Legal Consequences of Packet Inspection

Mark Perry
Dept. of Computer Science - Faculty of Law
University of Western Ontario
London, Ontario
mperry@uwo.ca

Thomas Margoni
Dept. of Computer Science - Faculty of Law
University of Western Ontario
London, Ontario
tmargoni@uwo.ca

***Abstract*—Sophisticated network management is now very common. However, the legal consequences in terms of the liabilities, whether civil or criminal, of the Service Provider in connection with the type of management used have been poorly explored. In this work in progress, we identify the research questions, the methodology and work hypotheses of our future research.**

***Keywords*-Deep Packet Inspection; Telecommunication Intermediaries; ISP Liability; Safe Harbours.**

I. INTRODUCTION

Access to the internet is seen by most as a fundamental right [1][2]. It is not just about leisure, email, tweeting, accessing Facebook or Google maps, but rather access to the information that has become a prerequisite to freedom of expression in the modern world. It is about fundamental rights connecting the services for citizens from governmental bodies, such as obtaining a birth certificate, a temporary working permit or to e-vote (where applicable). In the 21st century, the internet has become the means to achieve a deep realisation of fundamental rights such as freedom of association, of thought, of pluralism, of communication, of realisation of one own happiness [3][4].

Most importantly, the Internet itself is not about commerce. This is a key point. It does not mean that you cannot commercialise your products or services on line. On the contrary, the creation of new business methods based on the virtualisation of value has been, is, and will be of fundamental importance for the development of economies especially during the current harsh financial times. Nonetheless, the nature of Internet is not to be a network of businesses. It is to be a network of people, who might want to do business, to form a Facebook friend (or to unfriend) somebody, or to elect their representatives. The internet is a platform that has become a social paradigm of our time and of our anthropological evolution as human beings [5].

We are living during a revolution that is much more pervasive than what the Industrial revolution has been some 250 years ago. The economic, social cultural, legal and anthropological modifications that happened then are still under analysis, though nobody doubts that it has been a major cornerstone in human evolution. It has also been said that for the success of the industrial revolution more fundamental than the invention of the steam engine has been the legal invention of the limited liability for incorporations [6]. Through this legal tool, the allocation of risk and benefits changed the old paradigm: it allowed, fostered, and offered the fundamental incentive to the accumulation of capital necessary for risky enterprises that otherwise would have not been undertaken.

The digital revolution is happening simultaneously almost wherever in the world, and in just a fraction of the time it took for the Industrial one. Let us take the example of Blu-Ray. On a single Blu-Ray disk we can store many times more information than that of a new desktop computer of five years ago, *i.e.*, comparing the five dollar disk to the drive of a 3,000 dollar computer. However, the Blu-Ray system will not be the commercial success if its predecessor – the DVD. This is despite it winning the battle against the competitor standard, the High-Definition DVD, HD-DVD [7] – resembling the Betamax versus VHS battle of a few decades ago [8]. In five years, or maybe 5 months, there will be no need for support any more. More and more the latest cutting-edge devices we can buy – or helplessly admire on the shelves of computer stores – come without an optical reader. No DVD, no Blue Ray, no ComboDrive. Did anybody noticed the progressive disappearance of the floppy disk? Although geeks, such as the authors, may keep on our desktop a five and a half inch floppy disk as an archaeological relic, as it was the leading technology of but a few years ago, Moore was right [9].

Information and knowledge will need no physical support any more in order to circulate. And every day somebody reminds us that we are living in a knowledge society or that now the businesses are based on information assets. Expressions such as Software as a Service, Cloud Computing, Web2.0, or their business implementations, GoogleDocs, OviMaps, EC2, etc. are nothing more than a confirmation that everything is translated into information. A lot of information is sent over fibre-optic cables or 3G or 4G networks. Physical support is becoming too slow, and too costly, and do not offer the same level of control that streaming and packet sniffing permits. Everything will be sent over the internet, such as money and knowledge, and furthermore relationships formed.

 ISBN: 978-1-61208-122-9

In terms of economic analysis of the law, to allocate upon users, or even worst, telecommunication intermediaries, the liability for what is transmitted over the Internet (such as that which may violate someone else's intellectual property or privacy, etc.) can be analogised to corporations having to pay for the their debts with the personal assets of the shareholders, beyond the face value of their shares. No limited liability any more. However, whereas governments and policy drafters have never put industrial revolution legal key concept under debate, the same does apparently not hold true for the digital revolution key concept. To charge Intermediaries operating as mere conduits with the legal liability of the potentially infringing content transmitted on their wires would stop the digital revolution, it would stifle innovation, it would disrupt new business methods in favour of the rent-seeker positions of those who have based their success on the old business paradigm. Not differently from those farmers that many years ago started suing the first commercial flights for trespassing the air over their fields, just because Blackstone Commentaries reported that property is a right that extends over the land and up to the stars [10].

In light of this futurist scenario, some legal amendments such as the "three strikes and out" provision of the HADOPI legislation in France [13], or proposals that at regular time intervals pop up internationally, to modify the liability profile of internet intermediaries, such as ISPs, are particularly threatening. In particular, the former states that if somebody is allegedly illegally downloading copyrighted material three times, her Internet connection will be cut. No more downloads. No more Facebook friendships. No more birth certificates. No more e-voting (where applicable). Whereas the protection of the legitimate interest of the copyright holders is out of question here, and it is widely agreed that measures to foster their business methods are necessary, the guise which many times these reactions take, as in the HADOPI legislation, are the worst we could image: the declared and legally sanctioned statement that the a few bucks of royalties are more important than constitutionally recognised rights. It is surprising and frightening that a country such as France (that has spread the light of Enlightenment over most of the world only a few centuries ago) falls back to such an obscurantist vision of the future.

For these reasons we aim to analyse the current situation in terms of the transmission of information over the internet. We look to information flows in a switched packet network, how it can be identified by the likes of deep packet inspection (DPI), the legal consequences of such identification (ISP liabilities), and which are the best policies that should be implemented.

II. How information is sent over the Internet

The default for the internet (TCP/IP) is based on sending pieces of data over the net as fast as possible. Communications are chunked into packets that are sent over the network toward their common destination. Packets of the same communication may take different routes to get to destination in the most fast, efficient and non-congested way. So, packets of different kind and of different communications travel together around the network. The way in which they are delivered, the general rule, is first-in first-out. This kind of design implies that there is not packet discrimination connected with the source, destination, content, type, carrier, etc. Every packet is treated equally. For example every packet suffers the same way and amount of latency, even regardless whether the packet is of a kind that is time-sensible or not (audio-video packets are treated like http packets, even though they are differently affected by delays in delivery). For this very reason it is argued that the internet, beside the fact that TCP/IP is open and publicly available, and it follows an end-to-end design, has grown so fast [14][15].

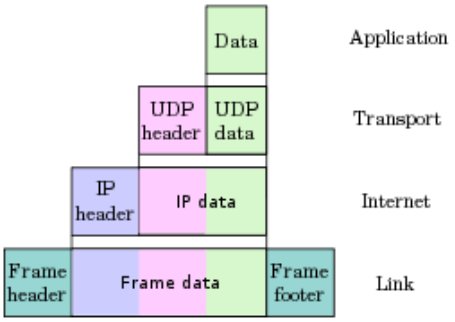

Figure 1: Encapsulation of Internet communications [11]

In such a scenario, no prioritisation of packets (*i.e.*, of type of communications) is envisioned. Some have argued that discrimination of packets might increase network efficiency. It is indeed true that, over an always more congested network, it might be efficient to prioritise those packets that are time sensitive. If a Web-page is visualised on the client browser top-down or bottom-up, it makes little difference for the end user. Contrast this with the increasing use of specific on-demand services. If the end user is visualizing a video or audio (or both) streaming, a delay of a few milliseconds might create a de-synchronization of the images and the audio. This would be noticed and not appreciated by the end user. In the case of a VoIP communication, it could render the communication useless. However, this type of packet discrimination, based on purely technical grounds, is not usually under debate. Also those who strongly advocate against packet discrimination, or in other words, Network Neutrality, do not argue on this aspect, and there are already implementations of communication techniques that try to limit packet latency of time sensitive data flow. The point of Network Neutrality has been already exposed elsewhere

 ISBN: 978-1-61208-122-9

[16].

Here we briefly recall the main features. In general, the usual arguments made at this regard may be summarised as follows:

A. 1) A usable and healthy Network:

To avoid a too high usage of the bandwidth by a few categories of users and to fix problems of slow and congested networks, bottle- necks, and similar problems (allegedly caused not by low investment in infrastructures, but by high usages of P2P networks). Many counter argue that the easy way to get this is to allocate a limited amount of bandwidth to any user and limit its usage to this given amount. The sum of the total amounts is what a given piece of network is able to carry. However, what usually happens in the wholesale (and partially also retail) market of cable companies and ISPs is quite similar to the behaviour known as overbooking by air companies: since statistically speaking is very unlikely that all the users use all their allocated bandwidth at the same time, it is possible to sell more bandwidth than that available, in a way that increases revenues with a very little probability of vexing users. Sometimes this same argument is sold as a benefit to users, arguing that they get more for their money.

B. 2) Price discrimination:

By dividing the market, ISPs can internalise the maximum consumer surplus. If an ISP can determine that some categories of users are interested only in basic services, say surfing and emails, while others need more variegate services, like connecting to Virtual Private Network (VPN) servers and Voice over Internet Protocol (VoIP), and the ISP is further able to accordingly shape/limit connections, then it will be able to sell the basic service to those customers who wouldnt pay a higher fee for extra services, while still charge a higher price to those who need the extra services. In this way, *i.e.*, through market segmentation, ISPs are able to charge the maximum price that each category is willing to pay for a given service and internalise a great share of consumer surplus, raising revenue but disadvantaging consumers. Such a situation is typical of those markets characterised by non perfect competition, *e.g.*, oligopolies.

C. 3) Vertical integration economies:

The same company may own the cable, sell the connectivity, and offer related services (*e.g.*, content purchase, emails, hosting, Television, VoiP, etc). The problem here is that of unfair competition, *i.e.*, if the company is a telephone company it is probably not happy with consumers using VoIP solutions, or at least not third party VoIP services that are sometimes a free of charge. If the ISP is a TV company, then you should rent its films, and not from another online store, or at least if one does it through her ISP store the download speed is faster. This kind of vertical integration represents a typical anticompetitive behaviour.

III. How information is inspected over the Internet

Deep Packet Inspection (DPI) is a set of methodologies used for analysis of data flows on the Internet. It is the intention of this research project to enter in the technical details of this issue [16]. However, it is clear that by using DPI technologies it is possible to know the content of TCP/IP communications. In contrast to other techniques, such as Stateful Packet Inspection where only the headers of the packets are inspected, through DPI the entire content of the packet is inspected and read. We have already indicated that data transferred over the Internet is ”chunked” into small pieces of data (called packets) and those packets are sent out individually over the network, so that they can reach the final destination in the most efficient way. Packets don’t get lost (usually) because the type of information necessary for their correct routing is present in their headers. So when a router receives a packet, the only think the router has to do is to look at the header and identify the information regarding the final definition and forward the packet to that place. When all the packets corresponding to a TCP/IP communication have reached the final destination (usually on a random order, depending of the different latencies, congestions and speeds of the different paths undertaken), the receiving device (application) rebuilds the communication following a specific packet order. Such information (the order in which packets should be ”re-assembled” for a correct representation of the carried information) is once again a type of information contained in the packet header [see Fig. 2]. This is of course an oversimplification of a TCP/IP data transfer. Much more information is contained in the headers, such as for example port numbers, etc. However, the exposed paradigm holds true.

bit offset	0-3	4-7	8-13	14-15	16-18	19-31
0	Version	Header Length	Differentiated Services Code Point	Explicit Congestion Notification	Total Length	
32	Identification				Flags	Fragment Offset
64	Time to Live		Protocol		Header Checksum	
96	Source IP Address					
128	Destination IP Address					
160	Options (if Header Length > 5)					
160 or 192+	Data					

Figure 2: IPv4 Packet header [12]

At this point, is apparent that for a correct routing of TCP/IP packets the content of such packets is completely helpless. What is necessary is the content of the headers. Once source, sequence, destination (and the rest of the identified informations) are read, the data flow can successfully happen. The content of the packet is not necessary for routing purposes.

However, the content of the packets may become interesting for other types of activities. Consider the following scenario: a subject (A) is interested in what another subject (B) is communicating to a third subject (C). If A has enough

 ISBN: 978-1-61208-122-9

access/control of the physical Network (say it gains control by breaking into the ISP or Cable Company mainframe, or technically speaking, is the ISP or Cable Company), one of the techniques A could easily use is Stateful Packet Inspection. If A can overlook what communications originate from B and what are received by C, A can easily identify communications from B directed to C. A can also infer additional information from the communication: depending on the time, length, port, it is possible to say, for example, that the communication was a SSH, a VPN, or a P2P. Such type of analysis can provide interesting information to subjects such A that are interested (legitimately or, more commonly, not) in what is sent over the Internet. Nevertheless, following this pattern, it is not possible to identify precisely the content of the information. Imagine the same scenario, but A now uses DPI tools. We said that DPI permits to read the information contained inside TCP/IP packets. Many times this type of intrusion into somebody else communications does not provide the intruder with a clear idea of the content, mainly for the already reported routing pattern of TCP/IP packets. Since they are sent following many different routes, it is not easy to collect enough packets as to rebuild the content of the information. However, if A has the type of control that we said it has in our scenario (A controls everything happens in its Network) then A can easily read the content of any communication that originates and ends inside its network. Not only from A to B or vice versa, but any communication that takes place within the limits of the Network under its control. In fact, if A can sniff all the packets, can read from the headers the source, destination, port, and sequence number, plus can read also the information carried in the body of the packet, A has a total control over the communication. Total control means not only read, but potentially also write privileges.

IV. Future work

Legislation in many jurisdictions regarding ISP liability, or more generally the liability of communication intermediaries, usually has a ”safe harbour’ provision’, which has its roots in the WIPO Copyright Treaty [17]. The agreed statement in article 8 reads: ”It is understood that the mere provision of physical facilities for enabling or making a communication does not in itself amount to communication within the meaning of this Treaty or the Berne Convention”. As usual in international agreements, the wording is vague and does not provide any hermeneutic tool or policy guidance for the development of national legislation. In future research we intend to address the relationship existing between the usage of packet inspection technologies, especially DPI, and the international and national legal and regulatory situation in terms of privacy protection, consumer protection, IP protection, and the exemptions that service and content providers enjoy.

Acknowledgment

The authors thank the Social Science and Humanities Research Council, IBM Center for Advanced Studies for their support, and colleagues for their useful comments and observations.

References

[1] See French Conseil Constitutionel decision n. 2009-580 of June 10th 2009, available in english http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bankmm/anglais/2009580dc.pdf.
All the online resources cited in this work have been last accessed during the month of November, 2010.

[2] See BBC world poll, available at http://news.bbc.co.uk/2/hi/8548190.stm

[3] See the United Nations Universal Declaration of Human Rights, adopted on 10 December 1948, in Paris, especially artt. 18, 19, 20, 26, and 27.

[4] See The Canadian Charter of Rights and Freedoms, in the Constitution Act 1982.

[5] Castells, M., The Rise of the Network Society, The Information Age: Economy, Society and Culture Vol. I. Cambridge,(1996, second edition, 2000) MA; Oxford, UK

[6] Ireland, P., Limited liability, shareholder rights and the problem of corporate irresponsibility, in Camb. J. Econ. (2010) 34 (5): 837-856.

[7] See http://en.wikipedia.org/wiki/HD_DVD

[8] See http://en.wikipedia.org/wiki/Betamax

[9] See the Moore’s Law http://en.wikipedia.org/wiki/MooreLaw

[10] See Lessig, L., Free Culture, New York, 2004, p. 3

[11] Source:http://en.wikipedia.org/wiki/File:UDPencapsulation.svg

[12] Source: http://en.wikipedia.org/wiki/IPv4header

[13] Loi favorisant la diffusion et la protection de la cration sur Internet : Loi n2009-669 du 12 juin 2009 parue au JO n135 du 13 juin 2009

[14] Saltzer, J., – Reed, D., – Clark, D.D., End-to-End Arguments in System Design. Second International Conference on Distributed Computing Systems, pages 509-512, April 1981. ACM Transactions on Computer Systems, 2(4), pages 277-288, 1984

[15] Lessig, L., – Lemley, M., The End of End-to-End: Preserving the Architecture of the Internet in the Broadband Era; UC Berkeley Law Econ Research Paper No. 2000-19; Stanford Law Economics Olin Working Paper No. 207; UC Berkeley Public Law Research Paper No. 37

[16] Perry, M., – Margoni, T., Interpreting ’Network Discrimination’ in the CRTC and FCC, in Digital Society 2010, 2010, 301.

[17] WIPO Copyright Treaty, 20/12/1996 , adopted in Geneva on December 20, 1996

 ISBN: 978-1-61208-122-9