J. (as she then was) rigorously dissented,

opining that the principle of vulnerability remains the hallmark of the fiduciary relationship.

116 P.D. Finn, "The Fiduciary Principle," in T.G. Youdan, ed., *Equity, Fiduciaries and Trusts* (Toronto: Carswell, 1989) 64.

117 Per Southin J. in *Girardet v. Crease & Co.* (1987), 11 B.C.L.R. (2d) 361 at 366 (B.C.C.A.). See also Waters, *supra* note 95 at 405, who argues that "not all relationships will be held to be fiduciary, even though they involve reliance upon integrity and the presumption that a party will fully disclose his position."

118 Welling, *supra* note 102 at 1097.

119 *Ibid.* at 1121 (emphasis in original).

120 *Ibid.* at 1124.

121 Per Dickson J. in *Guerin*, *supra* note 91 at 384.

122 See J. Kennedy, "Equity in a Commercial Context," in P.D. Finn, ed., *Equity and Commercial Relationships* (Sydney: Law Book Co., 1987) at 15.

123 *Hospital Products Ltd. v. United States Surgical Corp.* (1984), 156 C.L.R. 41.

124 *Supra* note 25.

125 *Supra* note 59.

126 *Aquacool_2001*, *supra* note 2.

127 *Supra* note 15.

128 See e.g. D.H. Rimer and P. Noglows, "Internet Appliances and Universal Access" (1999) 4 *iWord* 1 online: <<http://www.iwords.com/iword4l.html>> (date accessed: 23 May 2000).

129 M. Williams, "Oracle's Vision of Networked Future," *Newsbyte News Service* (5 October 1995). For other network strategies, see J.M. McCann, "Technology Cyber trends" online: <<http://www.duke.edu/~mccann/q-tech.htm>> (last modified: 20 April 1997).

130 L.E. Ellison, "New Model on the Info Highway," *USA Today* (15 November 1995) 2B. For an example of a Web-based application that exploits this strategy, see online: <<http://www.Personalsite.com>> (date accessed: 23 May 2000).

131 D. James, "So How Do We Take the Pulse Now?" *Bus. Rev. Wkly.* 68 (5 July 1999).