MASTERING E-COMMERCE AND GLOBALIZATION

Étienne Dubreuil
Heenan Blaikie SRL/LLP
1250, boul. René-Lévesque Ouest
Bureau 2500
Montréal, Québec H3B 4Y1 Canada
edubreuil@heenan.ca

Abstract: This paper is a survey of Canadian and American legislation as well as European guidelines in the area of electronic signatures and electronic identities. Differences will be commented upon.

Keywords: privacy, electronic signatures, electronic identities, e-commerce, fibreoptic, metacapitalism, OECD, Global Village

1. INTRODUCTION

For the purposes of this discussion, the expression “E-Commerce” is used in its most global sense as the transmission electronically by telecommunications means of any information on the web. The expression will therefore cover personal chats, personal e-mails, business e-mails, and even business-to-business transactions.

1.1 What is so different about E-Commerce?

It's the way it travels to get from its point of origin to its destination. It requires a telecommunications infrastructure be although it does not require that the whole of that telecommunications infrastructure used as it may jump from infrastructure to infrastructure travelling the world around in order to be reassembled at the place of destination.

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: [10.1007/978-0-387-35696-9_19](https://doi.org/10.1007/978-0-387-35696-9_19)

E. Nardelli et al. (eds.), *Certification and Security in E-Services*

© IFIP International Federation for Information Processing 2003

When one considers that the world wide web is a planetary phenomenon, one will conclude that any telecommunications infrastructure may suffice provided that one acknowledges that older infrastructures that use twisted pairs of copper wires will be at a net disadvantage when compared to the capacity of information that can run onto a fiberoptic strand. Is it possible to consider that every country in the world will have a fiberoptic telecommunications infrastructure to maximize Internet speeds and the massive amounts of information available? That is doubtful. Indeed, when one considers the financial disasters that have been caused by the bursting of the dot com bubble, the massive losses in the marketplace and the bankruptcies that some of the richest nations in the world have known in the telecommunications sector, we must recognize that fiberoptics and the most proficient routers on the web will require amortization over large volumes of users and large volumes of bits passing through the system hopefully using as much band width as possible. In reality, we must disassociate the content from the infrastructure in order to allow foreign contents to pass on domestic infrastructures and provide arrangements for the transport of those bits of information.

In networking the web, at a minimum, we will likely realize that universities around the world will enjoy access to the upper scale of the telecommunications infrastructure available in a given country while the general public may have an Internet access of a significantly different nature.

In the telecommunications environment, the physical access to telecommunications infrastructure even from one country to another does not appear to create any major difficulties. Indeed, countries around the world have been used to the interconnection of their network with foreign networks, sharing in costs and revenues generated and resulting from the inward and outward traffic flows. Perhaps that was back in the 1980s as the 90s have seen an acceleration of the challenge to the established rules by way of transit traffic and refile, telecommunications transport techniques, which allowed to by-pass domestic networks.

The advent of the digital technology has complicated things even further in that the packet switching technology allowed the streaming of bits of information not necessarily sequentially arranged providing the means to send such bits throughout various interconnected networks, ultimately guiding the information travelling at the speed of light to its point of destination and then being re-configured or re-arranged before delivery to the intended user. As a result of those technologies, the price for the transportation of bits of information onto the international telecommunications networks has dropped considerably. The promises of E-Commerce on the Internet created a theoretical demand for capacity on the international telecommunications network grid under one hand while IP

telephony was holding itself as the new low cost technology almost substitutable to the established international telecommunications common carriers. As a net result, the Dot Com bubble burst, IP telephony has not proven itself to be a viable substitute to the traditional telecommunications standards. From a financial perspective, those physical networks that were built to accommodate tremendous volumes of activities lost a tremendous amount of their inherent value and the value itself was created by added services including virtual networking — indeed within 10 years, a major shift in all the paradigms. Wireless networks can perform voice and data services as well as land lines and even less financially favoured countries can build a wireless telecommunications network which will allow tremendous competitive potential including the possibilities of accessing the traditional networks already established.

2. GLOBALIZATION

For me, the introduction of technology became the most important building block for globalization. The other building blocks were the introduction of capitalistic-based economies which allowed the human entrepreneurial spirit to flourish, the liberalization of movements of goods and services, the introduction of lower barriers to entry, (to a certain extent the levelling of plainfields) the increased reliance on technology for business management and the growth of business-to-business E-Commerce as an acceptable basis for a stable commercial relationship.

There are certain consequences that we must acknowledge from the foregoing. For instance, the chains of supply and demand are enjoying greater satisfaction in the execution and management of business relationships. Indeed, we have facilitated the communications of all required information between all the actors in any given supply and demand chain. In their book “*metacapitalism*” means and Schneider analyse the e-business revolution and its promises from an economic standpoint concluding that the chain of supply and demand can be arranged to work on a 24/7/365 basis without knowing any geographical boundaries. If there is one common denominator to all the participants in any such chain it will be the use of the Internet as a means of communications between the parties. The advantage is obvious it can be instantaneous, in multimedia format, interactive and technologies do exist to make this whole exchange quite safe from unwanted intrusions. This is fine when one views this approach of metacapitalism from a business and economic vantage point. For lawyers, however, it poses tremendous challenges in that the Internet is everywhere and nowhere at the same time. It comprises a series of bits of information moving around the

globe through a maze of interrelated computers ... a nightmare for anyone involved in the contractual analysis, best practices implementation a non-regulated environment and no one to direct traffic (read here no higher authority to refer to in case of problems).

3. CERTAIN ISSUES TO BE CONSIDERED

- On the Internet, where are the traffic cops?
- What is confidential?
- What is legal, what is illegal? (Consider for a moment the possibility of having a submarine engineering contract plan forwarded from a U.S. engineering firm to a colleague in Greece with bits of information passing through telecommunications networks controlled by unfriendly nations. Obviously, in such instances people might want to consider some dedicated networks and major encryption. However, from a legal standpoint this poses a real challenge).

Both foregoing issues are traditionally addressed to a rules book or a legal corpus acknowledged by the parties as the “rules we will follow”. Those rules may be a set of laws, rules, regulations, contractual arrangements. Traditionally, commercial rules of trade will appear by way of waybills or other such devices, which have been recognized as binding each participant to a transaction under the respective applicable laws or treaties between the countries. Those have been set either by the world trade organization while others have been developed under the hospices of the international telecommunications union, the united nations or other supra-national bodies but have served to address matters of regulating trade and commerce on an international level.

The Internet as such unlike activities such as radio frequency allocations international transport rules by air or terrestrial or by sea which are of long-standing tradition and have developed solid rules that parties abide by, the Internet has developed and is in fact being used while its rules and regulations are still to be made

4. ARE THERE NO RULES IN CYBERSPACE?

If there were none, there would be absolute chaos and such is not the case. To date, the Internet has been approached by the various countries on a self-regulation basis. Indeed, there are some elements of regulation in that the various networks that are inter-connected to one another in order to allow traffic flow must accept the telecommunications protocols and, at least from

a technology standpoint, there is some level of standardization. However, information or content has become a commodity, which is available on the Web, an asset which has value and which may be subject to transaction by itself.

At the very low end, these assets are situated somewhere in Cyberspace in a host computer. The more valuable information will be entrusted to a content provider in order that its access be controlled and its value protected through licensing, maintenance services, updating services. As a general comment, it should be the responsibility of the original supplier of the information to impose the standards for accessing the information. Perhaps this model works best in a commercial applications environment where a contractual relationship will serve as the law between the parties. It should not be forgotten that in commercial applications, at least the parties are aware of their respective interests and we would be entitled to presume that the parties using the Internet for such purposes would be sophisticated enough to put in safeguards that protect what they want protected. The matter is quite different, however, where the Internet is not being used for commercial purposes but is being used for personal matters. There, governments remain the only real defender of the rights of their nationals.

The regulation of the Internet could, however, be counter-productive in certain circumstances. For one thing, even most generally admitted concepts may not be the object of a similar interpretation between the nations. Secondly, certain countries could find in the resistance to such regulations a mercantile opportunity allowing, within their territory, the hosting of materials that have been, either proscribed or outlawed in other countries or worse, by posting pirated works available at discounted rates. On the basis that the current thinking of liability seems to attribute legal liability to content providers and host servers as being subject to the laws of the land in which they are situated, various legal loopholes can be exploited by locating host servers outside of those territories that try to achieve certain levels of regulations of the Internet. This very specific matter will be addressed by my partner Lucie Bélanger from a taxation angle.

5. GLOBAL VILLAGE

It certainly seems clear that this planet of ours has shrunk with the integration of telecommunications and the networking of computers through the telecommunications infrastructure. This phenomenon has traditionally been referred to as “*global village*”. However, from a legal perspective, the phenomenon is far from a global village. If it were one global village, we would most likely be working under one set of rules. The reality is way

different in that this global world is constituted from very many sovereign states each having to respond to its own constituency in adopting laws, rules and regulations that best serve its national interests as well as the interests of its nationals.

– How efficient are the rules of one state against those adopted by another?

That is a very complex question. Those questions are usually addressed in the realm of private international or public international law. The difficulty with international law is the enforcement of any sanctions that may be imposed by one party on the other.

Let us consider for one instant the Yahoo case. Yahoo of Santa Clara was sued before a French court by two groups of activists (The International League Against Racism and Anti-Semitism and the Union of Jewish Students). The lawsuit was brought on the basis that Yahoo was permitting an auction through an auction site it had opened in order to sell nazi memorabilia. Under French law, it was alleged that such items could not be the object of commercial traffic as they constituted racist materials and could not be offered for sale in France. The French court ordered Yahoo to block French citizens from accessing the items and imposed a monetary penalty in the event of non compliance. It should be noted here that the items for sale were on Yahoo's U.S. site and not on its French site. The U.S. court decided that the French court had no jurisdiction to decide what speech either prohibited or permitted was permitted in the United States soil although it had full competence to do it in France.

The French court's ruling was therefore non-enforceable in the United States. Nice legal battle but the issue was far from resolved. It was really the commercial pressure that was put on Yahoo from the outside that prompted that company to remove the hate-related materials from the auction site. The Yahoo case perhaps best illustrates that public opinion is sometimes more effective than anything else.

If you try to articulate at its simplest expression the various levels of sanctioning that should be considered and why in connection with the use of the Internet, it would seem to me that we would be trying to ascertain and attribute civil liability on the one hand and criminal liability on the other. Criminal liability is part of public law. It is the state which rules that a conduct, a behaviour, or other action or act should be prohibited as a question of social or national interest and should be punished as a crime either by way or imprisonment or fine. This part of wrongdoing or wrongful conduct must be deemed to be serious enough in nature to warrant the state's intervention, however, as addressed earlier there is no guarantee that each state will consider an action as warranting its intervention in the same way.

In connection with civil liability, normally referred to as liability of non-criminal nature implicating one party in its rapport with another party, the

issue must be reduced to what is a wrongful act giving rise to a claim in damages in favour of the aggrieved party. To date, two levels of concerns have expressed this preoccupation. The first deals with the rules governing protection of content, while the other deals with rules governing the protection of the users.

6. PROTECTION OF THE CONTENT

There appears to be a sense of defeat when it comes to protection of contents on the Internet. And perhaps it is not unjustified. On the other hand, to the extent the content is worthy of protection, its protection on the Internet would seem to me to pose similar challenges as that encountered in the broadcasting industry with the sale of illegal decoding devices or satellite smart cards, both activities preventing the legitimate rights owner and service providers from obtaining their fair compensation including copyright royalties.

Considering that the broadcasting industry is, at least in Canada and in the United States, a highly regulated industry, which has set itself up with proper safeguards, rules and regulations and controls, it has benefited from the intervention of lawmakers both from a civil as well as from a criminal law approach. Again, at the risk of sounding repetitious, we are dealing with an activity that has organized itself with set rules. It must be said, however, that in Canada, the use of Internet to send content to users is not considered a broadcasting activity although it is a sending of a telecommunication. Broadcasting rules and regulations do not apply to the Internet and until further notice the regulators of telecommunications have decided not to regulate the Internet as such. And perhaps understandably so. The Internet being by its very nature a network of international networks of computers it is really not controllable as a whole unless the sum of its moving parts follows some agreed rules. Without pre-agreed rules adopted through some supranational organization, it is next to impossible to have a coherent approach to the regulation of the Internet. Once launched on the Internet, a content will be made accessible to any and everyone who can locate its host which, by the way, could have a mirror somewhere else and so on and so forth the extent of which renders next to impossible the identification of which host is being accessed by whom and when.

The Napster matter although principally concerned with copyright infringement, was in fact from a technology standpoint, rather simple. The host computer was situated on U.S. soil while content providers and users were worldwide. Could the legal system be as efficient in tracking down the alleged offender if the same content was duplicated on numerous hosts each

situated in different jurisdictions and ultimately in one where certain works are not recognized from a copyright standpoint?

Is Cyberspace lawless? Perhaps we can find some elements, which may lead us to think that the Canadian Cyberspace may allow some tangible enforcement process in connection with copyrighted contents. The matter is far from resolved as we will have to see whether the Supreme Court of Canada wishes to change the state of the law or not before any final pronouncement can be made. Be it as it may, our courts have recently looked into the matter of liability for the collection of applicable royalties in a case we generally refer to as the Socan case. Socan is the society of composers, authors and music publishers of Canada. It is a body recognized to administer, on a collective basis, royalties which are payable to its members. Royalties are set under a tariff that it proposes for adoption before the Copyright Board of Canada, which holds a public proceeding for rendering its decision. In the Socan case, the Copyright Board decided, *inter alia* to exclude most of the Internet intermediaries from liability to pay the copyright royalties. This decision was appealed and it is the decision of the Federal Court of Appeal, which is interesting. The legal complexities which gave rise to the Copyright Board's decision was that it was of the opinion that Internet intermediaries' activities are a kin to telecommunications common carriers activities in that they have no authority on the content and therefore, as providers of the means of telecommunications for the communications of copyrighted work, they were not responsible for the collection of the royalties. Noteworthy is the fact that all participants were in agreement that a simple passive role of supplying the infrastructure would not suffice to bring liability for royalty payments. In the analysis, it was found that it was not feasible for Internet access providers to monitor and control in any systematic way, the contents transmitted to their subscribers. The court found, on the other hand, that operators of host servers from which infringing material is transmitted should be viewed in a different way given that they have a contractual relationship with the content providers. The court also noted that other countries such as Japan, the United States, Australia and the European Union, legislation had been enacted in order to shield Internet intermediaries from copyright liability as to copyrighted materials stored on their servers unless they had received constructive notice of infringement. Furthermore, the court determined that Canadian copyright law generally does not apply to communications by telecommunications means originating from outside Canada and that it is the place of origin of a communication that determines the situs of the communication. It would follow that a communication will occur in Canada if it originates from a server which is situated in Canada. As a first observation, we note that under this reasoning, the Canadian Copyright Act would not be applicable where

the originating server of the content is situated outside Canadian territory. Furthermore, what is recognized as a copyrightable work in Canada may not be recognized as a copyrightable work in another country and therefore even the court determined that:

“Ultimately, the satisfactory resolution of these transporter problems will require supranational solutions.”

Therefore, perhaps reopening the copyright treaties may be a solution to envisage. The court did, however, remark that in its view a royalty could be made payable in Canada in respect of a communication by telecommunication that has a real and substantive connection with Canada. That test of real and substantial connection could also apply to locating the infringing activity of authorizing a communication “that occurs where a content provider hosts copyright material on a host server.” The conclusions that we draw from this case are that obviously where the server is situated is definitely a factor to be considered as allowing attribution of domestic jurisdiction and that depending on the circumstances, national jurisdiction could be acquired where the facts support that there is real and substantial connection with the county which is being requested to assume jurisdiction. In many instances, hosting servers and other Internet intermediaries may have activities that would satisfy this test in a sufficient manner to attribute jurisdiction in a country where sanctions can be enacted from copyright infringements or other infractions dealing with prohibited contents circulation.

Granted this is far from settled law. However, the Socan case leads us to believe that domestic legal systems will not stand idle and would try to assume jurisdiction in redressing what, in their domestic law, would constitute a wrongful behaviour.

Dare we suggest that the organization for economic co-operation and development (OECD) could assume the leadership in this regard in promoting treaty-based legislation? The words treaty-based legislation only refers to the fact that a treaty is agreed to between various countries in order to enact a model type of legislation. OECD was instrumental in promoting legislation criminalizing money laundering activities as well as corruption of foreign civil servants, laws that have in Canada become part of the criminal law corpus. It should be noted that recently (2000), OECD published guidelines for consumer protection in the context of electronic commerce and published in May of this year a best practices to those guidelines going as far as drafting suggested language to be used in connection with E-Commerce transactions.

Clearly, the OECD whose secretary-general is one of the founding members of our firm has asserted credible leadership in matters dealing with Internet.

7. PROTECTION OF THE USER

In 1998, the OECD published guidelines on protection of privacy in the electronic environment and in particular the Internet. The basis of the guidelines revolved around the reaffirmation of its own guidelines in privacy and confidential information as applicable to the new technology, which could be used to collect and deal with private data. The foregoing guidelines encouraged industry to adopt rules of governance in connection with the use of their networks and stimulated public awareness and education. This organization acknowledged that the concepts regarding privacy perhaps not receiving unanimous interpretation, although the principles of privacy for those countries that had adopted them in their national law were viewed as a fundamental right.

The guidelines, which had been set by the OECD, enshrined certain principles such as:

- Limitations on personal information collection.
- Personal data collected should be relevant for its intended use, complete and accurate.
- It should be used only for specific purposes.
- The information should have limited use.
- There should be a reasonable assurance of non-disclosure and safekeeping.
- The process of collection, storing and use of personal information should be transparent.
- Each individual should have the right to know what information is available on him including the right to bring corrections to such information.
- Responsibility of the holder of the information should exist to make sure that the foregoing principles are respected.

If metacapitalism and the promises of economic growth held by beat be activities are to come true, individuals and businesses must be reasonably assured that communications by telecommunications on the Internet will be afforded the protection and the safeguards suggested by the directives above. Indeed, some softwares exist to assure privacy (platform for privacy preferences “P3” – Trust-E and E-mail preferences services) just to name a few, user confidence must be built up with regard to the privacy of their communications.

8. WHAT DO WE MEAN BY PRIVACY FROM A LEGAL PERSPECTIVE?

Most certainly, this is a fluid notion the characteristics of which may vary from country to country. Most certainly, it involves the right to control information which affects oneself and should be viewed as such as a fundamental right of a person which right must be exercised, however, taking into consideration the context of the exercise of the same right by another individual or another person. In Canada, the Supreme Court has discussed privacy as a right not as much in say but more as a fundamental right of reasonable expectation of privacy. This right will therefore have different significance depending on whether one is in the private or public domain and may be subject to some reasonable limitations such as territorial limitations, limitations, which are inherent to the person, and limitations which are applicable by reason of the informational context.

Murray Rankin wrote almost 20 years ago in *Privacy & Technology* “a Canadian perspective”:

“The claim of information privacy assures that all information about an individual is fundamentally the property of the individual; for him to communicate or withhold as he determines. Indeed, this is a Canadian perspective.”

9. CONCLUSION

Canada and the province of Quebec have legislated privacy safeguards for the benefit of individuals and have enshrined those safeguards in charters of rights. These charters set a threshold against which other laws will be judged in matters of privacy. While the state may be liable for adopting laws that might infringe the expected privacy rights of its citizens, it remains up to each individual or to each person to assume the control and manage and enforce such a personal fundamental right. It is my personal point of view that this responsibility should govern the conduct of anyone using the Internet.