Online Service Providers, Fidelity, and the Duty of Loyalty

IAN KERR*

We are losing control over ourselves. Our lives are no longer our own. We are bargaining ourselves away. The nature of this Faustian bargain in our brave new economy is straightforward: we are offered convenience and the speed of Hermes in exchange for complete exposure to everything we say and do online.

The bargain is not always irrational. Ours is not a blind faith. When we place our trust in online service providers (OSPs) 1 and other information intermediaries there are, usually, built-in legal safeguards. Our trust is founded on a number of promises. It is founded on contractual representations that our personal information and private communications will not be collected, used or disclosed to third parties without our knowledge and consent. But are these promises – and the legal mechanisms used to enforce them – sufficient to protect our privacy interests? Or is there a need for other safeguards that transcend the world of private ordering?

"TRY THIS!"

Dig, if you will, a picture. Suppose that someone whose name you would not recognize has just sent you an email styled, "TRY THIS!". As it turns out, you do not even know that this email has been sent to you because your email account has been disabled. After trying to login to download your email, an automated message appears indicating that you have exceeded your available disk quota. You are told to contact Supernet, your OSP. After spending 20 minutes trying to circumvent the automated voice system, you finally speak to a real person who assigns you a file number and dispatches a technician to investigate the matter. Off to work you go, trusting that your service provider will resolve the problem in a professional manner. Later that day, while you are at work, the technician begins to comb through your all of your email without your knowledge – something that you had supposedly consented to in the fine print of your Terms of Service

agreement. She is searching for files with large attachments that can be deleted so as to free some memory and thereby re-enable your account.

During her search, the technician happens upon the "TRY THIS!" message and notices that it contains a few very large attachments with suspicious sounding names. Suspecting child pornography, the technician opens the attachments. Sure enough, the "TRY THIS!" message, sent to you without your knowledge or consent, contains images depicting young children engaged in sexual activity with adults. Horrified and angered by the images – and assuming all along that you are culpable – the technician informs her supervisor, who in turn contacts the police. The police request an electronic copy of the illicit file. Supernet decides to cooperate. Consequently, Supernet forwards the "TRY THIS!" message and several of your other private communications to the police without telling you.

It merits taking pause to draw specific attention to the fact that, because your account had been automatically disabled, the illicit "TRY THIS!" file (the existence of which remains unknown to you) has not yet been delivered to your inbox. Knowing this and knowing that there is no case against you without it, the police have instructed Supernet to resend the pornographic email to you so that it will finally be in your possession. On this basis, the police will then be able to obtain a search warrant, seize your computer and arrest you. Supernet complies. You are subsequently arrested, tried and convicted for the possession of child pornography.

Right about now, you can stop imagining. All of this is in fact quite real.2. In a decision rendered by the Alberta Court of Queen's Bench, subsequently affirmed by the Alberta Court of Appeal, it was held that Supernet's search of the customer's inbox, its decision to open the customer's email without his consent, the police's instruction to copy and forward this mail to them without telling the customer, and the further police instruction to resend the illicit file to the user, did not unjustly interfere with the customer's reasonable expectation of privacy.3

Narratives such as this help to illustrate the incredible power that OSPs and other online information intermediaries hold over their customers and clients. OSPs are by default the gatekeepers of informational privacy on the internet. By providing online services such as email, Web site space, or portals to various online consortiums, OSPs gain access to and control over a plethora of personal information and private communications belonging to each of its many users. Each user is therefore dependent on their OSP not only for the proper storage, maintenance and management of personal information and private communications but, also, for determining whether and when that personal information may be disclosed to third parties. In other words, the safeguarding of user information is largely dependent on the benevolence and good judgment of OSPs.

A CHILLING POSSIBLE WORLD

One might try to discern a kind of moral from the above narrative. Perhaps those of us concerned about personal privacy ought to make an effort not to depend so heavily on information intermediaries. Or, at the very least, perhaps we should not store our personal information and private communications in digital spaces that we do not ourselves control. A good moral though this may be, it is not especially helpful. OSPs almost always require the disclosure of personal information as a precondition of the use of their services.4 As well, most information intermediaries collect and log digital copies of every informational transaction that takes place on their system. Thus, even if you download all of your mail, delete it from the server, and store all of your communications on your own private disk space, anything that you send through the system is almost certain to be copied and archived by your information intermediary.5 The only realistic means of circumventing this practical reality is through the use of anonymizer and encryption technologies.6

Individuals are bound to experience a further loss of control when the internet takes the shape of some of its current visionaries and power brokers. For example, Larry Ellison (current Chair and CEO of Oracle Networks) and Scott McNealy (current Chair and CEO of Sun Microsystems) are not merely predicting but are also pushing-with-all-of-their-might for a networked world in which information is no longer stored on individual hard

drives or company owned servers but, instead, is stored on more powerful internet servers, manipulated through personal information management applications, and accessed through inexpensive internet appliances.7 In this chilling possible world, desktop computers become extinct and professional 'information management' becomes the big money maker. The scheme is to supplant personal computers (PCs) with internet appliances thereby shifting most of the sophistication away from the user and toward the network end. Internet appliances will contain very little hardware and almost no software – just a basic input/output system allowing a complete operating system to be downloaded every time the basic internet appliance is switched on. Given their simplicity, internet appliances will rely almost exclusively on lightening fast, centralized networks (owned, operated and controlled by companies like Oracle and Sun).8

The rhetoric in support of the shift to internet appliances is premised on user convenience. Why spend time and money buying and installing software, obtaining upgrades, configuring hard drives, managing disk space, or fine tuning settings on your PC when those tasks could easily be delegated to an network administrator? In an appliance-based world, it is said, network users will no longer need to carry around heavy equipment or deal with complicated hardware and software problems. Given the projected ubiquity of the internet appliance, users will simply need to carry a 'smart card' that allows them access to the network from wherever they happen to be. Because all software 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 for an internet appliance user to gain access to their information from anywhere in the world, as if sitting in front of their own machine.

To date, the main obstacle preventing the shift from a PC to an appliance-based computing universe seems to be the limitations of broadband and other high-speed internet technologies.9 Surprisingly little concern has been expressed about the fact that centralized (rather than end-to-end) computing will require all of our personal information and private communications to reside on Larry Ellison's, Scott McNealy's, or some other information manager's computers, leaving it solely in their control and,

therefore, vulnerable to misuse, illicit trade or even theft.10 If this chilling possible world is fully realized, we will have lost all control over our personal data and private communications. In such a world we will become completely and utterly dependent on the benevolence and good judgment of OSPs and other information managers.

FIDELITY

Because OSPs have access to and an ability to make copies of most if not all personal information and private communications that pass through their systems, they are already de facto personal information managers. The possibility of online privacy is therefore dependent on a user's ability to trust an OSP with their personal information and private communications. One might therefore ask: what are the moral and legal foundations for such trust?

The relationship between an OSP and an internet user is contractual in nature.11 That is, it is based on an exchange of promises. The success of such a relationship is therefore founded in the moral notion of fidelity – the faithful adherence to one's promises. Where fidelity is concerned, one does not owe a duty except insofar as one has promised. Contractual relationships that are entered into at arm's length generally require nothing more than a fidelity to those promises voluntarily assumed by either party. Consequently, it is thought that internet users can reasonably rely on their OSPs to do as they have pledged, but nothing more. Where the moral institution of promising falls short and an unfaithful OSP fails to fulfill its promises, the user has legal recourse through the law of contract.

Is fidelity a sufficient moral foundation to ensure online privacy?

Thus far, many OSPs have poor track records when it comes to living up to self-imposed privacy obligations. Consider, for example, the case of Aquacool_2000.12 As a subscriber to Yahoo!'s online services, Acquacool_2000 was promised that his OSP is "committed to safeguarding his privacy online." When he signed up for Yahoo! services, he was further promised that he would be notified at the time of data collection or transfer if his

personal data was to be shared with a third party. He was also promised that he would then have the option of not permitting the transfer. As the Yahoo! Privacy Policy 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…13

At the bottom of its Privacy Policy and throughout its Web site, Yahoo! also displayed the TRUSTe certificate, a logo which is familiar to many Internet users. 14 By featuring the TRUSTe seal throughout its Web site, Yahoo! made a representation to Aquacool_2000 and to all of its other subscribers that it will comply with strict privacy policies and procedures and that it will not disclose personal information to third parties without prior permission or some other legal justification.

In fact, Yahoo! even set up technological measures to further encourage trust amongst its subscriber base. In order to facilitate a frank exchange of information on its message boards, Yahoo! constructed an architecture that allowed message board participants to select a nome de plume and thereby communicate pseudonymously. This further assurance of online privacy helped create a very lively online discussion. Relying on the express promise that their personal information would be kept confidential, online interlocutors felt free to speak their minds and trade important information on a number of important and sensitive issues.

Trusting all of these safeguards, Aqucool_2000 decided one day to throw himself into a heated debate online about a publicly traded corporation known as AnswerThink Consulting Group Inc. After Aquacool_2000 posted a number of critical remarks about its management team, AnswerThink came down heavy on Yahoo!, threatening the world's largest OSP with litigation if it did not unmask the identity of its public critic. When push-came-to-shove, Yahoo! caved. Not only did it break all of its promises to

Aquacool_2000 by disclosing his personal information to Answerthink, it did so without ever telling him. Had Aquacool_2000 at least been notified, he would have had the opportunity to seek a protective order to enforce his constitutionally protected right to speak anonymously.15 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.

The case of Aquacool_2000 illustrates that the moral institution of fidelity and the law of contract will not always ensure our privacy online. As this case demonstrates, when it comes to keeping promises, OSPs such as Yahoo! often have competing considerations. Even if they do not engage in data-mining or otherwise profit in the information trade, when faced with the prospect of a third party lawsuit, a court order, or a request from the police, OSPs will often disclose rather than protect the informational interests of their users.

It is important to realize that, even if all OSPs kept all of their promises, the moral institution of fidelity would still prove insufficient as a means of ensuring online privacy. This is because not all OSPs promise to protect the privacy interests of internet users to begin with, nor are they always obliged to. In fact, some OSPs make it clear right from the outset that their users should have a low expectation of privacy.16 Some OSPs even 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.17

Given that some OSPs will break their promises with impunity and other OSPs make no such promises to begin with, fidelity seems insufficient as a moral foundation for ensuring online privacy.

THE DUTY OF LOYALTY

The duty of fidelity can be juxtaposed to the duty of loyalty. As we have seen, fidelity simply means keeping one’s promises. The duty of loyalty is quite different. Historically,

its foundations are derived from the status of the relationship rather than any of the undertakings voluntarily assumed by the parties.18 Consequently, where loyalty is morally required, the duties entailed by the relationship are said to pre-exist any specific promises that are pledged.19 Because the duty of loyalty derives from the nature of the relationship rather than from any promises voluntarily assumed by the parties, it follows that a duty of loyalty is not necessarily discharged simply by keeping one's promises.20 The duty of loyalty demands something more.

One special instance of the duty of loyalty that has been carefully developed and adapted by the courts of common law is known as the fiduciary obligation. The rationale underlying the fiduciary concept is quite straightforward. Where one party has come to trust another, there is some danger that the trusted party may decide to serve its own ends rather than those of the trusting party. In order to avoid such mischief, the fiduciary obligation protects those who by virtue of their relationship have come to depend on others.

Professor Weinrib once characterized the fiduciary obligation as the law's realization of the economic importance of fostering incentive by protecting relationships of interdependence:

> A sophisticated industrial and commercial society requires that its members be integrated rather than autonomously self-sufficient, and through the concepts of commercial and property law provides mechanisms of interaction and interdependence. The fiduciary obligation ... constitutes a means by which those mechanisms are protected.21

According to Professor 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. An interactive and interdependent society mandates the monitoring of trusting relationships in order to avoid their potential for abuse. According to Professor Weinrib, the hallmark of a fiduciary relationship is that

one party has the leeway to affect the legal position of the other, putting the latter at the mercy of the former.

Other scholars have held 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 they 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. ... (T)rust 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.22

The most commonly cited examples of traditional status-based fiduciary relationships, where one party gains access to another's assets include: trustee/beneficiary, solicitor/client, principal/agent, director/corporation, partner/partner, employer/employee, guardian/ward, doctor/patient, parent/child and confessor/penitent.23 However, 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 chosen not to limit the fiduciary obligation to the fixed category of status-based fiduciary relationships.

In a nutshell, the duty of loyalty requires the trusted party to act in the best interests of the trusting party. Seen from another perspective, the duty of loyalty forbids the trusted party from furthering its own self-interest where doing so would be detrimental to the best

interests of the trusting party. If a conflict of interests arises, the duty of loyalty demands the trusted party to remain faithful to the trusting party, despite its own reluctance to do so. To use one of our narratives from above as an example, if Yahoo! had owed a duty of loyalty to Aquacool_2000, that duty would require Yahoo! to keep its promise (not to disclose Aquacool_2000's personal information) in spite of the threat of litigation by AnswerThink.

Under what circumstances, if any, might an OSP be said to owe a duty of loyalty to its users?

The courts of common law have in some instances been willing to impose such a duty when the following four indicia of a fiduciary relationship can be adequately demonstrated:

> 1. The trusted party has scope for the exercise of some discretion or power;
> 2. The trusted party can unilaterally exercise that power or discretion so as to affect the trusting party's legal or practical interests;
> 3. The trusting party is peculiarly vulnerable to or at the mercy of the party holding the discretion or power; and
> 4. 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.24

It is quite plain that a number of the constituent elements outlined above are fully present in many OSP-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 OSPs access to internet users' personal information and private communications in a manner unparalleled by even the most powerful financial institutions or arms of government. Access to these informational assets allows OSPs to exercise power to the benefit or detriment of its users. Aquacool_2000, for example, lost his job as a result of Yahoo!'s discretionary use of his informational assets. When

Supernet exercised its discretion, Dale Weir went to jail. Therefore, to paraphrase Professor Weinrib, there are times when an OSP has the leeway to affect the legal position of its user, putting the latter at the mercy of the former. An OSP acting in bad faith has access to and therefore could: i) convert a user's private communications to its own or to another's advantage; ii) disclose confidential information to a competitor; or iii) turn over otherwise privileged evidence in the course of criminal or private litigation, etc.

At the same time – even if Yahoo! did hold itself out as willing to act in the best interests of its users – it is not clear that all OSPs always do so. To take an extreme example (mentioned above in footnote 17), an employer who provides internet services does not generally undertake to do so exclusively for the benefit of its employees. Offering such services to employees is but a means to the corporation's own ends. Even the most benevolent employer (whose policy permits employees to utilize its internet services for personal use) does not offer such services for the exclusive benefit of the employees. If an employee uses those services to illicit ends or in any other manner that is not in the best interests of the corporation, how could it possibly be said that the employer is obligated to use the evidence that it has gathered to serve the employee's benefit rather than serving the best interests of the corporation or its shareholders? 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?

CONCLUSION

More and more, OSPs are in a position to observe and record everything that we say and do online. Increasingly, we are forced to rely on them not only to provide quality informational services but also to store and otherwise manage our private information. Because OSPs are in a position of control, we have come to depend on them to safeguard our personal information and private communications. This gives OSPs power and discretion: power to control our online behaviour; and discretion to alter our outcomes.

Currently, relationships between OSPs and internet users are governed primarily by the moral institution of fidelity and the law of contract. Given that many OSPs will break their promises with impunity and other OSPs make no such promises to begin with, fidelity seems insufficient as a moral foundation for ensuring online privacy. Consequently, it has been suggested here that an alternative set of duties might be derived from the very nature of the relationship between some OSPs and their users. Where a fiduciary relationship can be established, it is possible to impose a duty of loyalty on some OSPs. Where a duty of loyalty is owing, an OSP must remain faithful to its users despite its own reluctance to do so.

It has also been suggested that the possibility of imposing a duty of loyalty on OSPs who have created a reliance interest (by holding themselves out as acting in the best interests of their users) is an increasingly important consideration. While it would be wrongheaded to conclude that OSPs always owe a duty of loyalty (as if we could somehow generalize about a motley collection of private orderings) it would be equally misguided to conclude that OSPs never owe such a duty. The conclusion offered here is more modest than either of these two extremes. The only claim that has been made here is that some OSPs display all of the constituent elements of a fiduciary relationship and that we might therefore justifiably require those that do to act in the best interests of their users in some instances. In those instances, the OSP will be required to safeguard a user's personal information and private communications is spite of its reluctance to do so.

As we move with the speed of Hermes towards a world where internet users have little or no control over there own information, the moral demand for OSP loyalty to trump commercial convenience ought to gain significance. Absent such a demand, we might be bargaining ourselves away.

* Canada Research Chair in Ethics, Law & Technology, Faculty of Law, University of Ottawa; Special Counsel, Technology Law, Nelligan O'Brien Payne LLP: iankerr@uottawa.ca. I would like to thank the Centre for Innovation Law and Policy, University of Toronto, and the Canada Research Chair program for their generous contributions to the funding of this project. I would also like to convey my deepest gratitude to Marcus Bornfreund, Heather Gray, Vanessa Gruben, Greg Hagen, Michelle LaPierre, William Karam, Kathy Mah and Christine Staley for all of their extraordinary efforts and for the high quality of research assistance that they provided. Finally, a very special thanks to Barbara Rockenbach for her incredible enthusiasm throughout the development of this important book, for her talented and expert editorial support, and for the patience and kindness that she displayed during the editorial process.

[1] 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 like email, and, as a result, frequently blur this 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 Inc.* v *Compuserve Inc.*, 776 FSupp 135 (SDNY 1991); *Zeran* v *America Online, Inc.*, 129 F3d 327 (4th Cir 1997); and also the *Communications Decency Act*. US Code. Vol. 47, sec. 230 (1996). The term "online service provider" is used throughout this article as a generic term to refer to any email provider, bulletin board operator, auction host, anonymous emailer, commercial or amateur web site, or any other provider of an online service who is not merely a conduit to Internet access but 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*.

[2] The above narrative is based on the actual case of *R* v *Weir*, 1998 AJ No 155, (ABQB 1998) and *R* v *Weir*, 2001 AJ No 869, (ABCA 2001). Similar cases have arisen in the United States: *US* v *Maxwell*, 45 MJ 406 (CAAF 1996).

[3] It is important to note that, in the actual Alberta case, Dale Weir, the recipient of the "TRY THIS!" email, was not an innocent person who was framed by the sender of the email. On the facts set out in *Weir*, the addressee of the message was a consumer of child pornography. Though this revelation certainly makes it more difficult to sympathize with Mr. Weir about the fact that his personal information was ultimately disclosed, the manner in which Weir's private communications were discovered and disclosed should be troubling to 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.

[4] Ian R. Kerr, "The Legal Relationship Between Online Service Providers and Internet Users," 35 *Canadian Business Law Journal* 419, 421-423 (2001).

[5] Ibid., 423.

[6] See, e.g., www.zeroknowledge.com; www.pgp.com. In spite of the relative accessibility and affordability of such products, most people have not yet adopted their use on a regular basis. As security tightens in the so-called 'War Against Terrorism', it is unclear what the future holds with respect to the use of these technologies as a means of enhancing internet user privacy. Given that Zeroknowledge Systems has recently discontinued carriage of the Freedom Network, its basic anonymizer software

[see D. McCullagh. Leading Anonymity System to End. <http://www.wired.com/news/business/0,1367,47337,00.html> (October 2001).], it appears as though these techniques for ensuring user privacy could become less and less available.

[7] Fried, I. Ellison's NIC Co. to Team with Sun. <http://news.cnet.com/news.0-1006-200-6375843.html> (June 2001); Bartlett, M. Net Appliances Sales May be Set for Take-Off. <http://www.newsbytes.com/news/01/063710.html> (March 2001).

[8] Rimer, D.H. and Noglows, P. Internet Appliances and Universal Access. http://www.iword.com/iword41/iword41.html (1999).

[9] Hopper, G. S. Who Needs a PC? Why Internet Appliances Will Succeed. <http://www.allnetdevices.com/industry/industry/2000/06/21/who_needs.html> (June 2000); Streitfeld, D. "For a Dead Idea, the 'Network Computer is Downright Sprightly'", *Washington Post,* 12 June 2000, sec. H, p.3.

[10] Schock, J. Death to Desktop!. <http://www.jasonschock.com/writings/dtd/index.php3> (April 2001).

[11] Kerr, 423.

[12] See Plaintiff's complaint, paragraph 6, originally filed at United States District Court Central District of California. <http://www.epic.org/anonymity/aquacool_complaint.pdf> (May 2000). This suit, *Aquacool_2000* v *Yahoo!* [hereinafter *Aquacool_2000*], was ultimately dropped for undisclosed reasons. 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. For example, in *Hvide* v *ACLU*, 770 So 2d 1237 (Fla Dist Ct App 3d 2000) the court 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 Doe1*, Court File No. 4592/98 (Ont Gen Div 1998) and *Irwin Toy* v *Doe*, OJ No. 3318 (Ont Sup Ct 2000). OSPs were ordered to reveal the identities of their, respective, clients alleged to have posted defamatory comments.

[13] Yahoo! Privacy Policy. <http://docs.yahoo.com/info/privacy> (April 1994) [hereinafter *Yahoo! Privacy Policy*].

[14] 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!Truste Validation Page. <http://www.truste.org/validate/361> (May 2000). See also Truste. <http://www.truste.org/> (April 2000).

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

[16] For example, Verio's *Acceptable Use Policy* spells out to its users that: "In general, the Internet is neither more nor less secure than other means of communication, including mail, facsimile, and voice telephone service, all of which can be intercepted and otherwise compromised. As a matter of prudence, however, Verio urges its subscribers to assume that all of their on-line communications are insecure. Verio cannot take any responsibility for the security of information transmitted over Verio's facilities." [See Verio Acceptable Use Policy. <http://home.verio.com/company/aup.cfm> (May 2000).]

[17] 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.

[18] RT Allen, "When Loyalty No Harm Meant," 43 *Review of Metaphysics* 281 (Dec 1989)

[19] Karen Hanson, "The Demands of Loyalty," 16 *Idealistic Studies* 195 (1986).

[20] Conversely, though parties to a contract by definition owe a duty of fidelity to one another, they do not necessarily owe each other a duty of loyalty.

[21] Ernest J. Weinrib, "The Fiduciary Obligation," 25 *University of Toronto Law Journal* 1, 11 (1989) emphasis added.

[22] Robert Flannigan, "The Fiduciary Obligation," 9 *Oxford Journal of Legal Studies* 285, 308 (1989).

[23] Ibid., 294.

[24] *Frame* v *Smith*, 42 DLR 4th 81, 97 (SCC 1987); and *Hodgkinson* v *Simms* (1994), 117 DLR 4th 161, 179-180 (SCC 1994).