

PRESENTATION TO:

XXXXXXXXXXXX
“DATA-OVER-CABLE SUMMIT”

**Potential ISP Liabilities & Due Diligence
Considerations:
"What Every Cable ISP Should Know *and DO!*"**

Tuesday, September 26, 2000

**SIMPSON, WIGLE
JAY N. ROSENBLATT, B.A., LL.B., &
HUSSEIN A. HAMDANI, Student-at-Law**

**Seminar to Guests of XXXX
Potential ISP Liabilities & Due Diligence Considerations:
"What Every Cable ISP Should Know *and* DO!"**

Tuesday, September 26, 2000

TABLE OF CONTENTS

PART I INTRODUCTION: An Overview of Potential Cable ISP Liability

PART II WHAT TO DO: WHAT IS DUE DILIGENCE?:

PART III WHY WORRY/WHY SHOULD I CARE?:

PART IV WHAT CAN I DO TO PREVENT THIS?: PRACTISING DUE DILIGENCE:

SCHEDULES

Seminar to Guests of XXXX
Potential ISP Liabilities & Due Diligence Considerations:
"What Every Cable ISP Should Know *and* DO!"

Tuesday, September 26, 2000

PART I INTRODUCTION: An Overview of Potential Cable ISP Liability

First off, let's discuss those that are affected by potential ISP liabilities -- the Stakeholders. Please see my "**Checklist of Liability**" in the attached Schedules.

Trends in the Law.

The United States appears to be the trend setters when it comes to which way the this area of the law will develop. Generally speaking, legal action appears to be heading in two directions:

1. The requirement that **ISPs act pro-actively**;
2. Complaint driven responses.

Because ISP liability is still so novel in Canada, it is harder to detect which direction the law is going. In Canada, no direction is clearly defined **at this time**.

In some Canadian jurisdictions, attempts are being made to clarify the liability of ISPs for materials carried on their system. For instance, reforms proposed by the Canadian Advisory Council on the Information Highway in its "Final Report of the Copyright Subcommittee," included a recommendation that operators of BBBs (and presumably ISPs), should be liable for materials carried on their systems as they are not common carriers. However, the operators should have a defence if they do not have actual or constructive knowledge of the infringing material and acted reasonably to limit abuse.

The CAIP (Canadian Association of Internet Providers) has established certain Policies and Guidelines that should be considered and we can talk about that later in this Presentation.

ISPs face potential liability in 2 general areas: first, by their own actions/inactions; and secondly, by the actions of their subscribers.

1) ISP's own actions or inactions

It must be noted that ISPs could find themselves in a lawsuit by infringing the privacy rights of their subscribers.

The privacy interest that may be of concern relates to the collection, use and disclosure of personal information by Web site operators about visitors to their site. Web operators may collect such information by requiring or encouraging visitors to register certain personal information in order to obtain access to the site as a whole or certain parts of the site. Web site operators may collect such information by requiring or encouraging visitors to register certain personal information in order to obtain access to the site as a whole or to certain parts of the site. Visitors may be asked to provide their name, address, email address, phone number etc. Web site operators may obtain additional

information by monitoring the specific pages visited on the site or other activity conducted on a site (for instance, logging of searches conducted).

The information captured by web site logs may or may not provide personal information about identifiable individuals. However, when combined with information obtained during the registration process, or potentially provided by the ISP, such information can permit the creation of a comprehensive profile of a particular user. The profile can then be sold to advertisers and other interested parties without the consent or knowledge of individual users and can be used to direct targeted advertising to particular users. The inappropriate collection of personal information on the internet may constitute unfair and deceptive trade practice.

2) **ISP liability because of the actions / inactions of their subscribers**

Often ISPs provide users with access to the internet, as well as the ability to upload materials to a shared Web server that may then be accessed by other users. Many ISPs also operate a Usenet news server which can be used to post or read messages. Some also set up e-mail distribution lists (or list servers) that may be managed by a particular user for an additional fee. Since many ISPs provide their users with e-mail access and the opportunity to host a website, this **doubles** the opportunity for users to get the ISP in a liability dilemma. Although there are specific liabilities that are confined to e-mail users or confined to website operators, for the most part, the liability issues for both will revolve around the content of the materials in question. For example, e-mail users or web site operators may take advantage of these facilities/resources/services that ISPs provide to send and /or upload unlawful, defamatory or infringing materials. Examples of just a few of the areas where either an e-mail user or a website operator could get the ISP in trouble are under copyright laws and other Intellectual Property laws, the laws of defamation, export control legislation, and criminal laws applicable to obscenity, indecency, gambling, dissemination of hate materials and other criminal offences.

In almost all cases, users can upload content directly to the ISP=s storage devices without such material being reviewed by the ISP. In the case of a usenet news server, messages are received from other sites in addition to those that may be posted by local users.

Reviewing or otherwise screening content uploaded by subscribers of even a closed system, such as an online service, is not usually practical.

In considering potential liability for materials distributed on the Internet, it is important to distinguish between an operator of a Web site, where material is created and stored, and a service provider, such as a cable company that is simply providing communication of the work. Liability is most likely to be imposed on the former, especially in cases where the operator of the web site is informed of the presence of harmful materials on its system and does nothing to remove them. In the case of

defamatory statements, the ISP may be considered to be a re-broadcaster of such statements and liable to the same extent as the author.

While an ISP that is simply a conduit for content which originates from third parties generally may not be liable for such content, it may be incumbent on the ISP to take reasonable steps to remove such information once it is made aware of its harmful nature. The extent of ISP liability is relative to the degree of control the ISP exercises over the web site operator and/or e-mail subscriber.

Whether liabilities arise because of an ISP's own actions or because of the actions of its subscribers, one very effective way in which to deal with these potential liabilities is the use of **Due Diligence**:

PART II WHAT TO DO: WHAT IS DUE DILIGENCE?:

BE PART OF THE SOLUTION & NOT PART OF THE PROBLEM:
DO SOMETHING ABOUT IT!

HOW TO COMPLY

- ! BE A GOOD BUSINESSPERSON;
- ! EXERCISE DUE DILIGENCE;

THE DEFENCE OF DUE DILIGENCE:

- ! **Let's assume that a complaint against you as a Cable ISP is issued, how do you minimize your risk?**
- ! **Implement Due Diligence.**
- ! **In order to successfully rely on the defence of due diligence, the directors, officers, and managers must be able to show, as a minimum, the following:**
 - ! the Board is ultimately responsible for compliance of the law;
 - ! if the Board chooses to delegate its monitoring responsibilities, it must ensure a system of adequate & effective supervision, regular up-dates of internet matters;
 - ! the person delegated with the responsibility of monitoring the users must have proper training and resources to carry out that responsibility;
 - ! the Board can rely upon its representatives and their reports;
 - ! *****establishment of a Code of Conduct, User and Privacy Policies, dealing with email and web-page use is essential, along with regular reviews of the Code of Conduct and Policies to ensure they are up-dated and verified as effective,*****
 - ! the Board must be aware of the "standard" in its industry, and comply with that standard;
 - ! minutes of the Board should accurately reflect consideration of internet matters;
 - ! the Board must be informed of & react to internet concerns that affect the company as quickly as possible (BE PRO-ACTIVE);

! **Other considerations:**

- ! implementation of Code of Conduct, and User and Privacy Policies;
- ! officers/management report back periodically to the Board of Directors;
- ! officers/management report substantial non-compliance to the Board;

- ! that the Board of Directors attempted to ensure compliance with laws through a periodic evaluation system;

- ! that the Board of Directors ensure, as a minimum, implementation of industry standards,

- ! attempted to ensure compliance with laws through a periodic evaluation system;
- ! that the periodic evaluation system must be mindful of, and implement, changing industry standards;
- ! that depending upon the nature and structure of corporate activity, there should be:
 - ! remedial and contingency plans for copyright and other infringements;
 - ! a system of ongoing monitoring;
 - ! ongoing training programs;
 - ! other examples of proactive policies;
 - ! ongoing supervision and inspection to ensure that the plans are complied with;
 - ! establishment of an internet sub-committee of the Board of Directors;
 - ! directors' review of legal compliance reports although they may rely upon corporate officers counsel and other informed parties;
 - ! directors substantiating that officers are promptly addressing liability concerns brought to their attention by government agencies;
 - ! notice that the system has failed;
 - ! proper response program;

PART III WHY WORRY/WHY SHOULD I CARE?:

BE PREPARED: - ANTICIPATE THE PROBLEM & BE PRO-ACTIVE WITH IT!!

WHY COMPLY:

! **TWIN MOTIVES OF: PROFIT & COMPLIANCE**

EXAMPLES OF POTENTIAL CABLE ISP LIABILITIES:

Please see **Checklist of Liability” attached to the Schedule**

Civil law and Intellectual Property Examples

(i) Intellectual Property (Copyright)

Copyright subsists in virtually all the content on the Site, including text, graphics, images, photos, audio visual clips, music, icons, avatars, drawings, maps, software, databases. The copyright for all content used on the site should either be owned by the Operator, or licensed under a written agreement giving the operator sufficient rights (ie. to allow further downloading and use by Users of the Site).

An ISP may be liable for its role in allowing a subscriber or user to utilize its facilities to infringe the rights of another. For example, under Canada's *Copyright Act*, any person who "authorizes" any act which is an infringement of is deemed to be a party to such infringement. The concept of "authorization" has been judicially defined to include such acts as the countenance, sanctioning or encouragement of infringing activities by other parties.

Recent case law in the US also suggests that operators and owners of online systems or networks may also be liable for infringement of copyright by other parties in certain circumstances. For example the operation of computer bulletin boards which are used to upload or download unauthorized copies of video games or photographs may constitute copyright infringement. In some cases the courts have stated that a lack of knowledge by the defendant of the specific unauthorized copying or the fact that the systems operator did not copy the infringing material was inconsequential to the question of whether there was copyright infringement, and ultimate liability.

It can be argued that an ISP cannot reasonably be expected to be aware of the contents of the vast amounts of information which may be uploaded to, downloaded from, and accessed through its system, or to know whether, in any particular case, the owner of the copyright has consented to the copying or distribution of any work by means of its system. However, it would be reasonable to expect an ISP to establish rules governing the use of its system, which may include prohibitions against the distribution of material that infringes the rights of the third parties. It is also reasonable to expect an ISP to take appropriate steps to restrict access to a particular user who, to the

knowledge of the ISP, is obtaining access to infringing materials stored on an interconnected network.

(ii) Privacy

The main privacy interest that may be of concern for purposes of activity on the Internet is the expectation of users that messages that they send by means of an employer=s or a third party=s computer system or network will not be intercepted. Although ISPs have a legitimate interest in ensuring that their systems are not used for unlawful or improper purposes, the interception of messages may be a violation of the users= rights of privacy.

Criminal Law examples

(i) Criminal Sanctions Generally:

It is arguable that an ISP could be prosecuted under the criminal law for aiding and abetting in the commission of an offence, such as the distribution of pornography or publication of hate literature. For example, liability could arise for "aiding" in the commission of an offence if the ISP was aware that the network was being used to commit an offence and performed some act for the purpose of aiding the offence. Similarly, liability for "abetting" the commission of an offence can arise if the person encourages its commission; this generally requires prior knowledge that the offence will be committed. If an ISP was aware that the network was being used on a continuing basis for commission of an offence, and having the means to do so, and took no action to prevent its continuation, the ISP may be liable for having encouraged the commission of the offence.

One way of determining the extent to which an ISP should respond is the severity of the alleged offence. The more serious the offence/complaint, the more aggressive the ISP should be in its response to same.

(ii) Defamation

A person may be liable for communicating intentionally, or by a negligent act, a defamatory statement to a person other than the person defamed. A person may also be liable for intentionally and unreasonably failing to remove defamatory matter on property in his possession or control. Accordingly, an ISP Web site operator or online service provider may be found to have "published" material provided by third parties if its fails to take reasonable steps to prevent the dissemination of defamatory material.

(iii) Hosting of Unlawful Material

1. Hate Messages

Under Canadian legislation dealing with hate material, an ISP could be liable for "communicating statements in any public place" if it permits hate messages to be transmitted on its system. Liability will depend on the scope of access that users have to the system, which will determine, in turn, whether the system could be considered a public place. While the ISP is providing a medium through which others can communicate statements, the question of whether or not the ISP has any responsibility for the contents of such statements will depend on the control that the ISP exercises over such contents. The ISP may be found liable for "communicating statements" if its representatives are aware of the contents of hate messages being transmitted through the system and they have the capability of deleting such messages but fail to do so.

2. Pornographic or Obscene Materials

An ISP may be liable for having published, distributed or circulated pornographic material where the ISP knows such material is available on its system and the ISP has the capability of deleting or restricting access to such material but fails to do so. For instance, a Canadian ISP could be charged with distribution of obscene material under subsection 163(1) of the *Criminal Code* for its role in facilitating access to such material. It will be a question of fact in each case as to whether the ISP has sufficient knowledge and involvement to be a party to the publication, distribution or circulation of the information. The risk of liability would be greater where the ISP (or another person involved in its operation, such as the moderator of a news group) takes an active role in reviewing the material prior to its distribution on the system. An ISP would be less likely to face liability in respect of materials which are available from other internet sites and where its only role is to provide connectivity to the Internet.

PART IV WHAT CAN I DO ABOUT IT?: PRACTISING DUE DILIGENCE:

1. **AWARENESS & COMPLIANCE**

Research, study and implement existing regulatory guidelines and policies. Keep up-to-date with any developing laws or legal trends, than attempt to formulate internal and subscriber policies with these developments and trends in mind.

2. **ACTIONS**

(i) **Learn**

ISPs must continuously learn the law in this field. Attend more seminars, symposiums and other venues where information in this area can be disseminated., and join the appropriate industry associations. **Be pro-active.** Assist in the development of new regulations by becoming involved with associations or groups that lobby the Legislators.

(ii) **Contracts**

The best defence to a potential liability is a well drafted contract. Good contracts will have, as a bare minimum, the following provisions:

A. *a broad definition of 'content'*

B. *Rules of online conduct, including internet access and conduct*

C. *Rights*

 (1) *ISP*

 (2) *Subscriber*

 (3) *Third Parties*

D. *Duties*

 (1) *ISP*

 (2) *Subscriber*

E. *Restrictions on conduct*

(iii) **Acceptable Policy Use**

An ISP can minimize its risk of liability by taking certain steps to help establish a due diligence defence to a charge of publication or distribution under subsection 163(1) of

the *Criminal Code*. This includes implementing an "acceptable use policy." (Generally speaking, and at a minimum, this policy would state that users may not use the Web site in order to transmit, distribute, store or destroy material (a) in violation of any applicable law or regulation, (b) in a manner that will infringe the copyright, trademark, trade secret or other intellectual property rights of others or violate the privacy, publicity or other personal rights of others, or (c) that is defamatory, obscene, threatening, abusive or hateful). This policy should be incorporated into each subscriber's agreement with the ISP.

(iv) Industry Standards

Find out what the industry association are and join then determine the industry standards are and equal or better them. For ISPs, the industry standard is most likely that set by the Canadian Association of Internet Providers (CAIP). CAIP has responded to some of the concerns regarding ISP liability in its Privacy Code and Code of Conduct. Section 5 of the Code of Conduct provides that CAIP members will not knowingly host illegal content and that CAIP members will share information about illegal content for this purpose. While such rules will not in themselves provide immunity to ISPs, they may help an ISP demonstrate an intention to keep harmful content from being carried on its system.

(iv) **Respond******

An ISP **MUST** respond to any obscene material brought to its attention and must respond in an appropriate and timely fashion to such behaviour ((complaint-driven responses)).

Stakeholders

1. **ISP's;**
2. **Internet Users;**
3. **the Innocent Third Parties;**
4. **Employees;**
5. **the Business;**
6. **Business Owners;**
7. **Investors;**
8. **Directors, Officers and Key Employees;**
9. **Shareholders;**
10. **Lenders;**
11. **Press/Media;**
12. **Other Divisions of the Corporation;**
13. **All Levels of Government/Policy Makers**

- 14. *Rules of online conduct, including internet access and conduct*
 - (i) *Chain Letters*
 - (ii) *Commercial Communications*
 - (iii) *Inappropriate Communications*
 - (iv) *Respect for Intellectual Property and Proprietary Materials*
 - a. *Respect Laws*
 - b. *ISP's right to terminate*
 - c. *ISP's indemnity*
- C. *Rights*
 - (1) *ISP*
 - a. *General Rights*
 - b. *Intellectual Property Rights*
 - (2) *Subscriber*
 - a. *Right to access the internet*
 - b. *Intellectual Property Rights*
 - (3) *Third Parties*
- D. *Duties*
 - (1) *ISP*
 - (2) *Subscriber*
- E. *Restrictions on conduct*
- F. *Increasing network usage and traffic*
- G. *No Spamming*
- H. *No Maintaining Online Mailing lists*
- I. *Attempting to circumvent or bypass Security System Measures*
- J. *Commercial Use of the Internet and Online Services*
- K. *ISP's Right to Monitor and Communications Privacy Policy*
- L. *Server Maintenance*