Canadian Journal of Law and Technology

Volume 7
Number 1 *1 & 2*

Article 9

1-1-2010

Web 2.0 Regulation: A Risk Management Process

Pierre Trudel

Web 2.0 Regulation: A Risk Management Process*

Pierre Trudel**

INTRODUCTION

"Web 2.0" is sometimes used as a slogan or buzzword. It is fuzzy[1] and refers to a set of realities and situations that resist exhaustive definition.[2] Web 2.0 has some emblematic features, and includes a constellation of functions with shared characteristics, in particular, a high level of user involvement in content production. Web 2.0 is also associated with structured environments in which content is largely user-generated, such as collective publication sites like Wikipedia. Such sites allow cybernauts to edit and change content as they wish. In other cases, applications and content can be combined and websites can be synchronized with other websites.[3] Content-sharing sites, such as YouTube and Dailymotion, allow cybernauts to publish content online. Social networks, such as Facebook and MySpace, allow individuals to publish their personal profiles and information about other people.[4] Nicolas Vermeys notes that the Web 2.0 notion "designates the trend among some companies on the Web towards publishing user-generated content rather than employing the traditional business model of putting proprietary media content online."[5]

With the Internet, users have long been able to put content online but, on the legal level, what seems special about Web 2.0 is the user's role, which is more active than ever. The notion of Web 2.0 refers to a series of legal situations in

---

* Study conducted within the research program of the L.R. Wilson Chair in Information Technology and E-Commerce Law and as part of a research project sponsored by the Quebecor Foundation.

** Professor and holder of the L.R. Wilson Chair in Information Technology and E-Commerce Law, Centre de recherche en droit public, Faculty of Law, Université de Montréal, *pierre.trudel@umontreal.ca*.

1 Philippe Chantepie, "Éléments d'économie du Web 2.0: interfaces, bases de données, plates-formes" (2007) 24 Propriétés intellectuelles 285.

2 Dion Hinchcliffe, "Review of the Year's Best Web 2.0 Explanations", online: (2006) Web 2.0 Journal <http://web2.sys-con.com/node/165914/>.

3 Mary Madden & Susannah Fox, "Riding the Waves of 'Web 2.0'. More than a Buzzword, but Still Not Easily Defined", online: (2006) Pew Internet <http://www.pewinternet.org/Reports/2006/Riding-the-Waves-of-Web-20/Riding-the-Waves/Backgrounder.aspx?r=1>; Lisa Veasman, "'Piggy Backing' on the Web 2.0 Internet: Copyright Liability and Web 2.0 Mashups" (2008) 30 Comm/Ent 311–337.

4 Steven James, "Social Networking Sites: Regulating the Online 'Wild West' of Web 2.0" (2008) 2 Ent. L.R. 47–50.

5 Nicolas W. Vermeys, "Chronique-Responsabilité civile et Web 2.0" (July 2007) Repères, online: <http://rejb.editionsyvonblais.com/> [translated by author].

which roles seem less stable and have fuzzier boundaries. The realities associated with Web 2.0 are constantly changing and can be beyond the reach of state legislation. Given such an plethora of categories, we cannot restrict ourselves to a simple exegesis of promulgated state laws if we hope to describe the kind of regulation that could operate in environments associated with Web 2.0.

Some phenomena modulate the norms established by states and other Internet stakeholders, and prevent them from being enforced across the whole network. Despite the network's global nature, there are major differences in interpretations and values in the many cultural milieus in which rules apply.[6] Such phenomena prevent rules from being applied when they are out of context owing to the situation or cultural substrate. One such phenomenon seems to be legal risk.[7] Stakeholders' appraisals of the concrete possibility that national legislation and other rules will effectively apply to their activities are factors that explain why the Internet may be a global network but no one feels required to comply with all national laws that could theoretically apply.

In order to describe the law relating to Web 2.0, we have to look at the normativity that really operates there. Effective norms engender strong enough risks for stakeholders that they find it in their interest to comply. State legislation is not the only thing that governs Internet activities; the normativity that governs the resources associated with Web 2.0 flows from what the technology permits and prohibits, and also largely from stakeholder practices. Configurations and practices create risk or shift risk onto others. However, state regulators may consider that the risks arising out of Internet activities are worrisome enough that the state should impose obligations on stakeholders and thus modulate what they can do online. Through their regulations, states create risks for stakeholders.

When Web 2.0 is seen as a network, its regulation[8] can be described as active normativity resulting from risk management decisions made by regulators and stakeholders on the Net. On the Internet, governments, users, companies and other stakeholders manage risks. Through their decisions and behaviour, all normativity producers create risks flowing from the norms that apply to them, and relay those risks to co-contractors and partners. Norm producers cannot claim sovereignty in

---

6 Jack Goldsmith & Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (New York: Oxford University Press, 2006) at c. 9.

7 On legal risk analysis methodology, see: Kienle, H., *et al.*, "Managing Legal Risks Associated with Intellectual Property on the Web" (2008) 3 Int. J. Bus. Inf. Syst. 86–106, online: <http://www.inderscience.com/offer.php?id=16055>; Jan Trzaskowski, "Legal Risk Management in a Global Electronic Marketplace", (2006) 49 Scandinavian Studies in Law, 319–337; Franck Verdun, *La gestion des risques juridiques* (Paris: Éditions d'organisation, 2006) at 39ff.

8 Thomas Schultz, *Réguler le commerce électronique par la résolution des litiges en ligne* (Brussels: Brulant, 2005) at 162 — Schultz reports the points of views of the *Mission interministérielle français sur l'Internet* and the *Conseil supérieur de l'audiovisuel français*. He describes the findings of Marc Maesschalck & Tom Dedeurwaerdere, "Autorégulation, éthique procédurale et gouvernance de la société de l'information" in Jacques Berleur, Christophe Lazaro & Robert Queck, eds., *Gouvernance de la société de l'information* (Brussels: Bruylant-Presses Universitaires de Namur, 2002) at 77–103.

cyberspace, but they retain complete power to set rules that create risks for stakeholders.

I. RISKS AND STAKES FLOWING FROM FUNCTIONS ASSOCIATED WITH WEB 2.0

Even more than the first-generation Web, Web 2.0's prime feature is the omnipresence of the network. Resulting from constant interactions among stakeholders, Web 2.0 looks like a network made up of nodes that sometimes take the form of sites, sometimes users, and sometimes public and private regulators. Each node has the capacity to make rules and impose them on other interconnected stakeholders. The ability to impose rules on other bodies in the network follows from the amount of risk the node can generate for those with which it is inter-related.

Web 2.0 raises questions about the legal frameworks that apply to it because it involves risks and stakes that seem new. Since it removes boundaries and erases categories, the issues it raises are often perceived as a change in the scale of the risk that is inherent to online communication. Normativity creates, accentuates, reduces and transfers risk. Risks flowing from norms are in this respect legal risks.

(a) Risk on a Different Scale

Web 2.0 may not be entirely new, but it seems to shine a more dramatic light on the stakes and risks inherent to online environments. While the risks it involves are not necessarily novel, they seem to be greater. Franklin Brousse says that Web 2.0

> . . . repositions the cybernaut at the heart of the Web. It changes the legal risks and responsibilities most often related to website operation. By using the tools and technology of new Web 2.0 services to create, organize and freely share within a community all forms of content (text, audio and visual), every cybernaut becomes an author and/or editor of content, and must shoulder new responsibility related to both his or her new creations and the way they he or she uses the creations of others.[9]

The user's greater role shifts and increases the number of locations where risks and stakes arise, many of which have legal aspects. Owing to the active role they play, users become nodes of normativity that other stakeholders are required to take into account. Decisions made by Web 2.0 users are more likely than those of first-generation Internet users to have consequences for third parties. However, since the Web 2.0 environment does not have a central body that shoulders responsibility, the legal framework ends up being described as a set of risks distributed across an undetermined number of stakeholders of different sizes and statuses.

Risk is also on a different scale because of quantitative and qualitative changes in information publication. The Internet makes information circulation commonplace. Data can easily be published outside of legitimate circles, which

---

9 "Web 2.0: un point complet sur les aspects juridiques", online: (17 May 2005) Indexel.net <http://www.indexel.net/1_6_4523__3_/9/33/1/Web_2.0___un_point_complet_sur_les_aspects_juridiques.htm> [translated by author].

increases risk.[10] Web 2.0 environments change the spatial and temporal reference points that make it possible to identify legitimate and legal areas of information circulation. Web 2.0's many functions provide access to information that, until recently, was meant to circulate in restricted areas. Paradigms that were designed in a world where networks took up less space are inadequate in Web 2.0.[11]

The changes in the size of the stakes show how much evolution there has been in the level of risk caused by information circulation in the network. The new dimensions of risk are giving legislation new purposes. We may require regulatory tools that reflect the fact that relay processes and risk transfers occur in a network.

The Internet changes the spatial scale used to assess risk. Outside of the networked world, gaining access to information can require a major investment in resources. On the Internet, much information is just a search query away.[12] Such easy access makes information commonplace and increases the risk of things being taken out of context.

Time is also becoming less central: the persistence of information means that it can cross out of the time-spaces in which it can be held legitimately. For example, it can be legitimate for information to be available to the public owing to the topicality of an event. However, archiving and virtually permanent availability on the Internet gives it a persistence that extends beyond what is necessary to make sense of the news.

The ability to accumulate information makes it possible to create large deposits of information on people that could then be used by the police or wrongdoers. In sum, the fact that less effort is needed to find information erodes what used to be a kind of protection by default for many basic rights, such as the right to privacy and freedom from attacks on reputation.

(b) The Primary Categories of Stakes and Risks

Regulation of Web 2.0 is part of the fabric of the requirements related to modulating and managing risks. Those who take part in Web 2.0 activities do so more or less frequently depending on whether they are aware of how much risk they have to carry. Technological configurations, modes of operation, applicable norms and the topics involved in a Web 2.0 environment are all factors that can give rise to, increase or limit stakeholders' risk.

While it seems impossible to compile an abstract list of all the stakes and risks that can arise from operating a Web 2.0 site, we can identify the major categories of those that most stakeholders would want to consider in order to make decisions. Generically, Web 2.0 environments involve risks relating to behaviour, technological and ergonomic configuration, and regulation. Management of one kind of risk can create or accentuate the risks associated with the other categories.

---

10 Karl D. Belgum, "Who leads at Half-time?: Three Conflicting Visions of Internet Privacy Policy" (1999) 6 Rich. J.L. & Tech. 1.

11 Frederick Schauer, "Internet Privacy and the Public-Private Distinction" (1998) 38 Jurimetrics 555.

12 Daniel J. Solove, "Access and Aggregation: Public Records, Privacy and the Constitution" (2002) 86 Minn. L. Rev. 1137 at 1139.

(i) Risks Related to Behaviour

Behavioural risks flow from the conduct of the cybernauts who interact on the site. Practices that can infringe on the rights of other people are those that most often come to mind.

Risks to reputation — With Web 2.0, it is easy to speak about oneself and others, and to make such comments almost universally available. Mechanisms that protect the right to freedom from attacks on reputation take into account the context in which comments are published and assess their defamatory nature in relation to the meaning given to them in the circumstances of publication. Thus, a comment about an individual's professional actions may be licit within a restricted circle. However, the same comment may be defamatory if brought to the attention of a third party. Many Web 2.0 environments, such as social networking sites, provide unprecedented means of bringing comments about private life into the public sphere. Courts in Canada have considered the scope of dissemination of defamatory comments on the Internet in their assessment of damages.[13]

Risks to privacy — Many Web 2.0 applications have the potential to break the boundaries separating what is held as private or as shared within only a small circle, and information available to the broader public. For example, on a social networking site, one can publish information about oneself, but also about one's contacts. Such information can be disclosed through comments. Our contacts can also put information about us on their own personal sites.

Personal information revealed on a social networking site can be used in many ways. For example, companies can use information to test markets, sexual predators can find potential victims by searching for vulnerable profiles, and prospective employers can surf personal spaces to learn more about applicants before hiring.[14]

Accumulation and agglomeration of data on individuals by sites with user-generated content and use of other Internet functions means that large repositories of information can be available for surveillance activities of all kinds. This is a risk that seems inherent to the way the Internet operates today.

Risks to the right to be asked for consent to release an image — The stakes involved in publishing images obviously concern intellectual property rights, but they also bring into play an individual's right to oppose the publication of their image without their consent or in circumstances other than in the public interest or the interest of people close to the individual.

Risks to intellectual property — As applications that enable users to publish content on websites become more commonplace, intellectual property risks increase. Users can copy works without authorization and then publish them on a site without authorization. The legal principles that are brought into question by this kind of activity are not new, but the scope of the problem and the ease with which

---

13 *Southam v. Chelekis*, 2000 BCCA 112.

14 Susan B. Barnes, "A Privacy Paradox: Social Networking in the United States" (2006) 11 First Monday, online: <http://www.firstmonday.org/issues/issue11_9/barnes/index.html> (visited on 4 June 2007).

it is now possible to publish content raise major challenges. The risk of infringement of intellectual property rights seems greater.[15]

Risks of publication of illegal content — The more decision-making centres there are with respect to publication on the net, the greater the risk that illegal content will be published.

On sites with user-generated content, risk flows mainly from the behaviour of cybernauts. In such cases, there is a multitude of decision centres that are all able to publish information from their own perspectives. The amateur's increased role in situations that used to be dominated by professionals tends to blur the borders between producers and consumers, which makes determining status and responsibility all the more problematic.[16]

The infinite number of possible situations, the difficulty in identifying those in which laws are violated, and the fact that users are crucial factors makes the legal risk analysis a useful approach. In a world where the network seems omnipresent in human activity, it is less and less realistic to give a specific status to each user. User behaviour can depend on a wide range of highly volatile variables that can affect the legal status of what users do. Risk analysis makes it possible to re-establish a degree of legal and normative predictability.

(ii) Risks Related to Configuration

Web 2.0 environments involve some risks that do not flow exclusively from the intention or behaviour of the site administrator or users. The way that environments are configured can make it easier to perform actions that may be illegal. For example, the technical facility with which it is possible to put content on a blog or site where audio and video documents are shared is in itself a source of risk. Such default normativity facilitates actions that could easily contravene other rules, such as those pertaining to intellectual property.

The breadth the Internet and the power of information processing functions mean that the cyberspace environment involves increased risks that have to be managed within the network. For example, attention has often been drawn to the brawn of information aggregation tools and the astonishing abilities of search engines.[17] Information, even when it is public, can easily be found and then combined so as to deduce private information. Thus, risks to privacy are on a different scale on the Internet. This kind of phenomenon requires risk management that necessarily operates in a network.

The very configuration of the Internet, which ignores territorial borders, engenders risks. For example, many Web 2.0 functions make it possible to use information out of context. The design of personal networking sites is based on recognition that every individual has different spaces in which the status of information will not necessarily be the same. For example, it could be wrong to take a comment made in an intimate setting and publish it to a wider circle.

The Internet is not a univocal environment: it contains all sorts of places. Some are more risky than others for the privacy of the people who visit them. For

15 Veasman, *supra* note 3 at 311.

16 Pierre-Yves Gautier, "Le contenu généré par l'utilisateur" (2008) Légicom 1.

17 *Supra* note 12.

example, social networking sites are configured so that people can meet others. Sites such as MySpace and LinkedIn offer online services that bring people into contact. Such sites can be used to increase one's circle of friends, create work relationships, publicize musical groups, get people with the same interests together, find old classmates, etc. One need only choose a site that meets one's needs and register to be potentially linked with millions of people.

The registration form generally allows you to create a basic profile, which can contain your user name, hometown and job. The user can then complete the information pertaining to him or her by adding details, photographs, a CV and information on interests. The information will be contained in a personal space.

In order to contact others, users can add people to their address books by searching for individuals who are already members of the site and asking them if they want to become friends. Users can get in touch with people who are not site members by inviting them to register and make contact. Some sites make it possible to import lists of contacts from email addresses so that all the people on the lists can be sent invitation emails. If the people in question join the site, they will bring in their contacts in turn, and the network will thus grow.

Finally, content circulating in many Web 2.0 environments is extremely volatile. It can be changed by users and recombined in an infinite variety of ways. Users can edit and change content and, thus, it cannot be thought of as definitive in the way that professional publications used to be considered. Publishing now looks like a continuous process in which many players with different statuses can take part.

(iii) Risks and Stakes Related to Regulation

Regulation, whether it results from technological configuration, stakeholder activity or rules established by state authorities, generates risks. Rules are obviously meant to be followed, but in practice stakeholders will not comply with those that are not in their interest if they see that there is little danger that they will suffer adverse consequences if they fail to do so.

Risk is increased when roles and categories defined in the legislation of different countries are superimposed on one another. Jan Trzaskowski notes that "[i]n the absence of globally accepted standards for geographical delimitation of content on the Internet, the infringement of foreign law is a risk which businesses inevitably will run when carrying out electronic commerce."[18] In Web 2.0 environments, different stakeholders occupy different positions and play changing roles. The volatility can make it difficult to determine responsibility. It follows that it is difficult to identify who is liable for content and activities. The accountability deficit tends to increase relative uncertainty about the identity of those who will have to answer for harmful and illegal actions.

Network habits and practices also generate regulations that can create risks for users. Creating a site that permits any user to introduce comments or images about other people is certainly a form of regulation by default that creates risks for the third parties possibly concerned by the documents put online.

Users act in a network — they interact and at the same time develop solutions to problems they encounter. They find ways of minimizing the risk they face.

---

18 *Supra* note 7 at 320.

In many situations they adopt a set of rules that govern their activities. In short, norms themselves are partially produced in network interactions.[19] However, once they are established, they necessarily generate risks for others.

II. NETWORKED REGULATION

Once acknowledged, risk entails the duty to take precautions; it has to be managed. Legal risk flows from situations in which the rights of others could be infringed upon. While they are different, there are strong links between technological and legal risk. When technological risk is acknowledged, there is almost always a corresponding obligation to take it into account and behave accordingly. Legal risk can also flow from the possibility of non-compliance with a law or other form of obligation, such as a contract. Legal risks result from situations in which an individual can be held liable.

It is unusual to employ the notion of risk with respect to law. Legal theorists traditionally see risk in the phenomena that they are required to examine, but they do not generally consider that the risks include the fact that punishment could follow from transgressing a rule.[20] However, when a management approach is taken, legal risk is clearly a notion that needs to be considered. Managers see laws as carrying risks. Trzaskowski points out that "[l]egal risk management is not a well-established or well-defined concept, which, like risk management in general, is of a proactive nature."[21] Yet, it seems clear that the legal theorists who are asked to advise those who make decisions concerning the Internet take a legal risk management approach.[22]

In a network environment, legal risk has two components: one or more norms and an event. Legal risk flows from the conjunction of the norm and the event. The norm may be stated in legislation or regulations, but it may also follow from a contract or technical configuration. What is specific to a norm is that sanctions can follow from it, in other words, adverse consequences can result from transgressing it. Transgression is an event, and can take the form of a positive action or an omission in a concrete context. The event necessarily has to be anticipated or at least its possibility has to be identified. The damages following from the event have to be assessed.

In order to produce compliant behaviour, a norm or regulatory process has to be perceived as generating more risks than benefits if it is transgressed. On the

---

19 David D. Johnson, Susan P. Crawford & John G. Palfrey Jr., "The Accountable Internet: Peer Production of Internet Governance" (2004) 9 Va. J. L. & Tech. 1.

20 Franck Verdun, *La gestion des risques juridiques*, (Paris: Éditions d'organisation, 2006) at 20.

21 *Supra* note 18 at 321.

22 Rachel Burnt, "Legal risk management for the IT industry" (2005) 21 Computer Law & Security Report 61; David N.Weiskopf, "The Risks of Copyright Infringement on the Internet: A Practitioner's Guide" (1998) 33 U.S.F. L. Rev. 1; Keith J Epstein & Bill Tancer, "Enforcement of Use Limitations by Internet Services Providers: How to Stop that Hacker, Cracker, Spammer, Spoofer, Flamer, Bomber" (1997) 19 Comm/Ent 661; Karl Belgum & Hilary Rowen, "Insurance for Internet-Related Risks" (2000) Journal of Internet Law 11.

Internet, stakeholders assess legal risks. How else could we explain the fact that despite the network's universal nature and thus the certitude that websites with unrestricted access can be visited in all countries, no site administrator has decided to comply with all the applicable legislation of all countries? In fact, on the Internet, effective regulation is that which generates among stakeholders a minimum threshold of perception of the risks resulting from non-compliant behaviour.

A government or other regulator can take action to increase the risk associated with certain forms of behaviour and some activities, or reduce the risks linked with good conduct. For example, when a government adopts a strict law against some practices, it increases the risks associated with them. The government can also put boundaries around or limit risks to users engaging in legitimate activities. In such cases, the risks inherent to the activities in question are necessarily borne by others.

Regulation of Web 2.0 can be seen as a set of measures designed to reinforce one another so as to limit the risks facing cybernauts engaging in legal activities. The normativity is deployed in the network by imposing rules on stakeholders and inciting them to relay requirements to those over whom they have influence.

State actions will be more efficient with respect to risk if they are complemented by dynamic surveillance policies and court action because those are the conditions necessary for stakeholders to see that breaking the rules entails risks. The risks flowing from legislation then have to be relayed to all who engage in illegal activities.

In a network, anyone who can impose his or her will has the ability to increase risk for others. Thus, a state can impose responsibilities on people who are within its borders. Such people will then have to manage the risks flowing from those obligations. They will try to ensure that their partners comply with the requirements that they themselves have to meet and with respect to which they can be held accountable. The obligations and risks will be relayed by contract or in other ways.

Regulation of the Internet results from constant temporary balancing of risks and precautions. All stakeholders try to minimize the risk to which they are exposed when they are involved in situations over which they have some effective control. Regulation of Web 2.0 activities has to aim to increase the risks associated with behaviour that puts others in danger, and to reduce the risks to those with prudent conduct. Normativity usually comes into play when it is seen as appropriate to adjust the relative risks borne by participants in an activity.

(a) Nodes of Normativity

In a network, norms are developed and expressed in various places that can be considered nodes of normativity. Within its jurisdiction, state law is a major node of normativity: those in the territory have virtually no choice but to comply because the risks associated with non-compliance are generally high. However, people may be tempted to run the risk and find themselves in non-compliance if they think that the laws are enforced only rarely or that there is no clear will to apply them. Here we can see how cyberspace is an environment in which users have a great deal of control. If they think they can break the law with little risk of suffering consequences, it is more likely that they will take the chance and engage in a prohibited or harmful activity.

In networked worlds such as Web 2.0, there are many nodes of normativity and their ability to generate enough risk to make norms effective seems to be constantly fluctuating.

(i) State Legislation

Criminal and civil law are major guides for cybernaut practices. For most stakeholders in cyberspace, responsibility with respect to the laws of one or more countries can be seen as a set of risks to be managed. Individuals and companies have to ensure that their practices comply with the legislation that is likely to apply and entail liability. They seek to control the risk flowing from their activities by taking precautions against the adverse effects of enforcement of national legislation. When rules are set out in legislation, stakeholders tend to adjust their practices so as to limit the risk that they will break those rules.

Even though it may be insufficient in itself, legislation is highly symbolic. Most stakeholders see its very existence as a message. When legislation is enforced, stakeholders understand that it is better to adopt behaviour that is free of harmful practices.

In order to have optimal results, legislation has to target all situations that can be associated with Web 2.0 practices. Moreover, in a network, effective normativity is often that set by influential supranational legislation and the laws of powerful countries. Network interactions and consistency with outside law have to be taken into account when designing national legislation.

The legislation in question can cover many different forms of activity. Competition legislation, in particular provisions concerning fraudulent advertising and false claims, and consumer protection legislation can apply to several typical forms of Web 2.0 behaviour. Civil liability can arise out of many Web 2.0 activities. The idea that one may have to answer for one's actions in civil court can be a significant risk for many Web 2.0 stakeholders. Indeed, it is largely through rules that limit liability for some categories of stakeholders that legislators in many jurisdictions have altered the risks associated with publishing information on the Internet.

For example, in US law, section 230 of the *Communications Decency Act*[23] provides "Good Samaritans" with immunity[24] with respect to content-related actions and omissions. The *Communications Decency Act* protects interactive computer services from liability, even after they have been informed about publications that are claimed to be defamatory or threatening.[25] Only an interactive computer service provider or user can benefit from the immunization from liability afforded by the CDA.[26] CDA section 230(f)(2) defines the expression "interactive computer service provider" — it is any information service, system or provider of software that permits a number of users to access a computer server, specifically including services and systems that provide Internet access and such systems managed by libraries and educational institutions or the services that they offer.

---

23 *Communications Decency Act*, 47 U.S.C. §230 (1996).

24 *Communications Decency Act*, 47 U.S.C. §230(c) (1996) — "Protection for 'Good Samaritan' blocking and screening of offensive material."

25 *Zeran v. America Online Inc.*, 129 F. 3d 327 (4th Cir., 1997).

26 *Communications Decency Act*, 47 U.S.C. §230(c)(1) (1996).

The well-known user-generated content sites have been able to develop in the United States thanks to the immunity given to interactive service providers with respect to content provided by third parties. Each country has to decide on the level of risk that seems optimal in order to encourage the development of online services but at the same time protect other interests, such as reputation, privacy and intellectual property.

(ii) Technological Configurations

What seems characteristic of the cyberspace environment is that the normativity that is effective in it is that which is enforced immediately, such as that resulting from technological configurations, and that which leads stakeholders to see that there are risks. The Internet is an environment built by technology; the risks that it involves necessarily result from normative decisions such as those that provide the basis for technological configurations.[27] This is especially clear in Web 2.0 environments.

Grimmelman notes that software configurations are automatic, immediately enforced and have some flexibility in that software designers can set up any system that "they can imagine and describe precisely."[28] However, regulation through legislation is even more flexible, and does not share software's lack of transparency. Grimmelman writes:

> Frequently, those regulated by software may have no reasonable way to determine the overall shape of the line between prohibited and permitted behavior. The plasticity of software and its automated operation also bedevil attempts to have software explain itself. Even experts may not understand why a program acts as it does.[29]

In Web 2.0, the technical architecture determines the conditions for access and use of the resources made available to cybernauts. For example, the terms for using MySpace provide that "MySpace performs technical functions necessary to offer the MySpace Services, including but not limited to transcoding and/or reformatting Content to allow its use throughout the MySpace Services."[30]

In the end, the fact that Web 2.0 environments are fundamentally structured by technology leads us to re-evaluate the conception that we tend to have of Web 2.0 as a place where users are the masters and are free to insert whatever content they want. Indeed, users' great latitude is a result of technological choices and configuration, but would such technological choices would have been possible in a legal environment less favourable to online service operators than that prevailing in American law?

---

27 Joel R. Reidenberg, "Lex Informatica" (1998) 76 Tex. L. Rev. 553; Lawrence Lessig, *Code and Other Laws of Cyberespace* (Basic Books, 1999).

28 James Grimmelman, "Regulation by Software" (2005) 114 Yale L.J. 1719 at. 1723.

29 *Ibid.*

30 MySpace: "Terms of Use Agreement", 6.6ff., online: Terms & Conditions <http://www.myspace.com/index.cfm?fuseaction=misc.terms>.

(iii) Cybernaut Practices

Cybernaut practices also establish normative frameworks on the Internet. In the Web 2.0 world, where user involvement is greater, the importance of user practices is also greater.

Edward Lee says that the emergence of user-generated content brings back into question the traditional conceptions of law enforcement.[31] Using examples of cybernaut practices relating to copyrighted works, he argues that the formalist conception of law is off-target. Intellectual property legislation has grey areas and gaps that are only very occasionally filled by court decisions. User practices help to fill in the holes and eliminate ambiguities in legislation. When faced with practices that seem to be in violation of legislation, it is as if rights holders weighed the advantages and disadvantages of going to court. Users adopt practices that reflect what they see as reasonable risks, in particular, the risk of being sued.

There is general consensus on the need to ensure the existence and appropriate spread of what stakeholders identify as "good practices", in other words, exemplary practices that reduce risk on Web 2.0.[32]

Even though customs and practices in a field of activity are often taken into account and integrated into state law, use of that type of norm lies in its ability to organize the behaviour and transactions of members of a community autonomously. Compliance with customs and practices is, in such circumstances, the essential condition for a participant's membership in the community. It is in this way that "good practices" are a source of regulation that often complements the more formal requirements of state law. In particular, "good practices" are often solution-oriented so as to limit the risks that can result from some forms of behaviour.

(iv) Norms Set in International Forums

International forums are the most efficient places for developing meta-norms, in other words, those expressed in the form of principles to be relayed in national legislation and other places where normativity develops. Both conventional international authorities and non-governmental organizations are places where meta-norms are developed. They are places where people seek to identify common denominators.

It is often in international forums that universal lines are drawn between what is licit and illicit. In order to remain relevant given the speed of change in practices, such authorities increasingly have to operate in networks.

Moreover, given the need to take into account a very wide spectrum of contexts in which norms have to apply, international deliberations lead to the development of principles that are designed to be relayed at the normative levels of states and other influential bodies. National legislation tends to be applied in a subsidiary way. Abstract principles are developed in worldwide forums and then relayed in specific cultural contexts. This is why it is possible to consider that the effective-

---

31 Edward Lee, "Warming Up to User-Generated Content" (2008) U. Ill. L. Rev. 1459.

32 Adam Thierer, "The MySpace-AG Agreement: A Model Code of Conduct for Social Networking?", online: (2008) The Progress & Freedom Foundation 15 <http://www.pff.org/issues-pubs/pops/pop15.1myspaceagreement.pdf>.

ness of state law lies in its ability to efficiently relay basic values and principles that are held to be legitimate.

(b) Ensuring Relays

The processes by which effective application of rules is achieved[33] in a realm like the Internet are major components of networked normativity. The relays are the different means by which stakeholders receive and implement the norms they see as relevant and compulsory.

On the Internet, the rules that users and other stakeholders consider relevant or compulsory are those that entail risks. For example, a company that decides to operate on the Internet by setting up a site where transactions can occur will necessarily assess the laws and other norms that it has to follow in order to minimize its risks. The rules it will consider relevant are those that are likely to be applied to the activities that it carries out. Thus, a restaurant in Calgary that delivers pizzas to local homes may consider that it is justified to place little importance on the laws in effect in Nepal!

This is the phenomenon that explains why we do not feel we have to comply with the requirements of all the laws of all the countries on Earth when we conduct activities on the Internet. Indeed, we consider it necessary to comply only with the laws that are likely to be enforced with respect to our activity. In other words, we are careful to comply with legislation and other norms that can really be applied to us in a significant manner. It is generally by assessing the risks associated with non-compliance with the laws of countries with which we plan to have close ties that we identify which national laws we should comply with when engaging in Internet activities. For example, a company located in Québec and considering doing business in the United States and Europe will not feel obliged to comply with the laws of Nepal, even though its site could very well be viewed in Nepalese territory. However, it may find it necessary to ensure that it is in compliance with Québec, American and European law.

Internet stakeholders and users can often manage risk adequately by taking into account activities they really perform, anticipating conflicts and identifying, within the context, how the requirements flowing from law and norms will be relayed and applied in practical terms.

For example, site administrators have to adopt a policy to determine conduct with respect to different aspects of the way their online environments function. For that, they have to take into account what is considered illegal in the territories in which their infrastructures are located and the virtual places where the sites could engage in significant activity. To determine which measures should be taken, they will necessarily have to analyze the situations in which they could be held liable. With Web 2.0, this has to be taken even further because users have some capacity to generate risks for other users and for the body that has set up the site.

---

33 "Effectiveness" ["effectivité" in French] means the ability to produce a sufficient degree of compliance with rules in social practices. André-Jean Arnaud, ed., *Dictionnaire encyclopédique de théorie et de sociologie du droit*, 2nd Edition, (Paris: L.G.D.J., 1993) s.v. "effectivité."

Relays are a way of describing the dialogue among different stakeholders and nodes of normativity. Stakeholders necessarily have to take cognizance of, and ensure they are in compliance with the rules that create risks for them. For that, they have to relay the rules to their partners and fill in the gaps so as to ensure the rules are applied in a concrete, effective way.

(i) Regulation Occurring on Websites

Like many online environments, Web 2.0 sites regulate user content and behaviour. Every site has its own internal procedures, which may involve user participation or only action by the site administrator. The procedures make it possible to identify and deal with possible issues and risks arising from non-compliance with legislation and other norms. These mechanisms also relay many of the rules considered imperative by the players at various levels of Web 2.0 environments.

(A) Oversight by the Site Itself

Web 2.0 sites often have moderators who check user content before or after it is put online. An Internet site can employ moderators, or it can ask for volunteer moderators from the public, for example, as it done on the HOTorNOT site.[34]

Moderation can be done before or after material is put online. When it is done, *a priori*, generally all content is checked before it is published on the site.[35] Thus, people who visit sites that are moderated *a priori* have a lesser chance of being involuntarily exposed to inappropriate material, since all user contributions have to be judged as appropriate by the moderators before they can be found online. With *a posteriori* moderation, users can contribute freely to the site.[36] Moderators generally rely on user complaints to target the content to be monitored. They can also submit the site to random checks. In all of these situations, it can be noted that having a moderator can actually expose the site to liability under the common law, as the site could be considered to be a publisher of material[37].

(B) Oversight by the Site's Users

Some Web 2.0 sites have developed monitoring schemes in which users play major roles. This reflects the difficulty for a site with millions of pages to control all of its content. User monitoring makes it possible to benefit from the work of an unknown number of users who assess whether contributions are inappropriate.

---

34 See online: HotorNot <http://mod.hotornot.com/>.

35 The Amazon.fr site <http://www.amazon.fr/> is a good example of an Internet site where the content is subject to *a priori* moderation. No user comment is put online immediately. The site reserves the right to wait five to seven days before publication so as to check the comments first.

36 For example, the RateMyProfessors site <http://www.ratemyprofessors.com/> uses *a posteriori* moderation.

37 Michael Deturbide, "Liability of Internet Service Providers for Defamation in the US and Britain: Same Competing Interests, Different Responses", online: (2000) 3 J.I.L.T. <http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_3/deturbide/>.

User ratings make it possible to manage risks that could flow from operating a Web 2.0 site. Such monitoring is performed by visitors to the site, who rate the content on a scale that is generally from 0 to 5.[38] In principle, content that is in bad taste or of poor quality will be given a bad rating. However, site users do not all have the same taste. Some people may give a good rating to content that others find disgusting. They may also give a bad rating to something that other people would consider a masterpiece. This approach is based on the hypothesis that visitors will not be inclined to watch videos that do not have good ratings.

Identification of inappropriate content, in other words, flagging, is one of the most common methods used on Web 2.0 sites to encourage users to report material that could be offensive, insulting, threatening or otherwise illegal. This method consists in inserting with every user contribution a link that makes it possible to report the content if it is inappropriate.[39] When a person visits a Web 2.0 site and comes face to face with child pornography, for example, he or she need only click on the link, and a warning will be sent automatically to the site administrators, saying that inappropriate content was found at such and such a place. Some Internet sites invite all visitors, whether or not they are members, to report inappropriate content; other sites allow only their members to do so.[40]

In order to avoid increasing the damage caused by offensive content, some sites automatically hide the contribution that was reported until a decision has been made on whether or not to withdraw it.[41]

The reporting method allows the site to count on a large number of monitors. Indeed, it is hard to imagine that a limited number of moderators would be sufficient to monitor a complete Web 2.0 site with millions of user contributions. By counting on visitors to report offensive content, the site gains access to a larger pool of monitors. Naturally, for such monitoring to be effective, users have to take the time to report inappropriate content.

(C) Dispute Resolution Mechanisms

A number of Web 2.0 sites provide users with dedicated dispute resolution mechanisms. Dispute resolution can range from simple reporting of inappropriate content so that it can be assessed by a paid or volunteer moderator, to elaborate

---

38 The YouTube site <http://www.youtube.com/>, for example, allows visitors to give up to five stars to published content.

39 The YouTube site <http://www.youtube.com/> is a good example of a site that makes it easy for visitors to signal inappropriate content. Every video added to the site is accompanied by a link called "Flag as Inappropriate", which makes it simple to report an offensive video.

40 See e.g. YouTube, online: <http://www.youtube.com/>, where you have to be a member to report a video.

41 For example, when a complaint is made about a rating on the RateMyProfessors site (*http://www.ratemyprofessors.com/*), the rating in question is automatically masked and replaced by the note "(Rating under review)" until the comment is approved or not.

arbitration mechanisms. The merchant-rating part of eBay[42] and the English version of Wikipedia[43] have complete dispute resolution mechanisms.

Evaluation of reported content: Visitors to Web 2.0 pages are often asked to use mechanisms on the site to report content that they consider inappropriate, for example, by flagging it. Once the content is flagged, the grounds for the complaint have to be analyzed before the contribution is withdrawn from the site. This is generally the moderators' job. Moderators look at the reported content and then decide if there is reason to remove it.

The delay between complaint submission and withdrawal of illicit material varies from one site to the next.[44] Thus, many people could be exposed to the content during the decision process and suffer damages as a result. This is why some sites consider it prudent to temporarily withdraw contributions that receive complaints until a moderator has had time to examine them.[45]

The process is unilateral. It is difficult to know how moderators base their decisions because generally everything happens in house. Some sites, however, base their decisions on their terms of use.[46]

Negotiation: Some Web 2.0 sites ask parties involved in a dispute to negotiate among themselves to solve the problem. Negotiations may involve simple discussions among the parties so that they can find an equitable resolution without having recourse to a third party.[47] The solution will ideally incorporate the suggestions of all those involved. Negotiation is a consensual process, and the parties can engage in it or withdraw from it as they wish.

Ways of negotiating vary from one site to the next depending on the means of communication made available to users. For example, on Wikipedia, people who submit texts generally use the discussion page to talk about issues. When a dispute arises concerning a Wikipedia page, the procedure is simple.[48] It is designed to

---

42 eBay: "Resolving Feedback Dispute", online: <http://pages.ebay.com/help/feedback/feedback-disputes.html> (visited on October 30, 2007).

43 Wikipedia: "Dispute Resolution", online: Wikipedia <http://en.wikipedia.org/wiki/Wikipedia:Resolving_disputes> (visited on October 30, 2007).

44 We tested the rating withdrawal system on the RateMyProfessors site <http://www.ratemyprofessors.com> to see how long it might take between the submission of a complaint and the withdrawal of a rating. In the case of obvious violations of the site's rules of conduct, for which we tested by saying that a professor preferred a certain ethnic group, the delay was relatively short: five days. In contrast, it took around two weeks for a moderator to approve a comment that was more ambiguous and less obviously in violation of the rules of conduct.

45 This is the method used by the RateMyProfessors site, <http://www.ratemyprofessors.com>.

46 See e.g. RateMyProfessors, online: Rater Guidelines <http://www.ratemyprofessors.com/rater_guidelines.jsp>, which contains the site's guidelines for writing a rating.

47 Karim Benyekhlef & Fabien Gélinas, *Le règlement en ligne des conflits: Enjeux de la cyberjustice*, (Paris: Romillat, 2003) at 66.

48 *Supra* note 43.

prevent the dispute from escalating, such as through editing and re-editing of the article in question, or writing personal comments on it. The people involved instead have to go to the discussion page and try to find a consensus so that the article can subsequently be changed. Negotiation is essential because the parties cannot submit their dispute to mediation or arbitration unless they have shown that they first tried to iron out their differences.[49]

Disputes on eBay concerning ratings by co-contracting parties are also supposed to go through a negotiation process. Indeed, eBay takes a very hands-off approach to such disputes and, in the end, resolution depends on the good will of the parties involved. Dispute resolution tools are nonetheless made available to users; for example, through the mutual rating withdrawal, two parties can agree to have controversial ratings withdrawn so that they are no longer counted when final ratings are calculated.[50] However, the comments remain in the parties' files.

Mediation, unlike negotiation, involves the active presence of a third party. In mediation, the parties agree to submit the dispute to a mediator who will help them find a satisfactory solution.[51] Unlike that of an arbitrator, the mediator's decision is not binding; it is only a suggestion. The parties are not required to accept the solution, and they can end the mediation process at any time.

The Wikipedia site offers its users mediation services if the people involved in the dispute cannot come to a consensus in any other way. The party who wishes to get help from a mediator has to fill out a form, send it to the Mediation Committee and give the other parties to the dispute notice of his or her desire to take part in the process.[52] Mediation is a voluntary process, and the people who have received notice have seven days to agree to participate in it or else it will not take place.[53] If there is agreement to engage in the process, a mediator will intervene after a few weeks, and the parties will be able to defend their points of view.[54]

The eBay site sends its users to the SquareTrade site,[55] which gives users means to resolve disputes. If a problem arises between two co-contracting parties, either party can complete a complaint form on SquareTrade giving the reasons for their dissatisfaction. After the complaint is submitted, the opposing party will receive an email explaining that the first party has submitted a complaint, that SquareTrade is a service designed to help resolve disputes on eBay, and that the second party can also complete a form describing his or her version of the facts.[56]

---

49 *Ibid.*

50 eBay: "What is Mutual Feedback Withdrawal?", online: How Feedback Works <http://pages.ebay.com/help/feedback/questions/mutual-withdrawal.html>, (visited on October 30, 2007).

51 *Supra* note 47 at 67.

52 Wikipedia: "Mediation", online: Wikipedia <http://en.wikipedia.org/wiki/Wikipedia:Mediation>, (visited on October 30, 2007).

53 *Ibid.*

54 *Ibid.*

55 eBay: "SquareTrade Warranties", online: <http://www.squaretrade.com/>.

56 Ethan Katsh and Janet Rifkin, *Online Dispute Resolution: Resolving Conflicts in Cyberspace*, (San Francisco: Jossey-Bass, 2001) at 181

The next step involves negotiation, but if that does not work, SquareTrade makes mediators available to its members. For a fee, a mediator can help resolve the dispute.[57] When a mediator is assigned, he or she takes cognizance of the case and then suggests a solution. Both parties have to agree for the solution to be accepted. While SquareTrade's purpose is not limited to resolving disputes over ratings, it is one of the tools that can be used to come to an agreement on mutual withdrawal of ratings.

Arbitration is a process in which people involved in a dispute decide to entrust its resolution to an independent tribunal that will make a decision after the parties have each presented their cases. The decision will be binding and eliminate the possibility of recourse to the courts.[58]

For example, the Wikipedia site offers its users an arbitration procedure that includes an arbitration board that has discretion to decide to hear certain cases.[59] Cases that are heard by the arbitration board are in particular those that have been referred to it by the mediation committee and those that have already gone through all the other steps of the dispute resolution process, but remain unresolved.[60]

Arbitration begins when one of the parties completes a request for arbitration.[61] The party must specify the procedures that have already been followed to resolve the dispute, explain the dispute and send notice to the other parties that a request for arbitration has been submitted.[62] Next, if the case is accepted by the arbitration board, a web page will be set up where evidence can be published and the parties can try to persuade the arbitrators.[63] Once the evidence is established, the board will vote and the final decision will be that of the majority.[64] Measures have also been taken to prevent conflicts from dragging on — they range from a prohibition on editing a category of articles, to a complete ban from participating in the Wikipedia site.[65]

Internal regulation mechanisms set up by various sites open to user participation are clearly designed to manage the risks inherent to operating a site where most of the content is provided by users. These are certainly crucial locations where the normativity that is applied effectively on the Internet is developed and relayed, and this is especially true in Web 2.0 environments.

---

57 *Ibid.* at 183

58 *Supra* note 47 at 72.

59 Wikipedia: "Arbitration Policy", online: Wikipedia <http://en.wikipedia.org/wiki/Wikipedia:Arbitration_policy> (visited on October 31, 2007).

60 *Ibid.*

61 Wikipedia: "Requests for Arbitration/Request Template", online: Wikipedia <http://en.wikipedia.org/wiki/Wikipedia:Requests_for_arbitration/Request_template> (visited on October 31, 2007).

62 *Ibid.*

63 *Ibid.*

64 *Ibid.*

65 *Ibid.*

(ii) Liability Mechanisms

Most stakeholders see liability with respect to state legislation as a set of risks to be managed. Individuals and enterprises have to ensure that their practices comply with the requirements of the legislation that could apply and could entail liability. In the case of sites with user-generated content, the actors truly at the origin of punishable publications cannot always be identified and may be beyond reach. A victim may be in a situation in which an intermediary seems to be the only one able to take responsibility for the publication of wrongful material that causes harm. Those who provide environments to users are often easy to identify and more financially solvent that the individual at the origin of the wrongful publication. This is why it is important to determine the extent of intermediaries' liability in the chain of information transmission on the Internet.[66]

When harm is caused, sanctions and compensation are sought. State normativity is often called in to help. Liability seems to be one of the primary loci where we identify and define the contradictory values hidden in rights and freedoms. By specifying what constitutes wrongful behaviour, liability regimes help to establish the different levels and forms of precedence among basic rights. For example, a strict liability regime can lead stakeholders to adopt measures and precautions. In contrast, a regime in which there is great immunity for some actors can make it possible to develop activities that would otherwise seem very risky. It is unlikely that sites with user-generated content, such as Facebook, YouTube and rating sites (e.g., RateMyProfessor) would have been put online in a legal environment that did not provide the immunity in 230(a)(1)2 of the *Computer Decency Act*.[67]

(iii) Contracts

Contracts are both nodes and relays of normativity. Internet stakeholders use contracts to try to transfer some risks to co-contracting parties. Through this, they relay many requirements of the national legislation of the countries where the sites are located. With Web 2.0, contracts entered into online are increasingly in an open transaction environment where credibility and trust tend to play central regulatory roles.[68]

Contracting practices make major contributions to identification and development of the habits of Internet operators. In an environment where contracting practices are so important, the development of guides and model contracts is also a

---

66 Pierre Trudel, *Internet Liability in Quebec Civil Law*, Report prepared for the National Judicial Institute's 2008 Civil Law Seminar held in Ottawa on June 13, 2008; Fabrice De Patoul, "La responsabilité des intermédiaires sur internet: les plate-formes de mise en relation, les forums et les blogs" (2007) 27 R.D.T.I 85.

67 *Computer Decency Act*, 47 U.S.C. s 230(a)(1); Melissa A. Troiano, "The New Journalism? Why Traditional Defamation Laws Should Apply to Internet Blogs" (2006) 55 Am. U.L.Rev. 1448; Robert G. Magee & Tae Hee Lee, "Information Conduits or Content Developers? Determining Whether News Portals Should Enjoy Blanket Immunity from Defamation Suits" (2007) 12 Comm L. & Pol'y 369.

68 Shmuel I. Becher & Tal Z. Zarsky, "E-Contract Doctrine 2.0: Standard Form Contracting in the Age of Online User Participation", (2008) 14 Michigan Telecommunications and Technology L. Rev. 303–366.

relay through which principles stated in legislation and texts from influential authorities are made concrete. A policy of cooperation with influential private stakeholders is a means of accentuating the effectiveness of state action. In order to optimize private and other sector initiatives, experiments and good practices established in the private sector have to be promoted and encouraged. Private sector initiatives come into play not only at the level of repression, but also at the preventive level. Contracting practices play a significant role.[69]

A strong policy in favour of cooperation with respect to model contracts can be an effective relay that raises awareness of risks among those most able to manage them. Contracts are the preferred tool for relaying legal obligations to the parties who are in a position to take action.[70] They are also a means of transferring risks. For example, an insurance contract is a mechanism for transferring some risks, and it is one of the contract-based forms of regulation that can be used to manage risks.[71]

Finally, developing contracting practices helps to relay the normative principles expressed in state legislation. Such relaying is often part of a co-regulation process.

(iv) Co-regulation Processes

The set of risks associated with Web 2.0 can be discussed, and solutions can be found in a circle of public, private and community stakeholders. The circle may be more or less wide, depending on the case. This explains the usefulness of co-regulation. Self-regulation and co-regulation[72] are crucial relays for norms governing Internet activities. Through these processes, legislation relevant to the various activities taking place on the Internet is updated, adapted and applied to specific cases.

Such processes can be seen as ongoing cycles in which requirements flowing from other normativities, such as state legislation, are systematically discussed, evaluated and adjusted in an evolving way. For example, in October 2007, a group of major companies, which are active on the Internet and have major copyright interests, promoted principles concerning the publication of user-generated content. The *Principles for User Generated Content Services* establish a set of goals shared by the promoters:

> In coming together around these Principles, Copyright Owners and UGC Services recognize that they share several important objectives: (1) the elim-

---

69 *1267623 Ontario Inc. v. Nexx Online Inc.* (1999), 46 B.L.R. (2d) 317 (Ont. S.C.J.); see Marie-Hélène Deschamps-Marquis, "Courriels indésirables, s'abstenir!", online: (Octobre 1999) Juriscom.net <http://www.juriscom.net/int/dpt/dpt20.htm#note1>.

70 Vincent Gautrais, *L'encadrement juridique du contrat électronique international* (Brussels: Éditions Bruylant, 1998).

71 Richard V. Ericson, Aaron Doyle & Dean Barry, *Insurance as Governance* (Toronto: University of Toronto Press, 2003) at 8.

72 Jacques Berleur & Yves Poullet, "Quelles régulations pour l'Internet?" in Jacques Berleur, Christophe Lazaro & Robert Queck, eds., *Gouvernance de la société de l'information* (Brussels-Namur: Bruylant, Presses universitaires de Namur, 2002) 133–151.

> ination of infringing content on UGC Services, (2) the encouragement of uploads of wholly original and authorized user-generated audio and video content, (3) the accommodation of fair use of copyrighted content on UGC Services, and (4) the protection of legitimate interests of user privacy. We believe that adhering to these Principles will help UGC Services and Copyright Owners achieve those objectives.[73]

The declaration then states fifteen principles concerning copyright protection and also commitments concerning use of identification technology to accommodate equitable use and cooperate with other stakeholders. While it is not a contract entailing obligations for the signatories, the declaration seems emblematic of the way legislation is applied in environments such as that of Web 2.0. The principles are based on existing state legislation, and show how the law will be complied with and applied. They also specify the circumstances in which civil action can be taken.[74] Here, we can see clearly how norms are relayed in this kind of co-regulation approach.

(v) Raising User Awareness

When a risk-management approach is taken, awareness-raising and education gain considerable importance. Every user has to be able to recognize and manage the risk at his or her level. The greater the user involvement, the more important it is to ensure that the user is adequately equipped to identify and manage the risks that have to be dealt with at his or her level. In an open environment such as the Internet, it is impossible to postulate that a body could take the user's place and identify and manage risks for him or her. This is the reason for measures designed to make users aware of risks. For example, the safety section of the terms of use of MySpace.com contains the following warnings to users:[75]

> MySpace makes it easy to express yourself, connect with friends and make new ones, but who you let into your space, how you interact with them, and how you present yourself online are important things to think about when using social networking sites. Here are some common sense guidelines that you should follow when using MySpace:
>
> - *Don't forget that your profile and MySpace forums are public spaces*. Don't post anything you wouldn't want the world to know (e.g., your phone number, address, IM screen names, or specific whereabouts). Avoid posting anything that would make it easy for a stranger to find you, such as where you hang out every day or a picture of you in front of your office or school.

---

73 *Principles for User Generated Content Services*, online: User Generated Content Principles <http://www.ugcprinciples.com/>; *Principles for User Generated Content Services*, Media Release, "Internet and Media Industry Leaders Unveil Principles to Foster Online Innovation While Protecting Copyrights", online: <http://www.ugcprinciples.com/press_release.html>.

74 "The Principles for User Generated Content Services: A Middle-Ground Approach to Cyber-governance" (2008) 121 Harv. L. Rev. 1387 at 1388.

75 See online: <http://www.myspace.com/index.cfm?fuseaction=cms.viewpage&placement=safetytips>.

- *People aren't always who they say they are*. Be careful about adding strangers to your friends list. It's fun to connect with new MySpace friends from all over the world, but avoid meeting people in person whom you do not fully know. If you must meet someone, do it in a public place and bring a friend or trusted adult.
- *Harassment, hate speech and inappropriate content should be reported*. If you feel someone's behavior is inappropriate, react. Report it to MySpace or the authorities.
- *Don't post anything that would embarrass you later*. It's easy to think that only our friends are looking at our MySpace page, but the truth is that everyone can see it. Think twice before posting a photo or information you wouldn't want your parents, potential employers, colleges or boss to see!
- *Don't say you're over 18 if you're not. Don't say you're younger than 18 if you're not*. If MySpace customer service determines you are under 13 and pretend to be older, we will delete your profile. If customer service determines you are over 18 and pretend to be a teenager to contact underage users, we will delete your profile.

Information on the risks and stakes facing users also has to be updated regularly. The essentially evolving nature of the environment makes it impossible to claim that the dangers are known and mastered once and for all. New trends and "tricks" have to be identified and their risks assessed. The best strategies for dealing with them have to be discussed and conveyed to the various categories of users.

CONCLUSION

Regulation of Web 2.0 can be seen from a risk management point of view. On the Internet, users are more active than ever. They manage risks by accepting and transferring them, and they can increase or minimize them. The effective scope and content of regulations controlling activities associated with Web 2.0 result from risk management decisions by all stakeholders. The main risks on Web 2.0 flow from the configuration of virtual spaces where people can interact. Such environments are constructed using technology, and what people can and cannot do on them is largely related to configuration. The behaviour of users and companies that are active on the Net also generates risks. Regulation itself, whether it results from legislation or other sources of normativity is, in practice, perceived as a risk to be managed.

Governments can set up measures that increase or decrease cybernauts' risk with respect to legislation. Once again, for Web 2.0 stakeholders, state legislation is a risk to be managed. State law and other normativities, such as norms flowing from technology, create more or less risk to privacy and other stakeholder interests on the net.

Seen as a set of risks to be managed, regulation of Web 2.0 looks like a network of norms that are developed and established in the many nodes of an environment that is itself networked. Norms are necessarily relayed through many processes. The incentive to relay the requirements of a rule so that another person is obliged to comply is a function of the rule's ability to generate a risk that will be

perceived as significant by those concerned. Seeing regulations in this way enables us to explain the regulatory dynamics that have to be set up by stakeholders when they are aware that they are running risks.

Technology-based normativity can create risks or provide solutions that limit the impact of risks. Government regulatory work could include updating the risks associated with some practices and activities in Web 2.0 environments. The state and other regulators can increase or decrease risk, for example, the risk flowing from social networking sites. Risk management decisions are taken by various individuals and bodies. Those that can impose their decisions create norms that are relayed to other stakeholders. Governments can impose requirements that limit risks to individuals and other bodies in their jurisdiction. On the Internet, such measures are generally perceived by stakeholders as risks to be managed and transferred to co-contracting parties. The effectiveness of regulation is a function of the real ability to increase risks to those who engage in potentially harmful activities and decrease risks to legitimate users.