

CANADIAN BUSINESS LAW JOURNAL  
VOL. 35  
2001

THE LEGAL RELATIONSHIP BETWEEN ONLINE  
SERVICE PROVIDERS AND USERS

Ian R. Kerr\*

I. 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.<sup>1</sup>

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.<sup>2</sup> Recognizing that its advertising revenue and stock valuations rest mainly

\*Canada Research Chair in Ethics, Law & Technology, Faculty of Law, Common Law Section, University of Ottawa; Special Counsel, Technology Law, Nelligan O'Brien Payne LLP, [iankerr@uottawa.ca](mailto:iankerr@uottawa.ca). I would like to thank the University of Toronto's Centre for Innovation Law and Policy, 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 contributions to the funding of this project. I would also like to convey my deepest gratitude to Marcus Bornfreund for all of his extraordinary efforts and for the high quality of research assistance that he provided. Thanks also to Karen G. McCulloch, David Arntfield, John Hoben and Bernard Sandier for their excellent help. Finally I wish to thank my colleague and friend, Michael Geist, for his invaluable comments and suggestions on an earlier draft of this article.

---

1. See plaintiffs complaint, para. 6, *Aquacool\_2000 v. Yahoo! Inc.*, originally filed at United States District Court Central District of California (hereafter *Aquacool\_2000*), online: Electronic Privacy Information Centre <[http://www.epic.org/anonymity/aquacool\\_complaint.pdf](http://www.epic.org/anonymity/aquacool_complaint.pdf)> (last modified: May 20, 2000). This suit was ultimately dropped for undisclosed reasons.

2. Yahoo!'s global audience is said to have grown to more than 145 million unique users worldwide. 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/pr11g00pr.html>> (last modified: April 5, 2000); see also G. Fontaine, "Internet Portals" online: *idate* <<http://www.idate.com/multi/lpi/lpi.pdf>> (last modified: February 1, 2000). This 1999 study revealed, *inter alia*, that Yahoo! was, at that time, the second largest portal, AOL being the largest.

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".<sup>3</sup> In fact, Yahoo! had set up similar message boards for nearly every publicly traded corporation.

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".<sup>4</sup>

As the story goes - and as one might imagine - AnswerThink did not think highly of Aquacool\_2000's remarks and answered with the threat of legal action. Capitulating to the pressure exerted by AnswerThink, Yahoo! decided to disclose personal information about Aquacool\_2000<sup>5</sup> without 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.<sup>6</sup> 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 online service providers<sup>7</sup> collect personal

---

3. *Supra*, footnote 1.

4. *Ibid.*, at para. 7.

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

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

7. In Netspeak, a distinction has been drawn between Internet Service Providers (ISPS) and Application Service Providers (ASPS). ISPS are utilized in order to gain access to the Internet, the client connecting to the ISPS' servers which provide the necessary uplink into cyberspace. ASPS make available assorted software applications, such as personal banking, once a user has already gained access to the Internet. Many ISPS, however, also provide application services such as e-mail and, as a result, frequently blur the distinction. There has been a tendency in several jurisdictions to treat ISPS - who merely provide access to the Internet and do not exercise any control over their users - as mere conduits of users' interaction. ISPs are thereby excluded from liability for the conduct of their users: see for example, *Cubby v. Compuserve*, 776 F. Supp. 135 (S.D.N.Y. 1991); *Zeran v. America Online, Inc.*, 129 F. 3d 327 (4th Cir. 1997); and also the U.S. 1996 Communications Decency Act, 47 USC, s. 230. The term "online service provider" is used throughout this article as a generic term to refer to any e-mail provider, bulletin board operator, auction host, anonymous re-mailer, commercial or amateur web site, or any other provider of an online service that is not merely a conduit to Internet access but

information about people like 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.<sup>8</sup> In order to obtain the plug-in, the user will be asked to complete an information form. Given the relative insignificance of the plug-in, the Macromedia form makes it optional for a user to include his or her first or last name. But every user is required to supply his or her e-mail address. If the user is willing to provide this basic information, he or she will then be able to download the plug-in and will thereby be enabled to view the desired content in an optimal manner.

Other online services will demand more extensive information in return for their more extensive products. For example, to become availed of its e-mail and Web page services, Yahoo! makes its users fill out a form that not only requires the disclosure of their names and e-mail addresses, but also their street addresses, interests, hobbies, etc. Data collected from forms such as these are combined into massive databases that are 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.<sup>9</sup> These are small files downloaded from a 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 then retrieved from the user's computer, allowing the service provider to maintain details on the movements of the user within its site. Some online service providers have set up wide-ranging networks of cookie senders and collectors, in the form of banners, that appear on

an entity that offers a service in exchange for, among other things, the ability to collect and store their users' personal information or private communications according to certain terms of service.

---

8. Macromedia is a graphics design company that specializes in dynamic web content. Plugins 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: May 21, 2000).

9. See "What's in them Cookies? Web Site is Finding Out", Privacy Times (February 15, 1999) at p. 1.

web sites of all types and descriptions. The program associated with those banners pumps the cookie information into a single depot. Online advertising giant Doubleclick is one such company.<sup>10</sup> 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 to develop a highly detailed profile of where the user has been and when they were there.<sup>11</sup>

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 e-mail 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, 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 necessary 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 can 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 her 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 or her zip or postal code, gender, occupation, industry and interests. In addition to this information, which

---

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

11. *Ibid.*

is "voluntarily"<sup>12</sup> disclosed by those who wish to be subscribers, Yahoo! also collects other kinds of information about its subscribers without their knowledge. For example, it gathers information that would allow an interested party to trace the source of every comment posted on each and every one of its message boards. Yahoo! does this by saving a log of Internet Protocol (IP) addresses<sup>13</sup> 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 e-mails 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<sup>14</sup> their messages.<sup>15</sup>

---

12. Quotation marks are used to indicate a qualified sense of the word voluntarily. 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. It is interesting to note that many people do just that.

13. 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 to 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: May 4, 2000); J.R. Levine and C. Baroudi, *The Internet for Dummies* (San Mateo, Cal., IDG Books, 1994).

14. 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 confirmed 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.pcguardian.com/software/encryption\\_faq.htm](http://www.pcguardian.com/software/encryption_faq.htm)> (last modified: May 9, 2000).

Encryption may be divided into two types: symmetric 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 that 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. See, e.g., G. Greenleaf and Roger Clarke, "Privacy Implications of Digital Signatures" (IBC Conference on Digital Signatures, Sydney, Australia, March 12, 1997), online: Privacy Implications of Digital Signatures <<http://www.anu.edu.au/people/Roger.Clarke/DV/Digsig.html>> (last modified: March 10, 1997). See also Pretty Good Privacy, online: PGP Security <<http://www.pgp.com/>> (date accessed: May 17, 2000).

15. Of course, encryption would be pointless for those like Aquacool\_2000 who wish to make pseudonymous public commentary.

Given its remarkable technical means of gathering, copying, storing and manipulating personal information, it is no surprise that Yahoo! had exactly the information that AnswerThink was looking for. Moreover, this was likely not the first time that a high-powered corporation such as AnswerThink had instituted legal proceedings merely to intimidate and silence its online critics.<sup>16</sup> Is it any less surprising that Yahoo! decided to disclose to AnswerThink personal information about Aquacool\_2000?

Do not 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.<sup>17</sup> The first sentence of its Privacy Policy proclaims that "Yahoo! is committed to safeguarding your privacy online." It further states:

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 . . ."<sup>18</sup>

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".<sup>19</sup> 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.<sup>20</sup>

At the bottom of its Privacy Policy and throughout its Web site, Yahoo! displays the TRUSTe certificate,<sup>21</sup> a logo which 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

---

16. *Aquacool\_2000*, *supra*, footnote 1, at para. 26.

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

18. *Ibid.*

19. *Ibid.*

20. *Ibid.*

21. TRUSTe is an independent, non-profit privacy initiative dedicated to building users' trust and confidence on 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: May 17, 2000). See also online: Truste <<http://www.truste.org/>> (last modified: April 24, 2000).

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, until very recently, granted several such requests without ever notifying the subscriber that his or her personal information and private communications were about to be disclosed.<sup>22</sup> By failing to notify its subscribers, Yahoo! precludes entities 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. Other online posters' identities have similarly been sought after by corporations upset over the content of their posts.<sup>23</sup> This phenomenon is particularly pervasive in the context of financial bulletin boards. Likewise, Yahoo! is not the only online service provider known to have disclosed personal information to a third party upon request. Whether for alleged contraventions of laws or simply out of curiosity, many anonymous posters have had their identities exposed. No doubt there are many more who have been "outed" but are unaware.<sup>24</sup>

---

22. *Supra*, footnote 1, at para. 23. Coincidental to the settlement of the Aquacool\_2000 dispute, Yahoo! has recently changed its policy so as to provide notice of its intention to disclose personal information to third parties - see Lauren Gard, "Yahoo Hit With Novel Privacy Suit", *The Recorder* (May 15, 2000) online: Law.com <<http://www.law.com/cgi-bin/gx.cgi/AppLogic+FTContentServer?pagename=law/View&c=Article&cid=ZZZW330B68C&live=true&cst=1&pc=0&pa=0&s=News&ExpIgnore=true&showsummary=0>> (date accessed: April 23, 2000).

23. For example, in *Hyide v. ACLU* (Fla. Dist. Ct. App. 3d, 2000), Florida's 3rd District Court of Appeals upheld an order for Yahoo! and America Online, Inc. to reveal the identities of the eight anonymous defendants accused of posting allegedly defamatory messages. Also, in the Canadian cases of *Philip Services Corp. v. John Doe* a.k.a. Addicted 2PHV et al. (unreported, June 24, 1998, Ont. Ct. (Gen. Div.), Court File No. 4592/98) and *Irwin Toy v. Doe*, [2000] OT No. 3318 (QL) (S.C.J.) ISPs were ordered to reveal the identities of their respective clients alleged to have posted defamatory comments.

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 paras. 6-16. See also *U.S. v. Maxwell*, [1995] 42 MT 568 (A.F. Ct. Crim App.), where the plaintiff was revealed to trade in child pornography via e-mail and was subsequently discharged from his position as colonel in the U.S. Army. Similarly, in *McVeigh v. Cohen*, 983 F. Supp. 215 (D.D.C., 1998), the plaintiffs homosexual orientation was disclosed following a third party request, and he too was subsequently discharged from service.

American online 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. Someone sends you an e-mail with the subject header, "TRY THIS!". You are not even aware that this particular e-mail has been sent to you. Because your inbox is overloaded with messages, the "TRY THIS!" message has caused you to exceed your available disk quota. Consequently, access to your e-mail has been disabled. So you phone your Internet service provider, Supernet, to complain that you are unable to access your e-mail. 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 the 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 co-operate. 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 was 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 have instructed your Internet service provider to re-send the pornographic e-mail 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.<sup>25</sup> Perhaps even more surprising was the decision that was rendered by the Alberta Court of Appeal. It unanimously upheld the decision of the trial judge, who held that Supernet's search of the user's inbox, its decision to open the user's e-mail 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

---

25. *R. v. Weir*, [2001] A.J. No. 869 (QL) (C.A.), affd 213 A.R. 285 (Q.B.).



did not unjustly interfere with the user's reasonable expectation of privacy.<sup>26</sup>

After pausing for dramatic effect, I must now confess that, in the foregoing narrative, I sugar-coated the facts. In the actual Alberta case, Weir, the recipient of the "TRY THIS!" e-mail, 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 his private communications were discovered and disclosed should be troubling to everyone. 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 to disclose its finding without notice or any other form of due process.

These narratives illustrate the considerable power online service providers hold over their users. Service providers are by default the gatekeepers of informational privacy on the Internet. By providing online services such as e-mail, Web site space, or portals to various online consortia, a service provider gains access to and control over a plethora of personal information and private communications belonging to each of its many users. All users are 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. As illustrated by the above narratives, this is sometimes cause for concern.

In Canada, the newly enacted Personal Information Protection and Electronic Documents Act<sup>27</sup> prescribes a number of rules that are sure to have an impact on many of the informational transactions between service providers and third parties. But as Canada's former Federal Privacy Commissioner once 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

---

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.), c. 11.

27. Personal Information and Electronic Documents Act, S.C. 2000, c. 5 (hereafter Bill C6). See <[http://www.parl.gc.ca/36/2/parlbus/chambus/house/bills/government/C-6/C6\\_4/C-6TOCE.html](http://www.parl.gc.ca/36/2/parlbus/chambus/house/bills/government/C-6/C6_4/C-6TOCE.html)> (last visited: May 14, 2000).

inappropriate intrusions, be they brought about by dealings with personal information or by other forms of surveillance.<sup>28</sup>

The aim of this article 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 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.

Secondly, an examination of online service provider-user relationships in this context will have the 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, expertise), this study seeks to provide a more robust understanding of what it is that makes a relationship one of dependence. As such, the project will ultimately contribute to a broader understanding of the law of obligations.

## II. THE CONTRACTUAL UNDERPINNINGS OF SERVICE PROVIDER-USER RELATIONSHIPS

The proliferation of available online services defies comprehensive quantification or classification. However, it is useful to categorize Internet services according to the nature of the exchange between provider and user. For present purposes, it is sufficient to consider three kinds of basic exchanges: (a) services in exchange

---

28. Bruce Phillips, "The Evolution of Canada's Privacy Laws" (Canadian Bar Association Ontario Institute, Toronto, January 28, 2000), online: Privacy Commission of Canada <[http://www.privcom.gc.ca/english/02\\_05\\_a\\_000128\\_e.htm](http://www.privcom.gc.ca/english/02_05_a_000128_e.htm)> (last modified: April 18, 2000).

for cash; (b) services in exchange for personal information; and (c) services in exchange for tolerated advertising.<sup>29</sup>

Internet access is one kind of online service that is usually offered in exchange for cash.<sup>30</sup> Access providers often provide a range of services on a cash-for-service basis. Among these are email accounts, multiple e-mail addresses, access to the World Wide Web and to various databases, mailing lists of users with similar interests and hosting for user Web pages.

The second category provides various services in exchange for a user's personal information rather than money. Often these 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 exchange for the user's name, address, and other personal information about a user's habits and preferences, the user can get stock quotations, subscribe to a personalized news compilation service, be apprized of the local weather conditions and be provided with web site hosting.

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.<sup>31</sup> The other end of the spectrum is exemplified by a site that offers a free basic media player for downloading in the hopes that the user will then be tempted to license a more sophisticated version of the same software.<sup>32</sup>

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. Reduced to their

---

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

30. Although a number of free ISPS do exist. See, e.g., <<http://www.freedomlist.com>>.

31. See online: The Spark.com Purity Test <<http://test.thespark.com/puritytest>> (last modified: April 9, 2000). Apparently, the information collected for the purity test is not logged.

32. See online: Real Audio Player <<http://www.real.com>> (last accessed: April 24, 2001).

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.<sup>33</sup> For the purposes of this study, the analysis of online service provider-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.<sup>34</sup>

Limiting the investigation of online service provider-user relationships to situations where the service provider offers explicit terms of service that are manifestly assented to by the user, a relatively extensive survey of more than 40 such agreements<sup>35</sup>

---

33. See I.R. Kerr, "Spirits in the Material World: Intelligent Agents as Intermediaries in Electronic Commerce" (1999), 22 *Dalhousie 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: June 7, 1999); F.M. Buono and LA. 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 & Digital Signatures: An Overview of Law and Legislation" (1999), *PLI/Pat* 125.

34. Anyone who has conducted even the briefest appraisal of online user agreements will immediately recognize this assumption to be false. Most graphical interfaces for terms of service are poorly designed and would probably be unenforceable according to ratio in *Tilden Rent-A-Car Co. v. Clendenning* (1978), 18 O.R. (2d) 601, 83 D.L.R. (3d) 400 (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.

35. The list of ISP terms of service considered in this study included: online: Athome.com & Atwork.com <<http://www.athome.com>> (last modified: April 28, 2000); online: Acadia University <<http://www.acadiau.ca/cs/pubdocs/policies.html>> (last modified: April 8, 1998); online: Alberta Supernet <<http://www.supernet.ab.ca>> (last modified: March 25, 2000); online: AOL <<http://www.aol.com/copyright.html>> (last modified: January 20, 2000); online: AT&T Business <<http://www.attbusiness.net/terms/index.html>> (last modified: March 15, 2000); online: AT&T Canada <<http://www.attcanada.ca/about/ncterm.html>> (last modified: May 16, 2000); online: Bluelight.com <<http://bluelight.com/company.privacy.shtml>> (date accessed: May 22, 2000); online: Canada.com <<http://www.canada.com/members/register.asp?/home>> (date accessed: May 22, 2000); online: Concentric <[http://www.concentric.com/privacy\\_policy.html](http://www.concentric.com/privacy_policy.html)> (last modified: March 27, 2000); online: Cyberlink <<http://webservices.cyberlink.bc.ca/>

governing a variety of services in various jurisdictions<sup>36</sup> ultimately revealed a range of different obligations undertaken by service providers with respect to the disclosure of personal user information. The results of the survey indicate that service provider-user relationships can be understood as falling into one or more of five categories:<sup>37</sup> (a) confidential, (b) confidential within the limits of the law; (c) disclosure when illegality is suspected, (d) disclosure to protect

---

[acceptable\\_use\\_policy.html](#)> (last modified: February 27, 2000); online: Demon <<http://www.demon.net/info/helpdesk/aup/access.shtml>> (date accessed: May 22, 2000); online: DeVRY <<http://www.devry.ca/index.htm>> (last modified: December 22, 1999); online: DirecPC <<http://www.direcpc.com>> (last modified: May 19, 2000); online: Geomail <<http://www.geocities.com/svcagreement.htm>> (date accessed: May 22, 2000); online: Globix <<http://www.globix.com/support/aup.html>> (last modified: April 14, 2000); online: Imaginet <<http://www.express.ca>> (last modified: May 15, 2000); online: Inforoute (English) <<http://www.inforoute.net/terms.html>> or (Francais) <<http://www.inforoute.net/francais/terms.html>> (last modified: December 19, 1999); online: Interlog <<http://www.interlog.com/terms.html>> (date accessed: May 22, 2000); online: iPrimus <<http://www.iprimus.ca/personal/terms/acceptable.htm>> (last modified: March 23, 2000); online: Magma <<http://www10.magma.ca/services/corporate/hosting/faq/acceptable%5Ffaq.html>> (last modified: March 2, 2000); online: Mindspring <<http://www.mindspring.com/aboutms/aup.html>> (last modified: March 28, 2000); online: MSN Hotmail <<http://www.hotmail.msn.com>> (date accessed: May 22, 2000); online: Muskoka.com <<http://www.muskoka.com/conditions.html>> (last modified: May 8, 1999); online: NBTel (NBNet) <<http://www.nbnet.nb.ca/connect/accuse.shtml>> (last modified: January 20, 1999); online: Nipissing University <<http://kenm.unipissing.ca/uts/pollan.htm>> (last modified: September 29, 1999); online: Pangea <<http://www.pangea.ca/policy.html>> (last modified: March 13, 2000); online: Sprint Canada <<http://www.sprintcanada.ca/English/Terms.asp?Section=FORHOME>> (last modified: December 7, 1999); online: Sympatico <<http://www.sympatico.ca/help/About/ser-viceagree.html>> (date accessed: May 22, 2000); online: Telus (a subsidiary of BCTel <<http://www.telus.com>> (last modified: October 17, 1999); online: Toronto Free-Net <<http://freenet.toronto.on.ca>> (last modified: May 15, 2000); online: University of Alberta <<http://www.ualberta.ca/CNS/POLICY/Conditions.html>> (last modified: January 15, 1998); online: University of Toronto <[http://www.utoronto.ca/welcome.htm/utor\\_dist/general/utormail.html#eligible](http://www.utoronto.ca/welcome.htm/utor_dist/general/utormail.html#eligible)> (last modified: January 17, 2000); online: UWO <<http://www.uwo.ca/its/ftp/nic/security/AUP.html>> (last modified: October 10, 1997); online: Verio <<http://home.verio.com/company/aup.cfm>> (date accessed: May 22, 2000); online: Yahoo! <<http://docs.yahoo.com/info/terms>> (date accessed: May 22, 2000).

36. The survey included international service providers (who offered 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 whom are more accurately described as "regional" providers); and Canadian non-commercial/institutional service providers (including various "free-nets", government and university service providers); and workplace service providers (who may use any of the above service providers).

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

the service provider or in extraordinary circumstances, and (e) voluntary disclosure and active monitoring.

### 1. Confidential

Though this form of contractual undertaking is indeed quite rare, some online service providers 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 re-mailer service known as [anon.penet.fi](http://anon.penet.fi). By stripping e-mail messages of the identities and digital addresses of the original sender and then re-mailing them to the locations specified, the [anon.penet.fi](http://anon.penet.fi) re-mailer service allowed individuals who might not otherwise have participated in certain socially beneficial discussions to have a voice, without fear of reprisal.<sup>38</sup>

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.<sup>39</sup> However, when push came to shove, after a Finnish court required him to divulge the e-mail address belonging to one of his users who was suspected of distributing child pornography, Helsingius caved. Shortly thereafter, he decided to shut down his re-mailer.<sup>40</sup>

Online service providers are generally unwilling to promise absolute confidentiality to their users in the face of a court order as a result of recently proposed and enacted legislation in various jurisdictions that requires such providers to comply with law enforcement, failing which the provider will be strictly liable, either criminally or civilly, for the conduct of its users. For example, the recently proposed Bill C-23 1, the Internet Child Pornography Prevention Act,<sup>41</sup> requires service providers to "advise the Minister of the identity of [the user], the nature of the material and the means

---

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

39. L. Detweiler, "Anonymity on the Internet" (May 13, 1993) at p. L 1, online: Electronic Frontier Foundation <[http://www.eff.org/pub/privacy/Anonymity/net\\_anonymity.faq](http://www.eff.org/pub/privacy/Anonymity/net_anonymity.faq)> (last modified: May 11, 1994).

40. See J. Quittner, "Requiem for a Go-Between", Time (September 16, 1996), p. 75; Levine, *supra*, footnote 38, at p. 1532.

41. Bill C-231, Internet Child Pornography Prevention Act, 2nd Sess., 36th Parl., 1999 (1st Reading October 18, 1999) (hereafter Bill C-231).

whereby it may be accessed by others".<sup>42</sup> According to this Bill, a service provider 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.<sup>43</sup>

Provisions such as this have become known as safe harbours.<sup>44</sup> In the present context, a safe harbour aims to encourage responsible online behaviour by providing a statutory limitation on the liability of service providers. Notice the strategy here. Rather than involving government directly in the policing of online conduct, regulation is left in the hands of service providers and users. A safe harbour allows a provider to avoid liability for illegal conduct that takes place on its site or as a result of its services. Online service providers can protect themselves by taking affirmative action (e.g., removing the offending materials) and in some instances by disclosing information about their users.<sup>45</sup>

While this strategy circumvents problems typically associated with a top-down governmental approach to regulation, it has its own drawbacks. As John Sopinka 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.<sup>46</sup>

---

42. *Ibid.*, s. 6 (3)(c).

43. According to this Bill, online service providers would be required to obtain a licence.

44. See Levine, *supra*, footnote 38, at p. 1563. See also U.S. International Trade Administration Electronic Commerce Task Force, International Safe Harbour Privacy Principles (April 19, 1999), online: U.S. International Trade Administration <<http://www.ita.doc.gov/td/ecom/shprin.html>> (last modified: December 2, 1999).

45. 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.

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

Though it does not, strictly speaking, contain a safe harbour provision, s. 7 of the recently enacted Personal Information Protection and Electronic Documents Act<sup>47</sup> has a similar effect.<sup>48</sup> Assuming that service providers are governed by the Act,<sup>49</sup> it will encourage them to disclose personal information to third parties without the users' knowledge or consent whenever the service provider "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".<sup>50</sup> To restate the point made by Sopinka in a slightly different way, legislative initiatives such as these put online service providers in an unenviable relationship with their users. While service providers 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 a service provider's interest to disclose personal information in a manner that undermines the interests of its users.

Given that most service providers 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.

## 2. Confidential within the Limits of the Law

Many terms of service agreements promise that the service provider will take steps to ensure the confidentiality of a user's communications and will only release personal information in circumstances where the provider is legally compelled to disclose. An online service provider that adopts this approach will generally

---

47. *Supra*, footnote 27.

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

49. It is unclear whether this federally enacted statute applies to Internet service providers. Section 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 was therefore a federally regulated business: *Re: Island Telecom Inc.* (2000), C.I.R.B.D. No. 12 (CIRBD Decision No. 59) (hereafter *Island Tel*). If the *Island Tel* ruling is adhered to, then the Act will likely apply to ISPs.

50. *Supra*, footnote 27, s. 7(2)(a).



request that its 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).<sup>51</sup>

Service providers who have opted for internal sanctioning of their users often do not 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:

### 3. Disclosure whenever Illegality is Suspected

A number of service providers 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 was the practice adopted by Yahoo!.<sup>52</sup> Service providers who fall into this category tend to view co-operation 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 Weir's e-mails 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

---

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

52. What makes the Aquacool\_2000 case controversial is that 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".

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.<sup>53</sup> Presumably, notices such as these will make it difficult for users to argue that they reasonably held a high expectation of privacy.

#### 4. Disclosure to Protect Service Provider or in Extraordinary Circumstances

Some service providers 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.<sup>54</sup> Many commercial providers 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.

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 safeguarding its users' personal information than service providers falling into the other categories enumerated above. Still, providers in this category do promise that their default position is not to disclose personal information unless there is at least some reason for doing so. This can be contrasted with providers in the final category, who make no such promises.

---

53. See online: Alberta Supernet <<http://www.supernet.ab.ca>> (last modified: March 25, 2000) (emphasis added) (hereafter Supernet). 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/Termsasp?Section=FORHOME>> (date accessed: May 23, 2000).

54. Pursuant to s. 7(2)(b) of the Personal Information and Electronic Documents Act, *supra*, footnote 27, disclosure of personal information for these sorts of reasons is also permitted.

## 5. Voluntary Disclosure and Active Monitoring

The final class consists of online service providers who are unwilling to make any assurances as to the confidentiality of their users' personal information. Often, these providers 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

[i]n 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.<sup>55</sup>

Some service providers 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.

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

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.<sup>56</sup>

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

---

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

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

Thus far, we have only considered contractual approaches to various service provider-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.<sup>57</sup> The question that must ultimately be addressed is whether relationships between providers and users - though they are at their core contractual in nature - are always to be understood as relationships at arm's length.

### III. RELATIONSHIPS OF DEPENDENCE AND INTERDEPENDENCE

#### 1. 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.<sup>58</sup> By understanding social interaction in this way, it is clear that 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.<sup>59</sup> One can gauge the level of a person's needs by determining the extent to which that person's wellbeing 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.<sup>60</sup>

Some social exchange theorists have recognized that dependence in a relationship affects the power held by each of the

---

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

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

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

60. C.R. Agnew et al., "Cognitive Interdependence: Commitment and the Mental Representation of Close Relationships" (1998), 74 *Journal of Personality and Social Psychology* 939 at p. 940.

parties. This is so because one individual's power over another derives from the other party's being dependent on him or her.<sup>61</sup> Not straying 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 exchange episode at another's expense.<sup>62</sup> Accordingly, power is fundamentally rooted in the dependence actors have on one another.<sup>63</sup>

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 her behaviour, she 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.<sup>64</sup> When X has fate control over Y, she can affect Y's outcomes regardless of what Y does. It is therefore possible for X to employ her 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 her 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 wellbeing of both parties is dependent upon the existence of the relationship.<sup>65</sup> 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 the power that can be exerted upon the other with impunity. Increasing interdependence

---

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

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

63. 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 Inc., 1993), p. 127.

64. Thibaut and Kelley, *supra*, footnote 61, at p. 124.

65. *Ibid.*

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<sup>66</sup> adds two further dimensions. First, it suggests that dependence increases to the degree that the dependent party makes an investment in the relationship. Here, "investment" refers to the resources that a person has devoted to the relationship, either directly or indirectly.<sup>67</sup> 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 it.<sup>68</sup> The more that one invests in the relationship, the more he or she 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 wellbeing is influenced by Mary and their relationship.<sup>69</sup>

It is important to differentiate between dependence and commitment. Dependence describes the structural aspect of the relationship between two parties, whereas commitment characterizes one

---

66. CE. 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.

67. Agnew et al., *supra*, footnote 60, at p. 940.

68. Penner, *supra*, footnote 58, at p. 515.

69. Agnew et al., *supra*, footnote 60, at p. 940. 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, August 16, 1996) [unpublished], online: Association for Information Systems - Americas Conference <<http://hsb.baylor.edu/ramsower/ais.ac.96/papers/yoony.htm>> (last modified: September 27, 1997).

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 or her 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.<sup>70</sup>

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 service provider-user relationships.

## 2. Dependence and Interdependence in Service Provider-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 above in Part II. This theory can be used to explicate the degree to which users come to depend on online service providers.

### (a) 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 not possible nor is it desirable to compile a comprehensive list. A few examples will suffice. Perhaps the most basic need of Internet users which requires the establishment of a relationship with an

---

70. Agnew et al., *ibid.*

online service provider is the need to gain access to the Internet.<sup>71</sup> 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. While the question of universal access to online services may seem unimportant to some,<sup>72</sup> the issues surrounding access will become more pressing as government and private 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.<sup>73</sup> 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 a service provider, 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. With a continued social migration into digital environments, the wellbeing of individuals will come to depend on their relationships with service providers.

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

---

71. 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.

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

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



dependent on the relationship they have with their access providers.<sup>74</sup>

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

Applying interdependence theory to this scenario, a service provider has fate control over its users. That is, by being in a position to employ a user's private information to various ends,<sup>75</sup> a service provider can affect the user's outcomes, regardless of what the user does. To continue with an earlier example, Yahoo!'s decision to disclose the identity of Aquacool\_2000 to AnswerThink resulted in the dismissal of Aquacool\_2000 from his 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 powerholder in a relationship as a means of controlling the dependent party's behaviour. Thus a service provider'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 above in Part II.

---

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

75. Including, as we shall see in Part III below, promoting its own interests at the expense of the user's interests.

One might argue that, given the availability of alternative service providers, the power that can be asserted by any given provider is in fact limited to behaviour control. Those who espouse this position would say that a service provider does not have the power to control its users' fates, since users are not in fact bound to remain in that relationship.<sup>76</sup> If a user does not like the privacy policy of a particular service provider, she can simply change her 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 choices.

While it is true that, for many Internet services, a user might easily establish an alternative relationship which would result in better outcomes, it is crucial to recognize that, if the user had previously entered into a relationship with a different service provider, he or she may have made a very special sort of investment in the first relationship. He or she 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 or her 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 the parties, the same cannot be said of online service provider-user relationships. Though one consequence of many service provider-user relationships is that the service provider becomes privy to all sorts of personal information and private communications belonging to the user, most service provider-user relationships are not close personal ones. Since a service provider 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.

---

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

## (b) Service Provider-User Interdependence

Interdependence theory asserts that, for most dyadic relationships, the wellbeing of each party is to an extent dependent on the wellbeing of their relationship.<sup>77</sup> Notice that this is not so in the case of service provider-user relationships. Though providers are commercially dependent on the existence of users in general,<sup>78</sup> they are not usually dependent on particular users. This creates a serious imbalance in most provider-user relationships. From the perspective of an online service provider, the user is but an (IP) number. Unlike the situation where a husband or wife is reposed of confidence and is later pressed with a request to disclose personal or private information to a third party, the service provider is not psychologically committed to the relationship. Given the lack of interdependence in the relationship, the provider will be inclined to give greater weight to furthering its own interests than it would to furthering the wellbeing of the user (or to furthering its relationship with the user). Since each individual user is in essence dispensable, the power structure of most service provider-user relationships will never reach a state of equilibrium. Consequently, the service provider will not usually be inclined to protect the user's interests as against its own or others'. This puts online service providers in a position similar to banks and other commercial institutions that are in the care and control of their customers' personal information or other transactional information. The difference is one of degree. Given that online service providers often store and manage users' private communications on an unlimited number of subjects (not just financial information), the personal hold that a provider may have over its users could make users even more dependent on the confidentiality of online service provider-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 online service provider. But sometimes providers in whom trust or confidence have been

---

77. 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.L. & Juris.* 19.

78. Schwartz, "Privacy and Democracy in Cyberspace" (1999), 52 *Vand. L. Rev.* 1609 at p. 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."

reposed 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 a service provider 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.

#### IV. 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.<sup>79</sup> "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."<sup>80</sup> 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."<sup>81</sup> 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,<sup>82</sup> the law has been said to facilitate the development of interdependent relationships. In his well known work on the fiduciary obligation, Ernest Weinrib characterized the fiduciary obligation as the law's realization of the economic importance of fostering incentive by protecting relationships of interdependence - relationships which 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

---

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

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

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

82. See e.g. *Goldex Mines Ltd. v. Revill* (1974), 7 O.R. (2d) 216 at p. 224, 54 D.L.R. (3d) 672 (C.A.); *Guerin v. Canada* (1984), 13 D.L.R. (4th) 321 at pp. 340-41, [1984] 2 S.C.R. 335.

and interdependence. The fiduciary obligation ... constitutes a means by which those mechanisms are protected.<sup>83</sup>

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 interdependency.<sup>84</sup> An interactive and interdependent society mandates the monitoring of trusting relationships in order to avoid their potential for abuse.

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 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."<sup>85</sup> 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 modest. It is restricted to a determination of whether any of the core notions underlying the fiduciary concept might plausibly be ascribed to online service provider-user relationships.

## 1. The Fiduciary Concept

In the *Law of Trusts in Canada*,<sup>86</sup> Donovan 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".<sup>87</sup> The reposing of trust

---

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

84. See also L.1. Rotman, "Fiduciary Doctrine: A Concept in Need of Understanding" (1996), 34 Alta. L.R. 821 at p. 826.

85. Per La Forest J. in *Lac Minerals Ltd. v. International Corona Resources Ltd.*, [1989] 2 S.C.R. 574, 61 D.L.R. (4th) 14.

86. D.W.M. Waters, *Law of Trusts in Canada*, 2nd ed. (Toronto, Carswell, 1984), pp. 710-15.

87. Weinrib, *supra*, footnote 83, at pp. 4-5.

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.<sup>88</sup> 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."<sup>89</sup> Robert 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 or she 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.<sup>90</sup>

## 2. 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 in listing the traditional categories of relationships that attracted a fiduciary obligation, followed by an attempt to determine whether 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."<sup>91</sup>

---

88. Flannigan, *supra*, footnote 81, at p. 287.

89. Weinrib, *supra*, footnote 83, at p. 7.

90. Flannigan, *supra*, footnote 81, at p. 308.

91. Rotman, *supra*, footnote 84, at p. 825.

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.<sup>92</sup> 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 which is equivalent to a discretion or power to affect the trusting party's legal or practical interests. Many of the categories enumerated above consist in relationships wherein the trusting party has sought the advice of the trusted party. 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 Bruce 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.<sup>93</sup>

### 3. Fact-Based Fiduciary Relationships

Although the use of traditional categories to determine fiduciary relationships was originally effective as an abbreviation of a difficult legal concept, some commentators subsequently recognized

---

92. See e.g. Flannigan, *supra*, footnote 81, at p. 294.

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

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.<sup>94</sup>

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.<sup>95</sup> As a result, fiduciary doctrine has expanded to cover other fact-based fiduciary relationships. More recently, writing for the majority of the Supreme Court, La Forest 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.<sup>96</sup>

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 which underlie the fiduciary relationship with the aim of identifying its constituent elements. Over the last quarter century the Supreme Court has spent a great deal of time wrestling with the principles,

---

94. Weinrib, *supra*, footnote 83, at p. 5.

95. Guerin, *supra*, footnote 82; see also *Frame v. Smith* (1987), 42 D.L.R. (4th) 81 at p. 97, [1987] 2 S.C.R.99.

96. *Hodgkinson v. Simms* (1994), 117 D.L.R. (4th) 161 at pp. 179-80, [1994] 3 S.C.R. 377.



policies and essential ingredients underlying the fiduciary relationship<sup>97</sup>

#### 4. The Constituent Elements of Fact-Based Fiduciary Relationships

Ever since the Supreme Court of Canada's decision in *Lac Minerals v. International Corona Resources Ltd.*,<sup>98</sup> most fact-based fiduciary inquiries begin with an acknowledgement of the approach adopted by Wilson J. in *Frame v. Smith*:

[T]here 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.<sup>99</sup>

Sopinka J. also identified "depending or vulnerability" as the one characteristic which was indispensable to the existence of a fiduciary relationship. The indispensability of depending or vulnerability remained unchallenged until the Supreme Court's decision in *Hodgkinson v. Simms*.<sup>100</sup> In his majority judgment in

---

97. See e.g. *Canadian Aero Services Ltd. v. O'Malley* (1973), 40 D.L.R. (3d) 371, 119741 S.C.R. 592 (senior corporate officers/directors to corporation); *Jirma Ltd. v. Mister Donut of Canada Ltd.* (1973), 40 D.L.R. (3d) 303, [1975] 1 S.C.R. 2 (franchiser to franchisee); *Guerin v. Canada*, *supra*, footnote 82 (federal government to Indian Band); *Frame v. Smith*, *supra*, footnote 95 (custodial parent to non-custodial parent); *Molchan v. Omega Oil & Gas Ltd.* (1988), 47 D.L.R. (4th) 481 (partner to partner); *Lac Minerals Ltd. v. International Corona Resources Ltd.*, *supra*, footnote 85 (senior mining company to junior mining company); *Canson Enterprises Ltd. v. Boughton & Co.* (1991), 85 D.L.R. (4th) 129, [1991] 3 S.C.R. 534 (solicitor to client); *Norberg v. Wynrib* (1992), 92 D.L.R. (4th) 449, [1992] 2 S.C.R. 226 (doctor to patient); *M.(K.) v. M.(H.)* (1992), 96 D.L.R. (4th) 289, [1992] 3 S.C.R. 6 (parent to child); and *Hodgkinson v. Simms*, *ibid.* (investment advisor to client).

98. *Supra*, footnote 85, at pp. 627-29.

99. *Frame v. Smith*, *supra*, footnote 95, at pp. 98-99.

100. *Hodgkinson v. Simms*, *supra*, footnote 96.

Hodgkinson, La Forest 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 ...[W]hile the doctrine of unconscionability is triggered by abuse of a preexisting 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.<sup>101</sup>

After reviewing *R. v. Guerin* and *Frame v. Smith*, La Forest 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".<sup>102</sup> He reiterated that the oft-quoted dicta of Wilson J. is merely "a 'rough and ready' guide in identifying new categories of fiduciary relationships",<sup>103</sup> describing her three general characteristics as "indicia that help recognize a fiduciary relationship rather than ingredients that define it".<sup>104</sup> According to La Forest 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."<sup>105</sup>

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,

[t]he word "fiduciary" is flung around now as if it applied to all breaches of duty by solicitors, directors of companies 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, e.g.... by entering into a contract with

---

101. *Ibid.*, at p. 173 and 174.

102. *Ibid.*, at pp. 176-77.

103. *Ibid.*, at p. 176.

104. *Ibid.*

105. *Ibid.* (emphasis added). Given the current composition of the court, it is perhaps useful to note that McLachlin J. (as she then was) vigorously dissented, opining that the principle of vulnerability remains the hallmark of the fiduciary relationship.

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.<sup>106</sup>

Other critics also share this point of view. Welling, for example, has suggested that "The time has come to rein in runaway fiduciary duties."<sup>107</sup> As he has argued,

[k]idnappers 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.<sup>108</sup>

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 managed to stop the trendy nonsense by which every bit of corporate or professional nastiness became labeled a breach of fiduciary obligation",<sup>109</sup> 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".<sup>110</sup> 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.<sup>111</sup> This point has been recognized in a number of cases.<sup>112</sup>

To recapitulate, 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 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. Secondly, recognizing dependency

---

106. Per Southin J. in *Girardet v. Crease & Co.* (1987), 11 B.C.L.R. (2d) 361 at p. 362 (B.C.C.A.). See also *Waters*, *supra*, footnote 86, at p. 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".

107. Welling, *supra*, footnote 93, at p. 1097.

108. *Ibid.*, at p. 1121 (emphasis in original).

109. *Ibid.*, at p. 1124.

110. Per Dickson J. in *Guerin v. Canada*, *supra*, footnote 82, at p. 384.

111. See J. Kennedy, "Equity in a Commercial Context" in RD. Finn, ed., *Equity and Commercial Relationships* (Sydney, Law Book Co., 1987), p. 15.

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

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 or her 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.

## V. SERVICE PROVIDER-USER RELATIONSHIPS

Is the relationship between Internet service provider and user merely a relationship at arm's length? Or is it one 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 service provider-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 online service provider could ever be said to be a fiduciary. Without a doubt, a number of the constituent elements are present in many provider-user relationships. As we have seen, Internet users are very often in a relationship of dependence with their service providers. The current architectures of the networked world allow providers 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 providers to exercise power to the benefit or detriment of their users. Not only does this allow providers 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 a provider has the leeway to affect the legal position of its user, putting the latter at the mercy of the former. An online service provider 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, turn over otherwise privileged evidence in the course of criminal or private litigation, and so on.

At the same time, it is not clear that the services offered by most service providers are ever undertaken with a view towards acting primarily to the benefit of 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 employer's own ends. Even the most benevolent employer (whose policy permits employees to use 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 above in Part II. Such circumstances will arise whenever an online service provider has given clear notice that its allegiances are not always with its users. According to the broad categories of contractual undertakings outlined in Part II, this could occur when a service provider states in its contract that it will (i) disclose whenever illegality is suspected, (ii) disclose to protect the service provider or in extraordinary circumstances, or (iii) volunteer disclosure and actively monitor. These three categories of contractual undertakings are contemplated to be at arm's length. The case of Weir<sup>113</sup> discussed above in Part I furnishes a useful illustration. Recall that Supernet's Acceptable Use Policy and Liability Disclaimer provided that it

[w]ill 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.<sup>114</sup>

On the basis of having signed this agreement, which explicitly stated that Supernet's loyalty was limited whenever illegality is suspected, is there any credible basis upon which Weir could assert that he believed his relationship with Supernet to be one in which

---

113. *Supra*, footnote 25.

114. Supernet, *supra*, footnote 53.

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 service provider would remain loyal to him once it had inadvertently discovered that he was a regular consumer and distributor of child pornography?

The conclusion to be drawn from the above examples is not that service provider-user relationships are always at arm's length. In fact, other cases like *Aquacool\_2000 v. Yahoo! Inc.*<sup>115</sup> raise interesting possibilities. What happens when a service provider holds itself out as "committed to safeguarding 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?<sup>116</sup> Further, what if the provider 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 service provider'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 which 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 providers 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 service-provider-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,

---

115. *Supra*, footnote 1.

116. Yahoo! Privacy Policy, *supra*, footnote 19.

manipulated through personal information management applications, and accessed through Internet appliances.<sup>117</sup> 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.<sup>118</sup>

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."<sup>119</sup>

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 a relationship at arm's length.

---

117. See, e.g., D.H. Rimer and P. Noglows, "Internet Appliances and Universal Access" (1999), 4 iWords online: <<http://www.iwords.com/iword41.html>> (date accessed: May 23, 2000).

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

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

## VI. CONCLUSION

Online service providers are often our gatekeepers. More and more, we come to rely on them not only to provide quality information services but also to manage our information. By controlling an asset which is characterized more and more as the new currency of the so-called knowledge economy,<sup>120</sup> users depend on service providers to safeguard their personal information and private communications. This gives online service providers power over their users: power to control their behaviour; power to alter their outcomes.

Currently, relationships between provider and user are governed primarily by the law of contract. Given the increasing extent to which users repose trust and confidence in their service providers, it is unclear whether the legal duties owed by providers 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 online service providers are always fiduciaries - as if we could somehow generalize about a motley collection of private orderings - it would be equally misguided to conclude that online service providers are never fiduciaries. The conclusion offered here is more modest than either of these. It is simply that some service provider-user relationships display all of the constituent elements of a fiduciary relationship.

---

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