# CONTESTED RIGHTS IN CYBERSPACE

by

LONGMEI SONG

Bachelor of Law, Beijing University, 1997
Juris Doctor, Washington University in St. Louis, 2003

A THESIS SUBMITTED IN FULFILMENT OF
THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF LAWS

in

THE FACULTY OF GRADUATE STUDIES

Faculty of Law

We accept this thesis as conforming
to the required standard

THE UNIVERSITY OF BRITISH COLUMBIA

September 2004

# Library Authorization

In presenting this thesis in partial fulfillment of the requirements for an advanced degree at the University of British Columbia, I agree that the Library shall make it freely available for reference and study. I further agree that permission for extensive copying of this thesis for scholarly purposes may be granted by the head of my department or by his or her representatives. It is understood that copying or publication of this thesis for financial gain shall not be allowed without my written permission.

LONGMEI SONG
Name of Author *(please print)*

31/08/2004
Date (dd/mm/yyyy)

Title of Thesis: CONTESTED RIGHTS IN CYBERSPACE

Degree: MASTER OF LAWS Year: 2004

Department of LAW
The University of British Columbia
Vancouver, BC Canada

# ABSTRACT

Ongoing development in the Internet technology and usage has brought controversies over the definition and scope of different private rights in connection with the use of the Internet. While relevant legal reforms and academic commentaries have mainly focused on institutional reform or micro-behavioral regulation, this thesis attempts to examine information rights in a bigger picture, by questioning the rationales and values that underpin current major regulatory regimes. Privacy right and copyright, two relatively well defined fields in most liberal democratic nations, now are subject to diverse contests as a result both of the traditional dichotomy of the public and the private power in neo-liberal regimes and of the control battle in which technology colludes with law to change the established equilibrium in the real world as well as in the cyberspace. Despite the varying regulatory preferences between the United States ("bottom up") and the European Union ("top down"), the prevalence rhetoric of private ordering – that cyberspace should avoid coercive rules laid by sovereign governments and welcome a laissez-faire network of contracts and customary norms – covers the factual assumptions of these norms.

The central question dealt by the thesis is: how much control should we allow over information, and by whom should this control be exercised? The thesis examines the major decision-makers and stakeholders in the information market; it also analyzes the dynamic process that enforces and legitimizes such decisions. The thesis takes side with technorealism that advocates rights consciousness, as most information-related rights are now being regulated in a more surreptitious way than before. If we are to have alternatives to the digital libertarianism, we will have to contribute our own input to the process of shaping and re-defining rights in cyberspace as well as in the real world. On the other hand, it calls for a right level of abstraction. We need to reconceptualize information privacy and copyright in cyberspace because doing so brings better understanding of the power structure of current Internet regulation, which in turn directs popular attention to focus on the ends rather than the means of regulation.

TABLE OF CONTENTS

## ACKNOWLEDGMENTS

I would like to thank my advisor Professor Pitman Potter for his valuable advice on my thesis writing and for his support and patience over my LL.M. years. I also like to thank Professor Philip Bryden for providing many useful advices and Professor Joseph Weiler for reviewing my thesis.

I am thankful for Green College's warm atmosphere and rich multidisciplinary environment, from which I benefit greatly. I also like to acknowledge the Webster Foundation for their generous fellowship to support my graduate study.

Finally, I would like to express my deepest gratitude to my family for their love and constant support.

# CHAPTER I CYBERSPACE SOCIALITY: EVOLUTION, CONTEXT, AND VISIONS

## 1.1 HISTORICAL REVIEW

The Internet evolved from the ARPAnet, established by the U.S. Department of Defense in 1968, as a device for load sharing among the large computers serving research facilities around the country. The architects of the ARPANet envisioned a "decentralized, self-maintaining series of redundant links between computers and computer networks . . . designed to allow vital research and communications to continue even if portions of the network were damaged, say, in a war."[1] Its design specifications called for providing secure communications in the advent of an outbreak of war, so that no centralized node would be vulnerable to destroying the entire network. As a result, the structure of the Internet has become a decentralized conglomeration of many different networks around the world. Unlike the telephone system, it allows any single user to broadcast a message simultaneously to numerous sites on the network. This possibility reflects the Internet's scientific purpose: to enable small elite of researchers to share critical information among themselves.

Although the Internet grew with such a short and idiosyncratic history, it quickly evolved beyond its original province of scientific study for the general public. Aware of the growing commercial interests in the Net[2], the National Science Foundation began slowly to privatize the Internet by the late 1980s, and consequently the Net has metamorphosed from a research tool into a forum for popular culture in the past decade. The global computer network which encompasses the Internet and the World Wide Web together

[1] ACLU, 929 F. Supp. at 831.

[2] The Internet, the Net, and Cyberspace are used interchangeably in this thesis.

with a whole host of other fora for electronic communication such as bulletin boards, chat rooms etc. now has millions of regular users and that number is rising as the technology becomes ever more accessible. As the number of users has increased, so the purposes for which they turn to this system have diversified. It is now common to use the Internet as a library or information source, for one to one communication and more open discussion, as a marketplace for buying and selling goods and services, and as a means of facilitating other experiences via participation in new "worlds" which have their existence only in the medium of Cyberspace. Private firms and networks – complete with rules, norms, standards, and expectations – are rapidly expanding their way. As a result, the Internet's relatively new business district – the ".com domain" – quickly swelled to become the largest sector on the Net, and By May 1996, 89% of the domain names on the Internet were commercial.[3] The Internet, now expanding at 20% per month according to some estimates, is "the place to be." One study projects a worldwide Internet usership of 250 to 300 million people by the end of the year 2000.[4]

History contains many examples of new technological developments causing problems for the application and enforcement of the law and other regulatory mechanisms and this has been particularly apparent in relation to computer technology. Saxby has commented that "The law is at a stage when it is trying to bed down a technology that has re-shaped society to its roots." Just how radical is this re-shaping?

## 1.2 CYBERSPACE AND PHYSICAL REALITY – CONTEXTUAL STUDY

What are the particular properties of Cyberspace, then, that deserve our attention in terms of social relations and legal intervention? This requires an examination of the cultural context of Cyberspace as contrast against physical world.

---

[3] TIG Internet Domain-Name Data Base, available at http://home.tig.com/cgi-bin/genobobject/domaindb (visited Dec. 12, 1999).

[4] See, Donald J. Karl, State Regulation of Anonymous Internet Use After ACLU of Georgia v. Miller, 30 Arizona State Law Journal, 513, 514 (1998).

"Cyberspace" is a word invented by a science fiction author, William Gibson, in his landmark work of the early 1980s, "Neuromancer". The term is used to refer to communications via computer networks. These methods of accessing the Internet are constantly evolving and difficult to categorize precisely. But, as presently constituted, those most relevant to this case are electronic mail, automatic mailing list services, "newsgroups", "chat rooms", and the "World Wide Web". All of these methods can be used to transmit text; most can transmit sound, pictures, and moving video images. Taken together, these tools constitute a unique medium – known to its users as "Cyberspace" – located in no particular geographical location but available to anyone, anywhere in the world, with access to the Internet. The term's immediate and widespread adoption arose precisely because it captured the essence of "virtual life" out there on the Net – it spoke to the people who practised that once-arcane art.[5]

Any space is not simply a physical location but a cultural environment with embedded norms and values.[6] New technologies are not simply tools or functional artifacts but are the components of a new cultural space. New technologies change our relationship with information, as well as our capabilities for working with information.[7] In his book *Law in a Digital World*, Katsh considered what Kuhn (1970) described some twenty-five years earlier as a "paradigm shift."[8] To Katsh, the technological changes are not effecting so much a *replacement* but rather a *displacement* of the existing state of affairs, i.e. "of changing patterns and operations. It is not all-electronic lawyers or electronic judges that we can expect but lawyers, judges and citizens who interact with machines in new ways

---

[5] See, Scott E. Bain, Examining Traditional Legal Paradigms in a Non-Physical Environment: Need We Invent New Rules of the Road for the Information Superhighway? 12 Berkeley Technology Law Journal, 1997.

[6] Edward Twitchell Hall, *Beyond Culture* (Garden City, New York: Anchor Press, 1976), p56.

[7] M. Ethan Katsh, Rights, Camera, Action: Cyberspatial Settings and the First Amendment, 104 Yale Law Journal, 1995.

[8] Kuhn wrote "a new theory, however special its range of application, is seldom or never just an increment to what is already known. Its assimilation requires the reconstruction of prior fact, an intrinsically revolutionary process that is seldom completed by a single man and never overnight." Kuhn, Thomas S. *The structure of scientific revolutions* (2d ed., Chicago: University of Chicago Press, 1970).

and, therefore, cause the process of law to become something different from what it has been."[9]

The broadening of the kinds of "places" that exist in Cyberspace is significant because context is important in both conflict generation and conflict resolution. As Leda Cooks has written, "[p]eople experience conflict culturally and relationally, as well as individually."[10] Robert C. Bordone notices that there are three fundamental changes in Cyberspace: (1) Communication transcends time and space on the Net; (2) A "virtual community" is professing their own culture; (3) Jurisdictional boundaries of the physical world are compromised in the "seamless" information flow in Cyberspace.[11]

Time collapses in Cyberspace. Information travels rapidly on the Web in comparison to the non-virtual world, and, more than telephonic communication, Cyberspace's ability to allow large numbers of people around the world to have real time conversations on the Internet multiplies the consequences of a harmful or unintended communication of attribution, of copyrighted material, or of secret information.

The Internet also collapses physical space in many ways, which has potential for increasing communication and understanding among peoples. The implications of Cyberspace's annihilation of distance and space on communication in relationships are also entrenched. Experience demonstrates that it is easier to communicate a difficult or unpleasant message via email than in person or on the telephone. The physical "distance" makes such communications feel safer for the messenger. The impact on the receiver, however, is not likely to be any better because the messenger felt more comfortable in

---

[9] Katsh, *Law in a Digital World*, Oxford University Press, 1995, p.15. See also, Andrew Terrett, Review of M. Ethan Katsh *Law in a Digital World* (Oxford University Press,1995), 1996 (1) *Journal of Information Law and Technology*, available at http://elj.warwick.ac.uk/elj/jilt/bookrev/1terrett/ (visited on Nov.23, 1999)

[10] Leda M. Cooks, Putting Mediation in Context, 11 Negotiation Journal, 1995.

[11] See generally, Robert C. Bordone, Electronic Online Dispute Resolution: A Systems Approach – potential, problems, and a Proposal, 3 Harvard Negotiation Law Review, 1998.

delivering it. In fact, the ultimate effect of using a computer-mediated communication to deliver "difficult" or "unpleasant" news or feelings can actually lead to more conflict between the involved parties in the long run. In the non-virtual world, persons communicate using much more than mere words. Tone, affect, space, and time all add to the richness of an interpersonal communication and help us to calibrate our responses appropriately to that of our counterpart. The challenges of Cyberspace in addressing these issues are unique.

Cyberspace has further evolved into a burgeoning "virtual community" that is separate from the "real" community in which these people live.[12] Unlike real space communities, Cyberspace communities are organized around unidimensional areas of interest. For many, Cyberspace is much more than computerized Yellow Pages or a place to get a 24-hour weather update. Instead, it has taken on many of the characteristics of community, replete with community-specific customs, needs, and desires. Customs, norms, and rules that differ from those we experience in the "real" world have developed within these virtual communities.[13] Because we are not physically proximate, our level of commitment to the moral community is likely to be low. Hardy also writes that "Customs are developing in Cyberspace as they might in any community, and rapid growth in computer communications suggests that there may be a great many such customs before long. Many of these customs conflict with "real" space customs....".[14] To identify a group as a community has its legal significance, because in general communities generate and perpetuate legal norms. The degree of sovereignty and autonomy granted to various

---

[12] Howard Rheingold writes: "People in virtual communities use words on screens to exchange pleasantries and argue, engage in intellectual discourse, conduct commerce, exchange knowledge, share emotional support, make plans, brainstorm, gossip, feud, fall in love, find friends and lose them, play games, flirt, create a little high art and a lot of idle talk. People in virtual communities do just about everything people do in real life, but we leave our bodies behind." Howard Rheingold, *The Virtual Community: Homesteading on the Electronic Frontier* 3 (1994).

[13] Bordone, supra note 11.

[14] I. Trotter Hardy, The Proper Legal Regime for "Cyberspace", 55 University of Pittsburgh Law Review, 1994.

online groups constitutes the final legal dimension vital to the shape of present and potential online communities.[15]

The most prominent and practical difference between Cyberspace and real space seems to be the borderless feature of the Internet.[16] Issues of personal jurisdiction and choice of law in the real world depend on where the action takes place. But there are no geographic boundaries in Cyberspace. Communication in Cyberspace transcends national borders and undermines the relationship between geographical location and the power of local government's efforts to regulate online behavior. Attempts by territorial jurisdictions to regulate the Internet have met with limited success largely because it is impossible for them to control the information which comes across Cyberspace from other territorial states or nations. Any dispute design system for Cyberspace must consider the implications that this borderless feature of the Internet will have on regulation, governance, and enforceability.[17]

In summary, the new context in Cyberspace will demand different appreciation of behavior patterns and norms in the "virtual reality" than what was expected in the pre-Internet age. Already we can witness a clash between the emergent culture and the entrenched culture. The level of conflict in Cyberspace will continue to increase, not only because there are more people interacting in traditional ways, but also because the kinds of interactions taking place in Cyberspace are broadening and changing in character. Will Cyberspace actually become important enough to lead to a substantial shift in sociological thought? Lyon thinks so. He tells us that "Cyberspace challenges

---

[15] Developments in the Law – The Law of Cyberspace, Part II. Communities Virtual and Real: Social and Political Dynamics of Law in Cyberspace, 112 *Harvard Law Review*, 1999.

[16] See, e.g., David R. Johnson & David Post, Law and Borders - The Rise of Law in Cyberspace, 48 *Stanford Law Review* 1367 (1996). (arguing that "[t]here has until now been a general correspondence between borders drawn in physical space 'between nation states and political entities' and borders in 'law space'.").

[17] Bordone, supra note 11.

time-honored notions of social reality"[18]. However, what impact Cyberspace will have on society remains a controversy among social scientists and common observers, which in turn affects legal policies toward this "new realm".

## 1.3 THE PRIVATE POWER IN CYBERSPACE

Another factor worth of attention in Cyberspace is the role of private power, as power is always closely correlated with the practice, or even, the formation, of right. There is no doubt that the Internet is a space of distributed power that limits the possibilities of authoritarian and monopoly control. But it has also become clear over the last few years that the Internet is no longer what it was in the 1970s or 1980s; it has become a contested space with considerable possibilities for segmentation and privatization.[19]

We cannot underestimate the extent that businesses are searching for ways to control, privatize, commercialize the Internet. In the U.S., AT&T already has the nation-wide infrastructure and a billing system in place to provide and charge for services. Major global alliances have been formed that aim at delivering a whole range of services to clients. Growth strategies and global alliances are not only geared to provide computer services and telephone calls, but also data transmission, video conferencing, home shopping, television, news, entertainment. Mergers and acquisitions have risen sharply in the global information technology industries, as companies are seeking the size and technology to compete in global markets. Powerful corporations and high performance networks are strengthening the commercial purpose of Cyberspace, which assumes that

---

[18] Brian D. Loader, *Cyberspace Divide: Equality, Agency, and Policy in the Information Society* (Routledge, N.Y. 1998), p33.

[19] See, Saskia Sassen, Digital Networks and Power, in Mike Featherstone & Scott Lash, eds., *Spaces of Culture: City, Nation, World* (London: SAGE Publication Ltd, 1999). "Three subjects can be read as an empirical specification of major new conditions: the growing digitalization and globalization of leading economic sectors has further contributed to the hyperconcentration of resources, infrastructure and central functions, with global cities as one strategic site in the new global economic order; the growing economic importance of Cyberspace which has furthered global alliances and massive concentrations of capital and corporate power, and contributed to new forms of segmentation in Cyberspace. These have made Cyberspace one of the sites for the operations of global capital and the formation of new power structures." P.54.

the Internet has emerged as a major new theater for capital accumulation and the operations of global capital.[20]

When the authority of the state appears to be challenged in the information age, the private authority takes on great significance.[21] In Cyberspace the private sector is taking the lead in establishing norms, rules, and institutions that guide the behavior of the participants and affect the opportunities available to others. Traditional focus on state authority and sovereignty that dominates theoretical and practical discussions of legal regulations is inadequate for explaining the full contours of the Internet activities. Although this phenomenon is not entirely new – for instance, merchants in medieval times played a large role in governance – there's something unique of current private governance activities in Cyberspace. The decentralized feature of the Internet, the complexity of the information technology, and the significant role of information plays in either the public or the private arena – working as a combined force – make private governance a vital factor whose significance cannot be ignored simply because that the interests, or rights, of all residents of Cyberspace, are at so high stakes. Saskia Sassen warns us:

> "We cannot take its democratic potential as a given simply because of its interconnectivity. We cannot take its "seamlessness" as a given simply because of its technical properties. And we cannot take its bandwidth availability as a given simply because of the putative exponential growth in network capacity with each added network. Further, when it comes to the broader subject of the power of the networks, most computer networks are private. That leaves a lot of network power that may not necessarily have the properties/attributes of the Internet. Indeed, much of this is concentrated power and reproduces hierarchy rather than distributed power."[22]

---

[20] Id. P.56.

[21] A. Claire Cutler, Virginia Haufler, and Tony Porter, eds., *Private Authority and International Affairs* (State University of New York Press, 1999), p.4-5.

[22] Sassen, supra note 19, p.56.

## 1.4 COMPETING VISIONS OF CYBERSPACE

Our thinking about Cyberspace has been shaped by the properties of the Internet. The Internet was traditionally a space of distributed power that limits the possibilities of authoritarian and monopoly control; nevertheless, the imbalance of power and segregation have already taken their hold in Cyberspace with the privatization movement in the past decade. The polarization between Internet romantics on the one hand, and the logic of business and markets on the other, is contributing to competing cultural visions of the future of Cyberspace: a utopian vision that emphasizes the decentralization and democracy of the Net, and a dystopian vision that emphasizes the global power of the large corporations.[23] We can see that both are to some extent realized in Cyberspace today.

The Internet romantics base their view on the assumptions of an earlier stage of the Internet – that the Internet will always be the open, decentralized space it was designed to be.[24] There is also an economic utopian view, especially strong in the USA, which sees the Net as offering the possibility of a whole new type of market economy, one truly open and democratic.[25] The utopian view, however, excludes the fact that Cyberspace is

---

[23] See generally, Debora L. Spar, Lost in (Cyber)space: The Private Rules of Online Commerce, in A. Claire Cutler, Virginia Haufler, and Tony Porter, supra note 21.

[24] John Perry Barlow's "A Declaration of the Independence of Cyberspace" probably epitomizes this view (1997), available at www.eff.org/barlow (visited on Sept 25, 1999).

[25] The California-based *Wired* magazine is a key axis for this line of thought. The second assumption, tightly interlinked with the first, is that Cyberspace is a purely technological event, and in that sense an autonomous space to be read in technical terms. One implication of such a technological reading is the notion that it can escape existing structures of power and inequality. Spar, supra note 23.
Margaret Jane Radin made a vivid characterization of this vision: "The utopian vision extrapolates from the old Internet model, which I have called early Cyberspace. In the utopian vision, a worldwide digital network transcends national borders and promotes open dialogue, cooperation, and self-regulation. It is a vision of free and robust scientific, artistic, educational, and political interaction. It is a model of "any to any", a two- way street where all recipients are also producers of information. It brings to the fore a hitherto submerged noncommercial tradition and extends it. It transforms politics by making true dialogue and free debate available to everyone. It makes concrete the intellectual and social infrastructure of cooperative inquiry and Undominated dialogue that democratic theorists from Dewey to Habermas have argued is needed for the basis of ideal democracy. It transforms our lives by making them more creative and satisfying." See Margaret Jane Radin, Property Evolving in Cyberspace, 15 Journal of Law and Commerce, 1996.

embedded in actual societal structures and is internally segmented. It ignores the existence of new forms of concentrated power that undermine the better features of the Internet; nor does it help in understanding the limits of such new forms of concentrated power, an important political issue.

The dystopian view of the Internet has its root of commodified manipulation and mind control.[26] According to this view, cyberspace communications are dominated by profit-driven advertising and information flow, serving nothing more important than the commercial purposes of big capitalists. The common citizens will be left out and at best reduced to passive consumers of Internet commerce. If realized, the dystopian vision would transform our lives by making them less political, less social, and ultimately less human. This is a cultural pessimism derived from a notion that the new digital technologies will replace all other technologies through which people connect: the telephone replaced by e-mail, work in office buildings by tele-work from home, social visits by on-line chat clubs, business travels replaced by video conferencing. Strong examples of this view are found especially among European intellectuals, typically those who are not vigorous users, if users at all, of the Internet.[27] This notion of "displacement" is not true, of course, as Katsh delineates in his "paradigm shift" argument. The dystopian view undermines the complementary dependencies of the new digital technologies – no technology is an absolute: it cannot replace all other technologies aimed at similar functions, in this case communication and interactivity. It also excludes the fact of growing contest between powerful economic actors and civil society in public Cyberspace, a force for strengthening political activity.

In spite of these limits, the explorations of both views did unfold analytic zones in their own right. There is an incipient literature that begins to negotiate the borderline between

[26] Radin, Id.

[27] Spar, supra note 23.

these two visions, among which is the so-called technorealism approach.[28] Dissatisfied with the extremes of utopian fantasy or high-tech doom, Technorealists manage to infuse shades of gray into a debate that has been black and white, and to bring a more realistic dialogue to the topic of technology. "We're trying to find a more nuanced, balanced and accurate way to discuss these things," Shapiro, a leading technorealist, said. As Shapiro sees it, cyber-romantics tend to eulogize technology, particularly the Internet. They have long argued for a hands-off approach by government in most matters related to Cyberspace.[29] Technorealism, unlike cyber-romanticism, implores us to see that online interactions have very real consequences for the rest of our lives. Technorealism maintains that the code of Cyberspace – that is, the collection of programs, protocols, and practices that make up our digital interactions – is itself a type of law that regulates our lives in real space. It therefore implores us to take code seriously, subjecting it to public scrutiny and criticism.[30] Cyberspace is "too important to be thought of as elsewhere (as an autonomous place). Rather we should think of it being right here... Indeed, today's intense and somewhat bewildered preoccupation with Cyberspace's distant unfamiliarity – its "otherness" – is to be expected, for this is how we treat every new technology at its

---

28 See their proclamation on Technorealism page <http://www.technorealism.org/> (visited on Dec. 10, 1999) "Technorealism demands that we think critically about the role that tools and interfaces play in human evolution and everyday life. Integral to this perspective is our understanding that the current tide of technological transformation, while important and powerful, is actually a continuation of waves of change that have taken place throughout history. Looking, for example, at the history of the automobile, television, or the telephone – not just the devices but the institutions they became – we see profound benefits as well as substantial costs. Similarly, we anticipate mixed blessings from today's emerging technologies, and expect to forever be on guard for unexpected consequences – which must be addressed by thoughtful design and appropriate use. As technorealists, we seek to expand the fertile middle ground between techno-utopianism and neo-Luddism. We are technology "critics" in the same way, and for the same reasons, that others are food critics, art critics, or literary critics. We can be passionately optimistic about some technologies, skeptical and disdainful of others. Still, our goal is neither to champion nor dismiss technology, but rather to understand it and apply it in a manner more consistent with basic human values."

29 Katie Hafner, Battle Cry of the Technorealists, *NewYork Times*, March 12, 1998, at G3.

30 See David Shenk, Andrew L. Shapiro, and Steven Johnson, Technorealism: An Overview, March 1998, available at www.technorealism.org (visited on Dec. 10, 1999); see also, Hafner, Id.

inception." But "the Net will increasingly be our interface with the world, our way of understanding and filtering reality."[31]

Technorealists have formed several principles in their understanding of the nature of cyberspace and the concurrent social changes. First, technologies are not neutral; they deem it important to consider the biases of various technologies and to seek out those that reflect our values and aspirations. Second, the Internet is revolutionary, but not Utopian. Revolutionary, in the sense that there are fundamental changes influencing the status of the individual in society – more individual control of life that were previously controlled by powerful institutions: government, corporations, and the news media. But it's not a revolution we can yet celebrate since there is resistance from institutions struggling to maintain their authority. And there is a grave danger that we will push the revolution too far, blinding ourselves to the need for balance between personal indulgence and commitment to something more. Third, Cyberspace is not formally a place or jurisdiction separate from Earth. Government has an important role to play on the electronic frontier. Markets encourage innovation, but they do not necessarily insure the public interest. Technology standards and privacy issues, for example, are too important to be entrusted to the marketplace alone. Technorealists are concerned about the role of government on the electronic frontier. They believe that people's notions of regulation, rights, and justice will have to evolve as power shifts increasingly to individuals. "Technology bestows great privileges upon us. The question is whether we will shoulder the responsibilities that accompany them."[32] Fourth, information wants to be protected. It's true that information technologies are challenging the print-age copyright laws and frameworks for protecting intellectual property. The answer, though, is not to scrap existing statutes and principles. Instead, we must update old laws and interpretations so that information receives roughly the same protection it did in the context of old media. The goal is the

---

[31] Andrew L. Shapiro, The Disappearance of Cyberspace and the Rise of Code, 8 Seton Hall Constitutional Law Journal, 1998.

[32] Andrew L. Shapiro, The Control Revolution, available at http://www.controlrevolution.com/ (visited on Dec. 10, 1999)

same: to give authors sufficient control over their work so that they have an incentive to create, while maintaining the right of the public to make fair use of that information. In neither context does information want "to be free." Rather, it needs to be protected. Last, understanding technology should be an essential component of global citizenship. In a world driven by the flow of information, the interfaces – and the underlying code – that make information visible are becoming enormously powerful social forces. Understanding their strengths and limitations, and even participating in the creation of better tools, should be an important part of being an involved citizen. These tools affect our lives as much as laws do, and we should subject them to a similar democratic scrutiny.[33]

## 1.5 CYBERSPACE IN LEGAL PARADIGM

Divergences of legal concerns are unavoidably influenced by the visions in Cyberspace sociality. Professor Lessig poses two basic sets of questions to start with the legal query. First question: Should this new space, Cyberspace, be regulated by analogy to the regulation of other space, or should we give up analogy and start anew? Should we muddle into this new space as ordinary observers, just applying our old ways of thinking, or should we enter this world as scientific policymakers, armed with a comprehensive view, structuring the environment of this world to fit with this comprehensive view? The second question follows the first: Is Cyberspace really anything new? Is there really a form of life here that we haven't known before, or is Cyberspace just an electronic version of ordinary space, where the electronics might add something, but not really very much?[34]

Depending on the answers to these questions, current regulatory perspectives can be categorized into three groups. The first approach considers that this new medium operates outside the legal *status quo* and therefore requires the construction of new legal rules for

[33] See Technorealism page < http://www.technorealism.org/>.

[34] Lawrence Lessig, The Path of Cyberlaw, 104 Yale Law Journal, 1995

its regulation. The second regards it as a challenge to legal ingenuity and seeks ways of adapting existing legal rules to that challenge. The third agrees in part with the second view (applying existing law to the Internet), but remains skeptical of the necessity to develop a body of "Cyberlaw" – "those who wish to bring order to Internet transactions should concentrate on the optimal means of applying existing legal principles to the new medium."[35]

### 1.5.1 Self-governance in Cyberspace

Those who propose self-governance in cyberspace base their argument on both descriptive and normative grounds. On the descriptive side, they claim that cyberspace is an ecological system; imposing geographically based conceptions of legal regulation and choice of law to a-geographical Cyberspace activity would harm the development of cyberspace community. On the normative side, they consider the practical difficulties of jurisdiction and enforcement of Cyberspace disputes, arguing that regulation of the information flow by any particular national jurisdiction illegitimately produces significant negative spillover effects in other jurisdictions. In contrast, they argue, Cyberspace participants are much better positioned than national regulators to design comprehensive legal rules that would both internalize the costs of Cyberspace activity and give proper notice to Cyberspace participants. The regulation skeptics conclude from these arguments that national regulators should "defer to the self-regulatory efforts of Cyberspace participants."[36]

The leading regulation skeptics are David Post and David Johnson. They argue in their landmarking article "Law and Borders – The Rise of Law in Cyberspace" that the rise of a global communications network renders obsolete traditional territorial borders and

---

[35] Supra note 15, Part I.

[36] Jack L. Goldsmith, Against Cyberanarchy, 65 University of Chicago Law Review, 1998.

jurisdictions.[37] For the purposes of law and norms, they encourage us to "separate the tangible from the virtual world." We should, they say, see Cyberspace "as a distinct 'place' for purposes of legal analysis by recognizing a legally significant border between Cyberspace and the 'real world'."[38]

Commentators who have made similar arguments include John T. Delacourt,[39] John Parry Barlow[40] and Joel R. Reidenberg.[41] These futurists emphasize the revolutionary character of the technologies and anticipate fundamental changes in the normative framework.

Self-governance proposal has incurred vehement criticisms, both on its political and legal assumptions about the state's supposed inability to regulate the Internet, and on its preference for technological solutions to hard legal issues on-line. Critics claim that it ignores the effects of private power and the state's own power in cyberspace.[42] Further, the technology solutions leave a false impression of neutrality – its origins are concealed, "whether those origins lie in state-sponsored scheme or market-structured order, and its effects are obscured because it is hard to imagine the alternative." While we think of a

---

[37] As they put it: "The rise of the global computer network is destroying the link between geographical location and: (1) the power of local governments to assert control over online behavior; (2) the effects of online behavior on individuals or things; (3) the legitimacy of a local sovereign's efforts to regulate global phenomena; and (4) the ability of physical location to give notice of which sets of rules apply. The Net thus radically subverts the system of rule-making based on borders between physical spaces, at least with respect to the claim that Cyberspace should naturally be governed by territorially defined rules." See David R. Johnson and David Post, supra note 16.

[38] See also, David G. Post, Anarchy, State, and the Internet: An Essay on Law-Making in Cyberspace, available at www.wm.edu/law/publications/jol/post.html (visited Nov 10, 1999).

[39] John T. Delacourt, The International Impact of Internet Regulation, 38 Harvard International Law Journal, 207 (1997).

[40] Barlow, supra note 24.

[41] Joel R. Reidenberg, Governing Networks and Rule-making in Cyberspace, 45 Emory Law Journal 911 (1996).

[42] James Boyle argues that the conceptual structure and jurisprudential assumptions of digital libertarianism lead its practitioners to ignore the ways in which the state can often use privatized enforcement and state-backed technologies to evade some of the supposed practical (and constitutional) restraints on the exercise of legal power over the Net. See James Boyle, Foucault In Cyberspace: Surveillance, Sovereignty, and Hard-Wired Censors, 66 U.Cin.L.Rev. 177, 183 (1997).

legal regime as coercing, technical solutions are less contentious: it seems to merely shaping – or even actively facilitating – our choices. The legal realists point out the shortcomings of that picture of the market and urge for a richer picture of Internet politics than that of the coercive (but impotent) state and the neutral and facilitative technology.[43]

### 1.5.2 Mapping Metaphors in Cyberspace

The opposing camp claims that Cyberspace transactions are no different from "physical-space" transactions. The actions of human beings online have a real impact on the lives of other human beings.[44] There is no general normative argument that supports the immunization of Cyberspace activities from territorial regulation. Although they involve people in real space in different jurisdictions, nations can exercise territorial authority to achieve significant regulatory control over Cyberspace transactions. Resolution of the choice-of-law problems presented by Cyberspace transactions will be challenging, but no more challenging than similar problems raised in other transnational contexts.

Given that the common law jurisprudence has a traditional doctrinal persistence against technological change, it is not surprising that a solution seeking metaphors in physical space is arising both in courts and academic area in the U.S.[45] There already exists vast,

---

[43] Id.

[44] "When a fraudulent securities offering on the Net causes novice investors to be bilked of their hard earned money, that's a real-space injury. When an Internet gossip maven with an audience of thousands knowingly publishes a false and injurious statement on an email list about a private figure, that also is a real-space injury. And when a group of terrorists use email to conspire to blow up a federal office building, there too is injury in real space." Shapiro, supra note 31.

[45] "Our minds, like those of legislators and Justices, are engraved with or rooted in patterns of thinking, modes of classifications. We – and our legal system – can only change by reference. Judges have a vested interest in the treasury of their prior analytic approaches, so painstakingly developed. Their very grounding in common law emphasizes a jurisprudence that – even when statutes intervene – has a gradual and organic quality. It is also fairly true that the history of communications is one of recapitulation, a repeating of categories or at least a long period of transition from one to the other... Change in technology, even massive change, is not a sufficient reason for changes in judicial doctrine. As we have seen, there is confusion over which elements of technological change affect which elements of categorical approach." See Monroe E. Price and John F. Duffy, Technological Change and Doctrinal Persistence: Telecommunications Reform in Congress and the Court, 97 Columbia Law Review, 1997.

albeit young, literature on this endeavor. A Westlaw search found that more than 100 published cases in the U.S. Federal Court system had already addressed issues related to Cyberspace, applying current "real world" law to Cyberspace issues such as copyright and free speech.[46] Scholars also enlists the commonly used term "Information Superhighway" as a metaphor for the information infrastructure in order to emphasize his point that a new legal structure is unnecessary.[47] Such metaphors serve as a map for sorting out what is similar and what is different when confronting a new problem. Litigants as well as lawyers, judges, juries, legislators and policy analysts all seek to cope with the unknown through known circumstances and prior experiences.[48]

---

[46] Hardy, supra note 14. (stating that academic and practicing lawyers are spending large amounts of time trying to determine how existing rules of libel or copyright apply in Cyberspace).

[47] See Henry H. Perritt, *Law and the Information Superhighway* (NJ: Wiely Law Publications, 1997). He compares the Information Superhighway to the interstate highway system which, like its electronic counterpart, requires various rules to ensure continued order, safety, and utility for those who use it. He notes that on a physical highway, one must have rules establishing tolls for use of the highway (analogous to NII regulation policy); payment systems for bus rides and automobile rentals and purchases (E-commerce); and rules for determining who gets to use which lanes and when (NII access policy). Likewise, the highway must have rules for allocating risk of loss for accidents (liability for harmful electronic communications); rules for assigning responsibility for fixing potholes (liability the creative process of writing often requires the use of familiar for information service failures); standards to ensure passable interconnections between roads (interoperability and standard setting); and safeguards to constrain police and others from unreasonable searches of vehicles (E-privacy). See, Scott E. Bain, supra note 5.

[48] The following models reflect only a few metaphors that might be applied to computer-mediated communication: (1) Publishers, such as newspapers, as Prodigy has been characterized; (2) Distributors, such as newsstands and bookstores, as CompuServe was characterized; (3) Libraries and Information Providers such as LEXIS, Dialog, and Medlars; (4) Private, Corporate, Non-profit Networks; (5) Personal and Club Bulletin Boards; (6) Common Carriers – traditionally government-operated postal services and today such telecommunications services as Deutsche Telecomm, Cable & Wireless, Regional Bell Operating Companies (RBOCs), MCI, AT&T, and SPRINT; (7) Mixed or Hybrid Systems, such as cable television; (8) Cooperatives, such as EduNet, NearNet, FarNet; (9) Trusteeship – Broadcasters licensed to operate "in the public interest" as trustees for publicly owned airwaves; (10) Marketplaces – the real world malls are replicated in aggregations of Information Providers such as found in the commercial malls on the World Wide Web or the search engines such as Yahoo, Lycos, or Alta Vista; (11) Information Utilities, like the electric or gas companies – community systems, such as the Santa Monica Public Information Network and the Cleveland FreeNet. See, Anne Wells Branscomb, Cyberspaces - Familiar Territory or Lawless Frontiers, Journal of Computer-Mediated Communication: Emerging Law on the Electronic Frontier Volume 2, No. 1, 1995.
But Branscomb also notes that existing legal models are designed to enforce laws within a given technology, e.g., broadcast or cable, telephone or mail. When the message traffic is mixed in a digital bit stream it becomes more difficult to sort out which kind of legal model applies, so we are never entirely

Metaphors, however, are not always "best fit" to accurately characterize all the novel activities involved in Cyberspace. It is far from certain that any mechanical metaphor (e.g., superhighway, printing press, telephone) is solely appropriate to Cyberspace. "Perhaps advocating for a new analysis is more accurate. A new analysis will necessitate a rethinking of the underlying mechanical-based metaphor(s) which define Cyberspace toward inclusion of organic-based metaphors."[49] Milner S. Ball also suggests the metaphors of law promote order rather than justice. "As the predominant form of communication shifts from print to electronic, away from printed volumes of statutes, regulations and court opinions and even further away from carvings on stone, legal metaphors will also change to reflect the changes in communication."[50] We can see that these scholars have transcended searching and mapping the existing laws as librarians looking up dusty indexes for arcane manuscripts: they are not content with the *status quo* simply because it is there; they are seeking for adaptation of the legal system from a evolutionary perspective. That is exactly what technorealism purports too, and what I believe is the strength of the third category of legal concerns. The purpose of metaphor, they believe, is not to find justification on grounds of the *status quo*, but to reconstruct our notion of rights to achieve greater balance in legal policy.

### 1.5.3 LAW OF THE HORSE?

Judge Frank Easterbrook, in his provocative article "Cyberspace and the Law of the Horse", sheds deep skepticism over the utility of developing a body of "Cyberlaw",

---

sure which one we are drawing upon. On the computer monitor we find mixed text, video, data, and even new types of texts called "hypertext" and new conglomerated forms called "multimedia." Indeed, some bulletin boards purport to be private communications among a discrete group of friends. Yet they may deliver email far and wide. When these private systems operators start delivering mail, they enter a legal domain where public interest in protecting the mail may come into play. Some more rational analysis must be devised to comprehend, much less attempt to regulate, online message traffic.

[49] Robert Reilly, Mapping Legal Metaphors in Cyberspace: Evolving the Underlying Paradigm, 16 John Marshall Journal of Computer and Information Law, 1998.

[50] Milner S. Ball, *Lying Down Together: Law, Metaphor and Theology* (Madison, University of Wisconsin Press, 1985), p112.

which he refers as "the law of the horse".[51] Unconvinced by the idealist proposition for "separate rules" in Cyberspace, as well as the hasty generalization and analogy of physical world rules for the purpose of regulating the new medium, Easterbrook leads us to think more than superficially on the regulation of Cyberspace. He believes that the task of applying existing law to the Internet is straightforward: develop a sound law in the physical world and use its general principles to guide dispute resolution in Cyberspace. "If we have not even managed to create well-defined property rights so that people can adapt their own conduct to maximize total wealth", he questions, "what chance do we have for a technology such as computers that is mutating faster than the virus in The Andromeda Strain?"

At least two points merit attention in his criticism: First, Cyberspace is not a sovereign place notwithstanding the claims of the cyber-romantics. However, it is not a separate subject (like torts or contracts or bankruptcy) from the standpoint of legal ontology that we should try to set off to one side, either. Most behavior in Cyberspace is easy to classify under current legal principles, so metaphors are feasible and necessary.[52] Second, although Easterbrook doesn't deny there's something new in Cyberspace that worth jurisprudential concern, he still insists that cautions be taken to avoid mechanical

---

[51] Frank H. Easterbrook, Cyberspace and the Law of the Horse, 1996 University of Chicago Legal Forum. "The best way to learn the law applicable to specialized endeavors is to study general rules. Lots of cases deal with sales of horses; others deal with people kicked by horses; still more deal with the licensing and racing of horses, or with the care veterinarians give to horses, or with prizes at horse shows. Any effort to collect these strands into a course on "The Law of the Horse" is doomed to be shallow and to miss unifying principles. Teaching 100 percent of the cases on people kicked by horses will not convey the law of torts very well. Far better for most students - better, even, for those who plan to go into the horse trade - to take courses in property, torts, commercial transactions, and the like, adding to the diet of horse cases a smattering of transactions in cucumbers, cats, coal, and cribs. Only by putting the law of the horse in the context of broader rules about commercial endeavors could one really understand the law about horses."

[52] It is in this sense that Easterbrook claims that there is no law of Cyberspace, and demands to develop existing laws to apply in Cyberspace. "What people freely make available is freely copyable. When people attach strings, they must be respected, and the tough question when someone copies commercial software will be whether the person making copies is a direct infringer or only a contributory infringer, and whether the remedy should be civil damages or time in prison. Lower costs of copying may make violations of the law more attractive, which suggests the allocation of additional prosecutorial resources, but movement along a cost continuum does not call for change in legal substance." Easterbrook, Id.

metaphors, especially for such a novel sphere as Cyberspace since we don't have sufficient knowledge or experience in dealing with it. Other scholars also agree that "Lawyers, legislators, and judges should tread lightly in cyberspace, lest their attempts to draw analogies to past and existing rigid legal rules limit the growth of a true computer-mediated information marketplace."[53]

But technorealists insist a critical legal perspective on technology and the implications of those seemingly "neutral" technical "code" in Cyberspace,[54] even admitting that no formal law of Cyberspace exists. Julie Cohen makes the point that the need for such a critical perspective might be analogous to the need for feminist legal theory, even though we don't have, or need, a law of women. As many would agree, our online interactions have distinctive legal and regulatory attributes – a combination of formal law, norms, market forces, and particularly code. However, in the view of technorealists, Cyberspace code should concern us not because of what it does to public values "in Cyberspace", but because of what it does to public values in our own real spaces. All code, in other words, is real space code. "The regulatory power of software code is not affecting some band of space travelers in a far off galaxy. And as Cyberspace becomes so integrated into our lives that it effectively disappears, an increasing proportion of all regulation – here, there,

---

[53] Owen Fiss, In Search of a New Paradigm, 104 Yale Law Journal, 1995.

[54] Lawrence Lessig, The Law of the Horse: What Cyberlaw Might Teach, Stanford Technology Law Review available at http://stlr.stanford.edu/STLR/Working_Papers/97_Lessig_1/article.htm (visited on Dec. 7, 1999): "My argument about Cyberspace comes down to this: that while there are similarities between the regulations of real space and the regulations of Cyberspace, these similarities hide important differences. Copyrights management systems are not the same as copyright law; code contracts are not contracts; a PICS enabled world is not this world; real space code is something less than Cyberspace code. The differences here come from the regulatory power of code. Code is a kind of sovereign – in the sense that Foucault, if not Austin, would have understood. My argument has been that we should take seriously the regulatory power of this Cyberspace code, if we are to preserve the values of real space there.Our way of thinking about regulation just now, and the scope of our thinking about the constitution, leaves little space for this point. But this is a point that we need to get quite quickly. As the net grows, as its regulatory power increases, as its power as a source of norms becomes established, real space sovereigns lose. In many cases, we might think that a good thing. But we can't think it a good thing generally. There is nothing to guarantee that the regime of code will be a liberal regime; and little reason to expect an invisible hand of code-writers to push it in that way." However, Lessig didn't deliberate on how to guarantee the regime not to be a liberal regime, and that is exactly what technorealists are deeply concerned, since to them, software codes affect people in real space relations.

and everywhere – will be by code. Rather than worrying about how we will regulate Cyberspace, then, we should be concerned about how Cyberspace will regulate us – our legal principles, our values."[55] Shaprio points two hazards in approaching to Cyberspace. On the one hand, seeing Cyberspace as elsewhere will cause us to misconstrue its legal significance. It will particularly keep us from seeing the way that regulatory forces like Cyberspace code are actually affecting us in real spaces. On the other hand, once we recognize that Cyberspace is simply a construct – a control space as close to home as our own minds – we may take it for granted. As this lens becomes ever more familiar, we must recall just how powerful it can be. This new way of seeing, and interacting with, the world can cause profound social, political, and legal change. As Cyberspace disappears, we must be vigilant in safeguarding our cherished values and rights against the rise of code.[56]

## 1.6 CONFLICT OF RIGHTS IN CYBERSPACE

By information rights I mean the right to control information. The right to privacy empowers individuals to control their personal information; copyright restricts unlicensed exploration of certain "expression" of information. A common feature of these rights is that they deal with the ownership and control of information and involve both the public and private sectors of society, the boundary of which has become blurred in cyberspace. The development of information technology and the facilitation of communication have given rise to a new realm of law – information law, a cross-section study that combines many ingredients of legal specializations: from public records law to consumer protection, from copyright law to digital agenda for user's rights.[57]

---

[55] Shapiro, supra note 31.

[56] Id.

[57] For a detailed discussion of the information law as a burgeoning legal branch, see Egbert J. Dommering and P. Bernt Hugenholtz eds., *Protecting the Fact: Copyright, Freedom of Expression and Information Law* (Deventer & Boston: Kluwer Law and Taxation Publishers, 1991).

### 1.6.1 RIGHTS IN CONFLICT

Two factors of information rights contribute to the conflict in cyberspace: the nature of Information as an economic and cultural commodity, and the overlap of rights (and therefore, conflict of interests) in information.

First, information is often characterized by economists as public goods. It is often expressive to generate but cheap to copy. Furthermore, one person's use of information does not exclude the possibility of their use by another person. This might cause underproduction because there will be too little incentive to create information. Ejan Mackaay rightly points out, "The exclusive individual use of a good can be achieved by payment of a price and transfer of a right. In the case of collective goods this is (virtually) impossible."[58] The "public good" quality of information has deep implications for information rights when digital technology greatly reduces the cost of replication and dissemination of information on the Internet. For example, if you have a copy of a copyrighted photo, rendered in a graphics file, you can make unlimited copies of that file with no effect on the original. When you make the one-hundredth copy, nothing indicates that it is the one-hundredth rather than the first. Consequently, even private copying activities are now deemed commercially relevant to the interests of right-holders as constituting competing activities. If unauthorized and widespread, such user activity could radically undermine traditional copyright markets.

Secondly, conflict of information rights is a ubiquitous phenomenon because different interests may coexist in one and the same object much more often than in the case of the ownership of material goods. While database owners have copyright over the compilation of data, such a right may be limited by the privacy right of the data subjects whose personal information is stored in the database. It is this duplicity of titleholders over the same source of information that often causes conflicts in information rights. Information

---

[58] Ejan Mackaay, The Economics of Emergent Property Rights on the Internet, in Egbert J. Dommering and P. Bernt Hugenholtz eds., *Protecting the Fact: Copyright, Freedom of Expression and Information Law*, Id.

rights are therefore constantly a balancing of ownership and privacy on the one hand, and the freedom to obtain and disseminate information on the other hand.

Therefore, the conflict of rights in cyberspace is analyzed in the thesis in two-dimensional sense: the information technology has profound impact on rights in the physical world; and the rights sanctioned by physical world laws further complicates rights in cyberspace. As a result conflicts exist both in Cyberspace and real space, and the solution in either area is correlated with the other. While I talk about "conflict of rights in Cyberspace", implicitly I take side with technorealists and probe into their relations with substantive rights issues in the real space. In this thesis I will examine two major aspects of cyberspace where rights in the real world come into conflict: Privacy and Copyright.

#### 1.6.1.1 Privacy

It was once too expensive for anyone but the government to collect, store, and coordinate data, creating profiles on hundreds of millions of citizens. But the growth of networked computing has allowed data compilers, direct marketers, and list-sellers to gather and sell personal information about practically everyone. The result is a broad and lucrative market for personal information that allows anyone to find out nearly the complete personal file about anyone else, just by trolling around the Internet. What are the responses of states? Choice between broad-covering, uniform regulation and discrete self-regulation has become a political issue in Cyberspace. While the EU has drafted detailed Personal Data Protection Directive, the prevailing wisdom in the U.S. has been that technology will empower individuals to protect their own privacy and major initiatives should come from private sector – the so-called self-regulation. Can citizens trust private sector's sincerity to respect their own privacy? The issue seems to be a matter of control rather than balancing privacy and commercial interests – Who has the right to personal information, the individual related, the information compiler, or some random surfer on-line? Already suggestions of creating property rights in personal information have come out in North America, with the emphasis on individual choice and control guaranteed by property rights and market-based solutions to social problems. Just

as there is demand for consumer data among corporations, so there is a counterdemand on the part of individuals to keep that information private. The answer, these privacy advocates claim, is to have consumers embrace this market and bargain with vendors over acceptable rules for data collection and use. The same way that advocates of direct democracy have called for government representatives to give individuals more control, these privacy advocates have demanded that consumers, not government, be empowered to control the flow of personal information.

Yet privacy meet greater challenge in a seemingly "benign" area, where personally identifiable information is widely disseminated with government's endeavor to make a broad range of public records available on-line and with the commercial exploitation of such public records. The Internet facilitates information flow, and in turn, put higher expectation on government's transparency in public management. Putting public records on WWW has its imperative to meet democratic demand rather than being a reproachable policy. The problem lies in the technological capacity of the Internet to transcend traditional restraints on government's dealing with personal information (restrictions on computer matching, for example), and it is further complicated by the commercial exploitation of public records under the protection of Freedom of Information Acts (FOI). While the right to information access competes with the right to privacy here, we need to understand how the nature of these rights has been changed by information technology before making a regulatory preference. Although there is every reason to applaud the idea of individuals working to safeguard their own privacy, expecting them to do so effectively without any help from government is dangerously naive. It assumes that individuals can use technology and the market to achieve a task of such complexity that it has, to date, confounded most governments. What it amounts to is the privatization of privacy protection, which will likely create as many dilemmas as it solves, if not more.

#### 1.6.1.2 Copyright

The conflicting notions of copyright in Cyberspace lead us to ponder over the nature of new right claims associated with technological innovations in general. It is about the

evolution of the assumptions underlying legal rights. It is, in essence, a question of legal philosophy on right *per se.*[59]

In her brilliant article "Property Evolving in Cyberspace", Margaret Jane Radin expounds on how copyright has changed in the digital context as opposed to printing context. "In the ideology of property that we have inherited, property rights are attached to objects." "Copyright perpetuates the notion that property attaches to objects", because "copyright is about copying objects, such as books and paintings, in which works are fixed in tangible form. Works themselves are thought of as fixed unchanging acts of authorship. The key words are 'fixed' and 'tangible'. 'Objects' in cyberspace, however collections of bits that are apprehended as works are ceasing to be fixed and tangible. They are becoming moving, dynamic, and malleable. There is no 'thing' that embodies the work, only fleeting electrical impulses. Works metamorphose as they move over the net. Works and the medium that embodies them are ceasing to be objects, and becoming processes."[60] Since print documents are objects, fixed, whereas electronic documents are

---

[59] Hart admits, "The notion of a legal right has proved in the history of jurisprudence to be very elusive." (H. L. A. Hart, Legal Rights, in *Essays on Bentham: Studies in Jurisprudence and Political Theory* (Oxford: Clarendon Press, 1982), p.162.) Legal positivists claim that rights are only the creatures of positive law. As Bentham put it, "Rights are the fruits of the law and of the law alone; there are no rights without law – no rights contrary to law – no rights anterior to the law." (John Bowring, *Works of Jeremy Bentham*, III (Edinburgh: W. Tait, 1838-1843), p.221.) "In proportion to the want of happiness resulting from want of rights a reason exits for wishing that there were such rights. But reasons for wishing there were such things as rights are not rights: a reason for wishing that a certain right were established is not that right – want is not supply – hunger is not bread." (*Works of Jeremy Bentham*, II, p.501.) Geoffrey Marshall, however, notices that "[m]ost general concepts in legal and political theory can be used without absurdity in broader or narrower senses and this is true of the notion of a right". "There is an obvious characteristic of a right which can be seen most clearly in the case of the typical constitutional or 'human' right, but which may have been partially obscured when 'claim rights' have been contrasted with 'liberties'. This is that a right is always subject to competition from other rights and entitlements." (Geoffrey Marshall, Rights, Options, and Entitlements, in *Oxford Essays in Jurisprudence*, 2nd series, ed. Simpson (Oxford: Clarendon Press, 1973), p228.)

With the pluralistic notions of right in mind, it might be safe to say that right has a broader usage beyond legal discourses, which correlates with such factors as moral values, interests, power and other customary social norms. Rather than a stagnant legal creation, it is in a constant evolutionary process in which some claims finally are given public force and thus become what Holmes call "legal rights". ("A legal right is nothing but a permission to exercise certain natural powers, and upon certain conditions to obtain protection, restitution, or compensation by the aid of the public force. Just as far as the public force is given a man, he has a legal right, and this right is the same whether his claim is founded in righteousness or iniquity." O. W. Holmes, Jr., *The Common law* (Boston: Little, Brown, and Company 1881), p.214.) The rights discussed in the thesis are referred to in this broader sense.

[60] Radin, supra note 25.

processes or fluid, the change from fixity to fluidity is thought to have profound implications for intellectual property. Michael Heim also observes that "If the work of the author no long carries with it definite physical properties as a unique original, as a book in a definite form, then the author's rights too grow more tenuous, more indistinct."[61] If the author, like the text, becomes dispersed, how does society fairly assign legal, commercial, and moral rights?

Understanding the gap between assumptions underlying traditional legal rights and the nature of the current hypertext technology has significant implications. It will help form a healthier approach in dealing with the competing claims on rights in the new medium where legal metaphors lose their force. Much of the copyright disputes on the Internet are in the form of hypertext,[62] which has been associated with individual freedom and empowerment from its invention.[63] Technology always empowers people. It empowers those who possess it, who make use of it, and those who have access to it. And it does so at a certain cost. Access to the Internet implies access to texts "on" it, and this access raises the issue of who has the right to access to a text – access to read it as well as to link to it. Attitudes toward the correct and incorrect use of a text written by someone else depend importantly upon the medium in which that text appears.[64] Conceptions of authorship relate importantly to whatever information technology currently prevails, and when that technology change or shares its power with another, the cultural construction of authorship of authorship changes, too, for good or ill. From the point of view of the

---

[61] Michael Heim, *Electronic Language: A Philosophical Study of the Word Processing* (New Haven: Yale University Press, 1987), p.221.

[62] It is text composed of blocks of words (or images) linked electronically by multiple path, chains, or trails in an open-ended, perpetually unfinished textuality described by the terms *link, node, network, web,* and *path.* See George P. Landow, *Hypertext: The Convergence of Contemporary Critical Theory and Technology*, Baltimore: The Johns Hopkins University Press, 1992, p.3.

[63] Id, p.169.

[64] As H.J. Chaytor comments, "To copy and circulate another man's book might be regarded as a meritorious action in the age of manuscript; in the age of print, such action results in law suits and damages." H.J. Chaytor, *From Script to Print*, Cambridge, England: Heffer and Sons, 1945.

author of a print text, copying, virtual textuality, and hypertext linking must appear wrong. They infringe upon one person's property rights by appropriating and manipulating something over which another person has no proper rights. In contrast, from the point of view of the author of hypertext, for whom collaboration and sharing are of the essence of "writing", or linking, appear absurd, indeed immoral, constraints. In fact, without far more access to (originally) printed text than is now possible, true networked hypertextuality cannot come into being.[65]

### 1.6.2 Taking Rights Seriously

I borrow the warning from Dworkin not for discussing citizens' moral rights against government in a centralized authority age,[66] but for suggesting individuals' rights against technologically facilitated private power in the decentralized information age. The point in common lies in the urge for "taking rights seriously", either in physical world or virtual reality, public affairs or private transactions. There are two worrying trends towards rights in Cyberspace which treat rights so "lightly" that has impeded proper appreciation of their essential nature. One is shopper-for-free's asking too much without discern; the other is passive spectator's wait-and-see attitude.

Too much discussion of rights begins with a shopping-list of demands for rights of every imaginable sort, as if rights have no cost – given as holiday coupons. It is no exception in Cyberspace where virtual communities are spawning. A web-document expresses a set of "electronic rights and responsibilities", "to provide an ethical standard with which to measure the policies of states and corporations with regard to the Internet and related multicast communications networks." It is an interesting mixture of pious hopes and practicability. Unfortunately, it fails to grapple with the problem of balancing conflicting rights. Worse, it seems to generally deny legal enforcement of responsibilities and constraints on rights, other than intellectual property and contract. Due to the non-

[65] George P. Landow, supra note 28, p.196-198.

[66] Ronald Dworkin, Taking Rights Seriously, in *Oxford Essays in Jurisprudence*, supra note 59.

geographical nature of Cyberspace, it's hard, if not impossible, for governments to effectively enforce laws relating to information flow, and hence freedom of access, freedom of expression and the intellectual property rights are becoming dependent on factors other than legislation, the courts and law enforcement regimes. You either have the means to discover and access documents, or you don't; you either feel free to post a document or express an opinion, or you don't. On the net – the electronic frontier, it's action that counts; a formal right may be superfluous, and in any case unenforceable by conventional authority.[67]

The laissez-faire attitude of "wait and see" is even more dangerous in that it ignores the private power in Cyberspace, and arrogantly assumes that corporations and providers will be altruistic enough to do the right thing. Such assumption results in part from the misconception that technology is neutral and market operates on the apolitical principle of economic efficiency. But to Shaprio, Cyberspace is a locus of control. "It is an interface that allows us to control other things – the information we are exposed to, the people we socialize with, the resources of the physical world."[68] The current situation in the network tends to favor giving the power of control to those with the power of the purse (i.e. service providers). Further, reliance on essentialized notions of "contract", "market", and "property" elides important empirical and policy questions about the extent of the monopoly that society should afford creators of digital works. But technology is not destiny. Rather, our perception of possible technological solutions is colored by our approach to market and legal institutions, and vice versa.[69]As one posting on the Web cries for attention, "If you want something, you have to fight for it – vigorously. It's not enough to sit back and wait. What makes you think that once something is well-

[67] Roger Clarke, Information Technology & Cyberspace: Their Impact on Rights and Liberties, available at http://www.anu.edu.au/people/Roger.Clarke/II/VicCCL.html (visited on Nov. 28, 1999).

[68] Shapiro, supra note 31.

[69] Julie E. Cohen, Lochner in Cyberspace: The New Economic Orthodoxy of "Rights Management", 97 Michigan Law Review, 1998.

established, that the people in charge will suddenly get up and do an about face on fundamental issues just because YOU want them to?"

The following thesis attempts to show that the definition of rights and responsibilities in cyberspace can be accomplished in a variety of ways. The obvious ways are the "top down" implementation of rules through legislative enactment or judicial decision. But there are also other "bottom up" rule making processes. Unilateral self help with empowering technologies (such as Platform for Privacy Protection – P3P, or the Electronic Rights Management System by copyright owners (ECMS)), contracts, the evolving customs and code rules on the Net, are all mechanisms by which behavior in cyberspace might be regulated. The thesis examines the major parties who are the decision-maker in determining the definition and entitlement of rights, as well as other stakeholders whose interests are impacted, whether with awareness or without, in the process. It also examines the dynamic process how such decisions be enforced or legitimized, and suggests when public input should intervene when self-help cease to work or contracts malfunction. In doing this the author intends to make the point that as the information becomes more and more automated by technologies, we should not be deluded by the attractiveness of technical solutions which appears to be "just the way things are." Instead, we need to be constantly conscious of the fact that our rights are implicitly undergoing a control battle in which technology and law are colluding to change the established equilibrium in the real world, as well as in cyberspace. If we are to have some alternatives to the digital libertarianism, we will have to contribute our own input to the process of shaping and re-defining rights in cyberspace as well as in the real world.

# CHAPTER II CONTESTED PRIVACY IN CYBERSPACE

## 2.1 PARADIGM SHIFT: THE PUBLIC VERSUS THE PRIVATE

A Portland company, Commercial Information System, offers online access to computerized public records to help businesses make pre-employment screening. Timely acquired and properly utilized, such information as background and propensity for misconduct can be a valuable tool for sound and efficient employment or public safety evaluations. "Public records resource companies make information more accessible and more useful," said Portland attorney Charlie Williamson, a business attorney. "They don't get at anything that's not already public. The only difference is the time it takes." Williamson and his colleagues use a commercial public records service to verify assets, property values and juror credibility.[70]

Florida, January 1999. Some Internet Service providers and electronic databases that offer subscribers look-up information about state motor vehicle records were accused for recklessly and illegally assisting anti-abortion groups to track down and harass abortion clinic patients. One of the defendants, TML, "the largest provider of online interactive access to motor vehicle records in the United States and Canada," offers clients access to the motor vehicle databases of 30 states without verifying via follow-up phone calls that the subscribers were permissible users of the information under Driver's Privacy Protection Act of 1994. "CompuServe and TML are basically selling a product they know

[70] James Rudolph Rauh, Open Public Records: When Does the Public Have the Right to Know? 56-June *Oregon State Bar Bulletin*, 1996.

can be badly misused," said a well-known abortion-rights litigator, "They have been selling roadmaps to stalkers."[71]

The above exemplifies how the Internet raises controversies over the availability and use of personal information from on-line public records. "On the one hand, we love our privacy. On the other, we want information, and we want to find it as quickly and conveniently as possible. However, if we can uncover the details of other people's lives, they can just as easily intrude into our own secretes..."[72] The conflict between these two interests – privacy versus easy access to information – has been a hot topic with the development of information technologies (IT) and the spread of Internet users. The Internet facilitates information flow, and in turn, put higher expectation on government's transparency in public management.

The issue is further complicated by the prosperity of E-Commerce which has turned information privacy into a scarce commodity without sufficient consumer unawareness. With the explosive increase in the Internet transactions, the collection of personal information has become a ubiquitous practice. While many transactions ask users' authorization to collect such information, many do it in a way that the users are unaware of. Certain technologies, such as "cookies" and Java applets, originally invented for convenient and efficient access to the web, allow web site owners to monitor people's interests in their products and services surreptitiously through the covert gathering of personal data.[73] Some web sites use computer programs such as "cgi-bin"[74] to massively

---

[71] Carl S. Kaplan, ISPs and Database Sued in Abortion Case, *Cyber Law Journal*, January 22, 1999, available at http://www.nytimes.com/library/tech/99/01/cyber/cyberlaw/22law.html (visited Nov. 27, 1999)

[72] Helen Burwell, in Carole A. Lane, Naked in Cyberspace: How to find personal information online, Wilton, CT: Pemberton Press, 1997.

[73] *Commercialization of the World Wide Web: The Role of Cookies* (quoting Privacy Times Editor, Evan Hendricks), available at http://ecommerce.vanderbilt.edu/cb3/mgt565a/group5/paper.group5.paper2.htm (visited Nov. 18, 1999).

[74] "CGI" stands for Common Gateway Interface, the programming interface for executing programs on Web servers. "CGI defines the structure for passing data from the server's gateway program, which does

collect personal information through on-line forms and registrations which are supposedly for verification purpose only. As a by-product of such on-line marketing practice, consumers leave more and more electronic footprints to unknown entities. With the help of the computer technologies, information can be analyzed in ways that were previously impossible or economically infeasible, and marketers are able to identify smaller "niches" of the population, ultimately "drilling down" to the individual level.[75] In September 1995, Market Inc., a list broker in Washington, announced the availability of a list of 250,000 e-mail addresses compiled from Internet newsgroups and Web sites. The controversial file, segmented into eleven "interest" categories (adult, computer, sports, science, education, news, investor, games, entertainment, religion and pets), was withdrawn a month later because of "vociferous" reaction from the public.[76] In June 1996 Lexis-Nexis released P-TRAK, an on-line product for attorneys and other subscribers to use to locate individuals. The files were based on header information from consumer credit reports. Swift and furious public outcry led the company to scale back the availability of some of the information (such as social security numbers) and give subscribers the option of being removed from the directory.[77]

It is worth noting that the most common case of information privacy invasion in cyberspace transaction takes place in voluntary disclosure: when one fills out a registration form or survey questionnaire on-line, he is seldom aware that the information would be sold or rent to a third party for commercial use, with unrelated purposes he is informed in the initial transaction. Ever increasing competition leads companies to use transactional data to engage in direct marketing specifically tailored to attract certain

---

the processing, and returning the results from the from the gateway program to the HTTP server back to the requesting client." Alan Freedman, The Computer Desktop Encyclopedia, p.119.

[75] Ann Cavoukian, Who Knows: Safeguarding Your Privacy in a Networked World (Random House of Canada, 1995), p. 85.

[76] Larry Jaffee, *List Company Resigns E-mail File*, DM News, October 23, 1995 at 1.

[77] Elizabeth Corcoran and John Schwartz, *On-line Database Draw Privacy Protests*, Washington Post, September 20, 1996 at 1.

kinds of consumers. As competition grows and profit margins shrink, companies sell this information in order to increase revenue.

In this Chapter three aspects of privacy will be examined: (1) the dissipation of the secrecy paradigm by the two-way data flow that extinguishes the border between the public and the private; (2) normative implications of the property rule for the commercial exploitation of personal information, and privacy concerns in personal data released by such "consented" transactions;[78] and (3) International initiatives in the regulation of information market. The conclusion is based on a cautionary note that when information technology has profoundly altered the conception of the right to privacy, the border between the public and private "paradigms" no longer exist in the practice of personal information collecting. We need to be more sensitive toward the value choice underlying current institutional responses. Whether personal data has become a commodity or we still retain moral rights in it, privacy norms in cyberspace should be shaped in a more transparent and holistic process.

## 2.2 INFORMATION PRIVACY IN THE PUBLIC SECTOR

Already, many governments are beginning to take the initiative to offer widespread dissemination of government records on World Wide Web (WWW) to meet democratic

[78] Some make a distinction between security and privacy on the Internet. Personal information gathered without the individual's knowledge or consent is referred to a security issue, while privacy refers to data protection: once a seller or other organization legitimately receives personal data, who many have access to the information and what other uses of it are permitted? See Peter P. Swire and Robert E. Litan, *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive* (Brookings Institute Press 1998), p.82.
A variety of technological tools are used to increase consumers' sense of security in cyberspace. The most popular and effective tool is encryption, one of the most powerful software encryption programs being PGP (Pretty Good Privacy). Another tool is the use of an anonymous server to send e-mail or access Internet sites anonymously. Security measures also include passwords, domain name filtering, Internet address filtering, or a firewall to prevent access by unauthorized users. Filtering can be used to reduce unsolicited commercial e-mail by blocking e-mail that matches categories, such as sender or subject. To avoid having a Usenet posting indexed by a search engine, "X-no-archive: yes" should be added to the header of the message or made the first line of the message. In response to concerns about cookies, newer versions of Web browsers, such as Netscape 3.0, have mechanisms which notify the user before a cookie is set. Software has also been developed to assist users in managing cookies.

demand of the public's participation. Others are selling computer tapes to entrepreneurs who have created searchable databanks containing hundreds of files. Court records, property tax records, law enforcement records, records of drivers' licenses, land titles, political contributions and professional licenses, and many other forms of public records now are finding their way to the Web. Large and small vendors of public information have sprung up in North America. These records can be compiled, searched[79], reorganized, and manipulated, so that valuable information emerges from them. Although public records are often made available to anyone who searches for them, the easy access and anonymous availability of the information online have raised serious privacy and public safety concerns.[80] There is a difference between an electronic compilation in searchable form and records that can only be found by a diligent search through scattered files. The former presents a far greater threat to privacy. The technological capacity of the Internet, complicated by the commercial exploitation of public records under the protection of Freedom of Information Acts (FOIA), has circumvented the traditional restraints on government's dealing with personal information (restrictions on computer matching, for example). It's not surprising that privacy advocates view Internet access to public records as risky business. They see it as an opportunity for imposters to access and misuse the data. However, before we haste to make a regulatory preference, it is necessary to understand the changed concept of privacy by the information technology.

### 2.2.1 From the Secrecy Paradigm to Freedom of Information

James Madison in 1822 during his incumbency as the U.S. president: "A popular government, without popular information or the means of acquiring it, is but a Prologue to a Farce or a Tragedy; or perhaps both. Knowledge will forever govern ignorance; and a

---

[79] Information can be located by search engines, some of which index every word on the page. We now hear of "meta" search engines, which provide search results covering multiple search engines simultaneously. If personal information exists on the Internet, it can be found by anyone who is interested enough to go looking for it. See Helen Burwell, in Lane, supra note 72.

[80] Hal R. Varian, Economic Aspects of Personal Privacy, in *U.S. Department of Commerce Privacy and Self-Regulation in the Information Age*, available at http://www.ntia.doc.gov/reports/Privacy/selfreg1.htm#1C (visited Jan. 22, 1999)

people who mean to be their own Governors, must arm themselves with the power which knowledge gives."[81]

Public records are those records which a governmental unit is required by law to keep or which it is necessary to keep in discharge of duties imposed by law. A "public record" is "a record, memorial of some act or transaction, written evidence of something done, or document, considered as either concerning or interesting the public, affording notice or information to the public, or open to public inspection."[82] The public has an interest in the activities and operations of government, and public availability of some personal data is appropriate. Information is sometimes collected primarily for the purpose of making it public. Some basic functions and institutions depend on the public availability of records to operate. The land ownership and transactions rely on the public availability of land title records. The public-accessible bankruptcy records are also integral to legal process. In other cases, public access may be neither essential nor desirable. We do not make income tax returns public nor do we release library loan records, criminal investigatory files, or welfare records. [83]

Public's access to information is usually balanced with private's interests in protecting information privacy. But the appropriate level of privacy protection is not easy to determine. Privacy interests can conflict with interests in the free flow of information. In addition, the free flow of information promotes other interests, for instance, the development of dynamic marketplace, which produces substantial benefits for individual

---

[81] Letter from James Madison to W. T. Barry (Aug. 4, 1822), reprinted in *The Complete Madison* (S. Padover ed. 1953), p. 337.

[82] *Black's Law Dictionary*, 6th ed. West Publishing Co. 1991.

[83] Robert Gellman, Public Records, Public Policy, and Privacy, 26 Human Rights, Winter, 1999.

consumers and society as a whole.[84] Concerns over consumer Internet privacy, however, can weaken the efficiency of the electronic commerce.

Besides the compromising effect of privacy to many societal interests of freedom of information, privacy is a notoriously vague concept that eludes definitive legal protection. Although privacy was described by Justice Louis Brandeis as the "most comprehensive of rights",[85] and people often invoke their "right to privacy" in their casual conversation, it is hard to define what constitutes an invasion of privacy. Because of these emotive definitional problems of privacy in different philosophical and political perspective, many refuse to take privacy as a legal right that worth protection for its own purpose. "Privacy has a social value in itself; it can be regarded as a human right. Data confidentiality... is a means to an end. It has no intrinsic value."[86] Applying economic methods of analysis, Richard Posner agrees that data protection can best be regarded as an intermediate economic good used to acquire other utilities.[87]

Bennett categorizes three broad policy questions in privacy: 1) the right to be free from unwarranted intrusions (from law enforcement officials, persistent journalists, telemarketers and so on); 2) the right to make private decisions free from government interference, especially in relation to intimate family decisions; 3) the right to have some control over the collection, storage, manipulation and dissemination of personal information. This last concern has been termed "information privacy" or "personal data protection" (the European nomenclature), the problem confined to the difficulties that arise when modern public and private organizations employing the latest information

---

[84] National Telecommunication & Information Administration, U.S. Department of Commerce, *Privacy and the NII: Safeguarding Telecommunications-Related Personal Information,* p.24-25 (1995).

[85] Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

[86] James Rule et al., *The Politics of Privacy: Planning for Personal Data Systems as Powerful Technologies* (New York: Elsevier, 1980), p.22.

[87] Richard A. Posner, An Economic Theory of Privacy, in *Philosophical Dimensions of Privacy*, ed. Schoeman, (Cambridge University Press, Cambridge, England, 1984), p.333-345.

technologies process enormous quantities of information about individuals.[88] It is in this third sense – information privacy – that is concerned in the discussion of online public records.

Some may argue that privacy concerns have little, if any, conflict with the FOIA, since the deal with different types of information which have little overlaps. But this view has several serious problems: First, the advent of the Internet technology has made the border between "public" and "private" more and more fuzzy. In modern society, privacy pertains to relations between individuals and corporate or government organizations as well as to relations among individuals. When these organizations are part of the public realm, privacy concerns cross the boundaries between public and private.[89] Further, a most prominent source of online public records comes from the private "look-up" Internet services. Another problem in legislating privacy is its definition as an individual right. "Our individual rights-laden public language" impoverishes our political discourse because issues "tend to be presented a absolute, individual, and independent of any necessary relations to responsibilities".[90] Nevertheless, privacy serves not just individual interests but also common, public, and collective purposes. Privacy is both a "social value" and "an individual interest" because record-keeping relationships are "inherently social".[91] It should be balanced against other significant societal values and interests, including the freedom of information interests, the freedom of expression, the societal interests in law enforcement and costs.[92]

---

[88] Colin Bennett, Personal Data Protection in Canada's Private Sector: Current Regulation and Future Prospects, in *Freedom of Information Law: materials prepared for a Continuing Legal Education seminar held in Vancouver, B.C. on November 19, 1993.*

[89] Priscilla M. Regan, *Legislating Privacy: Technology, Social Values, and Public Policy* (Chapel Hill & London: The University of North Carolina Press, 1995), p.213.

[90] Privacy Protection Study Commission, *Personal Privacy in an Information Society*, Washington, D.C.: Government Printing Office, 1977, p.21.

[91] Id.

[92] Regan, supra note 89.

The U.S. Federal Freedom of Information Act (FOI Act) contains two exemptions that allow an agency to withhold information if it concludes that release would invade the privacy of individuals. One exemption protects "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy."[93] The other applies to "records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information...could reasonably be expected to constitute an unwarranted invasion of personal privacy."[94] The statute involves two components for recognizing a right to privacy: subjective and objective. As Justice Harlan in Katz v. United States delineated:

"There is a twofold requirement, first that a person has exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'realizable.'"[95]

Harlan's two components represent a balancing test: the individual's subjective expectation in remaining private versus the public's objective expectation regarding what can reasonably be kept private. It is not only necessary that the person claiming privacy have a subjective expectation of privacy, but that expectation must be objectively reasonable in light of existing social practices and social values. But problems of uncertainty still exist in both components.

In terms of subjective matter, the need for privacy and the effects of deprivation vary from person to person over time and in different situations. Some are, by inclination, more 'public figures' than others, who may prefer the role of private citizen. Actually, we may feel it easier to decide when our privacy has been invaded or intruded upon, rather than drawing a definitive zone of privacy around us.[96] Realizing this emotive nature of

---

[93] 5 U.S.C. 552(b)(6)

[94] 5 U.S.C. 552(b)(7)(C)

[95] Katz v. United States, 389 U.S. 361 (1967). (Harlan, J., concurring).

[96] Terry Thomas, *Privacy & Social Services* (Aldershot, Hants, England: Arena, 1995), p.11-15. "Whilst a legal definition of privacy remains problematic, perhaps a definitive definition on psychological or

privacy, Wacks suggests us measure information privacy by identifying what special interests of the individual we think the law ought to protect. At the core of the preoccupation with the "right to privacy" is the protection against the misuse of personal, sensitive information.[97]

In terms of "reasonable expectation" – objective aspect of privacy, it is also highly context-based. Competing social values and the need to function in society often require individuals to make decisions to disclose otherwise personal facts; for instance, the need to disclose financial and tax records to obtain mortgage financing. In other cases, individuals may disclose private information based on personal values and relationships (e.g., to one's spouse, a confessor, or a physician). The balancing of competing interests – freedom of information v. privacy – has been a timeworn dilemma for legislators and policy-makers.

### 2.2.2 Rethink Information Privacy in Cyberspace

Privacy is a subjective, contextual, and culturally sensitive concept. Our notion of privacy has always been influenced or even formed by technological capability, societal values and cultural norms. "As new technologies are adopted and incorporated into the routines of daily life, new wrongs can occur, and these wrongs are often found to invalidate the tacit presuppositions on which ideas about privacy had formerly been based. The moral interest at stake in data-protection regulation has seemed unclear to many."[98] Laws that protect privacy mirror societal values. In many jurisdictions around the world, privacy is protected by law and enforced by the courts, not merely because the individual has a subjective expectation of privacy, but because that expectation is also considered

---

philosophical grounds is less important. It could be argued that other values, like "equality", "freedom" and "liberty, are equally difficult to pin down. Perhaps of more importance is the value we generally place on privacy".

[97] Wacks, R. *Personal Information* (Oxford: Clarendon Press, 1989), p.10.

[98] Agre and Marc Rotenberg eds., *Technology and Privacy: The New Landscape* (Cambridge, Massachusetts: The MIT Press, 1997), p.7.

objectively reasonable in the context of current social practices and values. The Internet is already changing both the individual's reasonable expectation of privacy and the concept of what is socially acceptable or reasonable to expect.[99]

First, it is changing the means by which we obtain and generate information. Much of the personal information available now has been available for many years. However, they have been relatively inaccessible. For instance, while public records containing personal information theoretically have always been open to inspection, for various reasons they were too inconvenient to obtain. Even in the early days of the Computer Age, information searching remained inconvenient. Records existed only on large, expensive mainframe computers, and they could be accessed only from a terminal in the same building. It still was necessary to visit the repository or to order records and wait for them to arrive by mail. The long, broad tail of records that we all leave behind remained difficult and tedious to follow.[100] Now all the cumbersome processes have become a past with the advent of the Internet. Access to numerous databases is far easier than previously, and computer usage within the population at large is increased dramatically. The importance of "merely" quantitative differences cannot be underestimated just because they are differences of degree and not differences of kind. The Internet has posed threat to privacy simply by increasing the ease and thus the frequency of access to otherwise private information, even when such information was previously accessible, but accessed only rarely.

The Internet has also significantly changed the qualitative nature of information privacy by empowering people novel means of privacy invasion, which demands new responses independent of any quantitative differences. In the past, most of the personal information in birth records, education records, mortgage applications, land titles, legal cases, and many more were transient and scattered. Putting the scattered data bits together was an

---

[99] Joseph I. Rosenbaum, Privacy on the Internet: Whose Information Is It Anyway? 38 Jurimetrics Journal, 1998.

[100] Lane, supra note 72, p. 44-45.

arduous and complicated process. Perhaps only the most resourceful governmental bureaucracies are capable of overcoming the cost and difficulty of the data-gathering task. This is the traditional image of "Big Brother": the government's misuse of its surveillance power over individuals. However, two information technologies – computer matching and computer profiling – enable agencies to identify, target and perhaps manipulate a certain segment of the population that has common background characteristics.[101] As the world becomes increasingly networked and our daily movements start to leave more electronic footprints, the more serious privacy threats arise in the private sector, as well as the loss of our power of information self-determination.

The Internet is even changing our very conception of privacy. Since the reasonableness of an expectation of privacy depends on existing social practices, we are witnessing what Paul Schwartz characterizes as "the silent ability of technology to erode our expectations of privacy".[102] The widespread use of computers to collect, combine, and manipulate personal information may have already redefined the standards of "reasonable expectation". "Privacy interests lose without a struggle because technology comes without any inherent privacy restrictions. Once the use and the manipulation of data have become commonplace and profitable, opponents are hard pressed to argue successfully that those activities are unreasonable. Perhaps the best argument will be that consumers are unaware of the capabilities of technology and therefore have no contrary expectations."[103] Again, the issue of control over information about us is a growing problem, exacerbated by the Internet and technology. To the extent that the Internet environment pervades the lives and the experiences of more and more people, it will be

---

[101] Computer matching is the comparison of different computer tapes to expose instances of fraud, waste and abuse. Computer profiling is the derivation of classes of individuals most likely to engage in activities of interest to the agency in question. See Colin Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (Ithaca: Cornell University Press, 1999), p.19.

[102] Paul Schwartz, Privacy and Participation: Personal Information and Public Sector Regulation in the United States, Iowa Law Review 80, 1995.

[103] Robert Gellman, Does Privacy Law Work? In Agre, supra note 98, p.211.

harder to treat the privacy understandings within the Internet as limited to that medium. Rather, the increasing pervasiveness of the Internet may inform the society's general understandings of database privacy, both within and without the Internet. The implication may be that we should pay less attention to social understandings in developing our conceptions of legally protected privacy. The notion of the "reasonable" may become, or perhaps should become, more heavily normative, such that changing understandings of privacy may be less important than they are now. Perhaps the conception of what information people ought to be allowed to protect should be more important than a more social and empirical conception of what information people in fact expect to be protected.[104]

With all these conceptual changes in privacy in the Internet Age, the public's view of public records has changed as well. In the pre-Internet Age, legislatures casually designated government records as public with little concern about privacy. Although one could manually compile a personal profile by requesting FOIA documents, it would be a time-consuming and costly exercise, one that would not be undertaken unless the offsetting rewards were considerable. Privacy protections were inherent in the technology of paper, which made it difficult to exploit fully personal details. In sharp contrast, today, as more and more personal information appears online, such a profile can be built in a matter of minutes, at minimal cost.[105] Further more, greater ease of use made records more valuable to more people, and some states decided to exploit their records by selling the information to marketers and others. A U.S. Supreme Court case[106] held that federal

---

[104] Frederick Schauer, Internet Privacy and the Public-Private Distinction, 38 Jurimetrics Journal, 1998.

[105] Privacy Working Group, Information Policy Committee, Information Infrastructure Task Force, Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information, June 6, 1995, Introduction, at 1-2, available at http://www.iitf.nist.gov/ipc/ipc/ipcpubs/niiprivprin_final.html (visited June 23, 1999).

[106] Department of Justice v. Reporters Committee for Freedom of the Press (489 U.S. 749 (1989)). It is a Freedom of Information Act (FOIA) case involving the disclosure of criminal history records. Records of arrests and convictions are required by the U.S. Constitution to be made public. These records can usually be searched freely in police stations and courthouses throughout the country. The issue in the case was whether centralized compilations of this criminal history information (rap sheets) maintained by the FBI must be disclosed under the FOIA. The Court recognized the tradeoff between privacy and

agencies may withhold "rap sheets" – compilations of arrests, indictments, convictions or acquittals – on private citizens, even though the information is public at its original source. The court decided the threat of centralized and computerized records to privacy as following:

> "But the issue that we are now presented with is whether the compilation of otherwise hard-to-obtain information alters the privacy interest implicated by disclosure of that information. Plainly there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country, and a computerized summary located in a single clearinghouse of information."

### 2.2.3 Access and Aggregation: The Privatization of Public Records

On-line public records come from two sources: the public agencies and the private sector. The trend toward privatization of information dissemination has accelerated in recent years. Consequently, debates over the access right to on-line public records have transcended earlier emphasis on democratic participation, taking on a strong economic incentive in the Information Age.

Records containing personal information are valuable; public and private sector publishers long have earned a return by selling such information. But the value in public records is only enhanced significantly after digitalization and wide use of the Internet: a virtual explosion of real-time, on-line information services has enabled fast, efficient and economical means of public records access for business and government.

As raw material, online public records provide an economical and efficient way to find information. Employers can improve productivity, combat claim falsification, deter fraud and reduce the potential for hiring negligence through detailed background checks. Private investigators save much time (as well as cost) by avoiding wait for a response to their public records request form already overburdened government bureaus and

---

availability, and it came down squarely on the side of privacy. By narrowly interpreting "public interest", the court held that those seeking personally identifiable information from government records must show an intent to use the information to examine the workings of the government.

agencies. Insurance companies and human resource managers also find online public records improve speed, efficiency and customer service quality significantly. A record provider concludes, "Public records access, with reasonable protections against those who would acquire data for personal use, is an indicator of a society better-served."[107]

Online public records are also gaining economic value as an asset *per se*. The raw content of information contained in public records is generally considered to be non-proprietary because it is owned by governmental entities which either created it or collected it under legal mandates, and FOI laws in many countries mandate that the request for FOIA records be charged at nominal rates. However, as virtually all information products have something added to the raw content, the same with online public records. For instance, on the Internet we see record and file boundaries, paragraph breaks, and computer readable tags that can be accessed from elsewhere. In addition, more sophisticated products have "pointers," which either point to other parts of the same document, as in a table of contents, index, or cross reference; or point to a different document, as in a conventional footnote reference, or a Hyper Text Markup Language (HTML) reference to another resource on the Internet in the World Wide Web. These are all the added values to the raw content of paper-based public records and are of proprietary nature – if the records are provided by a commercial entity, the added part is often protected by intellectual property law. The digital technologies make profiling and online publishing significantly less costly but more profiting than print publishing technologies,[108] thus bring the quick ascendance an independent business of information services.

---

[107] James Rudolph Rauh, One View: Access to Information is Essential, 56 Oregon State Bar Bulletin, 1996.

[108] With print publishing technologies, the publisher bundles most of these attributes of value and the consumer buys the entire bundle from that publisher. Digital computer technologies, particularly as they are implemented in distributed and open systems like the Internet, permit unbundling of the attributes of value so that one supplier may supply only raw content, and another may make available one or more other value-added attributes such as pointers that the user combines with the raw content on demand. Still other suppliers might make available billing and collection value or promotion value. This facilitation for unbundling the value-added elements in publishing drastically changes the economics of publishing. In fact, it has already contributed to a more competitive marketplace with lower barriers to

The enhanced economic value of information in the digitalized public records and easy access, combined with the indirect economic impact of FOIA, permit commercial users to exploit personal information in new ways. Private businesses have created a thriving trade out of consolidating public records into commercial databases; the collection and cross-referencing of public records has become an industry taking its stride in North America. Increasingly, private companies acquire personal information and combine it with other data from private sources, including credit card companies and credit reporting agencies, banks and insurance companies, airlines and travel agents, supermarkets and other retailers, telephone companies, and Internet service providers. Direct marketing businesses accumulate or purchase such information to target potential customers.

Still, the most prominent in this line of business are some individual reference services companies which offer Internet "look-up" services that allow the search of computerized public records combined with records from other sources. For example, Information America's KnowX, which is a comprehensive source of public record information, includes aircraft and watercraft ownership, death records, bankruptcy, lawsuit, lien, and judgment information regarding individuals.[109] Right-Data offers a number of investigative services for a fee via its Web site.[110] CDB Infotek is at present, the largest online public records database commercially available. The file contains approximately 2.5 billion records in more than 1,400 databases.[111]

---

entry. With Internet technology, a would-be publisher needs only the capital to establish a server that adds a particular type of value, and not the capacity to own the content and other types of value, or to provide a full range of subject matter. The Internet thus provides demand economies of scope. A good example of the attractiveness of Internet technology is the "Thomas" system established by the Library of Congress to make congressional materials available in full text. Thomas uses a World Wide Web technology on the Internet, was established in a matter of weeks, and is free, contrasted with the more limited service of the Government Printing Office which uses mostly dial up access, and was established over a period of several years. See H. Perritt, Jr. Sources of Rights to Access Public Information, 4 William and Mary Bill of Rights Journal, 1995.

[109] Available at http://www.knowx.com/ (visited Nov. 14, 1999)

[110] Available at http://rightdata.com (visited Nov. 14, 1999).

[111] Teresa Pritchard-Schoch, Public Records 1995, Database, Oct./Nov. 1995, at 42 (discussing various online public records search services). Also see *Sellers of Government Data Thrive*, N.Y. Times, Dec.

In Los Angeles, companies can buy electronic access to certain courthouse records, and then sell the information. Some local and state agencies are seeking legal direction as to whether electronic access to public information can be sold. "The use of information is a commodity," said Peter Carton, a direct marketer. "So it's not surprising the question will be, 'what limits will local governments put on that information?'" In California, DMV records are closed to the public. Now legislators are struggling with how and when to allow access electronically to information already in public files.[112]

Much of the information provided on the Internet without charge is directory-type information, not traditionally considered private (and in fact, usually recognized as essential for communication), and is therefore not objectionable to most people. However, some of the fee-based Internet sites, for instance, records of motor vehicles, raise substantial concerns.[113] In addition, even more detailed, and often more objectionable, personal information is available on commercial online services which are marketed to legal and business professionals, and journalists. The personal information available through these services varies depending on the database, but generally includes name, address, telephone number, birth date, as well as the names and birth dates of other people living at the same address. Some databases provide real estate records including data on neighboring properties, approximate household income, plane and boat

---

26, 1991, at D2 (reporting that one company "set up a Legal and Financial Services division where clients can have access to 125 million public records, including lists of people who are delinquent in paying their taxes"). See H. Perritt, Jr., supra note 108.

[112] Rusty Dornin, Debate rages over electronic access to public records, August 17, 1996, available at http://cnn.com/TECH/9608/17/public.privacy/index.html (visited Dec. 28, 1999).

[113] Access to public record information has posed threat to privacy after several media reports on the misuse of vehicle information. In one case, an antiabortion group obtained address information from the State Department of Motor Vehicles (DMV) by using the license plate of a car driven by a woman who entered a clinic where abortions were performed. In another instance, a California actress, Rebecca Shaeffer, was stalked and murdered by a man who obtained her home address from the DMV. Karen McGlone, Another View: Caution Required on Public Records, 56 *Oregon State Bar Bulletin*, 1996.

ownership, motor vehicle records, voter registration records, law suits, liens and judgments, criminal records, and credit information.[114]

### 2.2.4 Seeking New Balance in Online Public Records

Ease of access to personal information has changed the public's view of public records. Traditionally these records have not caused much privacy concern: protections were automatic because the paper records were hard to access and difficult to exploit fully personal details. The digitalization and connectedness of public records make previous protection evaporate. If all traditionally public records from government files end up on the Internet, these records alone will result in the widespread availability of detailed profiles of everyone. At the same time, we cannot deny that these invasive devices also provide a convenient service that we often want very much. Many people appreciate the convenience of credit cards, ATMs, catalogue shopping, and cellular phones. Even the scary-sounding "smart roads" and "smart cards" mat become an indispensable part of our life. Having these services and conveniences means that there will be a trade-off. "We will have all the conveniences offered by computers, but we can never again expect that our personal papers and communications can simply be locked away from prying eyes and ears."[115] Therefore, the transition to the Information Age calls for a reexamination of the proper balance between the competing values of personal privacy and the free flow of information in a democratic society.

Prescribed conditions would be helpful for the balancing test. Current confusion over the acceptable privacy protection in public records arises from natural rights-based theories, high-minded but not very realistic or practical, of the right to information privacy. According to the utilitarian scholar Bentham, if a man has a right to something, all it

---

[114] Board of Governors of the Federal Reserve System, Report to the Congress Concerning the Availability of Consumer Identifying Information and Financial Fraud app. C (presenting samples of personal information available online), available at http://www.bog.frb.fed.us/boarddocs/RptCongress/privacy.pdf (visited Dec. 28, 1999).

[115] Ellen Alderman and Caroline Kennedy, *The Right to Privacy* (New York: Alfred A. Knopf, 1995), p. 331-332.

could mean was that government would guarantee his use and enjoyment of it. Rights were legally guaranteed patterns of behavior.[116] Unless rights are specified and utilitarian, they are nothing but "theoretical nonsense" and "bawling on paper". To reach an utilitarian balance to the challenging conflict between freedom of information and privacy protection in online public records, two key issue require legislative specification: 1) What kinds of "personal information" implicate more privacy concerns in the digital environment that demand exemption from disclosure on the Internet? 2) In view of the diverse sources of online public records, should the degree of protection accorded to personal information depend on the data delivery mechanism rather than on the type of information at issue?

2.2.4.1 Zoning Personal Information in Public Records

A public record is a record maintained by law, regulation, or practice by or for a unit of government that contains information that can be linked to an identifiable individual.[117] In many democratic countries that have FOI legislations, public records are subject to mandatory disclosure.[118] Apart from the statutory exemptions of disclosure, much personal information contained in public records is accessible as long as it's not considered a "privacy matter".[119] However, as the Internet technology is changing

---

[116] Mary P. Mack, *Jeremy Bentham: An Odyssey of Ideas*, 1748 – 1792 (London: Heinemann, 1962), p. 190.

[117] Often referred to as "personal information". Personal information encompasses any information which identifies or concerns a specific individual. Laurence Tribe, American Constitutional Law, § 15-16 (2d ed. 1988).

[118] Section 4 (1) of the Freedom of Information and Protection of Privacy Act of British Columbia (RSBC 1996, Chapter 165) stipulates "A person who makes a request under section 5 has a right of access to any record in the custody or under the control of a public body, including a record containing personal information about the applicant."
The US federal FOIA provides access to all federal agency records (or portions of those records), except for those records that are protected from disclosure by nine exemptions and three exclusions (reasons for which an agency may withhold records from a requester).

[119] In the U.S., although information involving matters of personal privacy is exempted from disclosure, it only pertains to "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy" (The Freedom of Information Act, 5 U.S.C. 552 b

people's notion of privacy, some personal information outside of traditional privacy law realm may bring new privacy concern.

But what is "personal information"? In general terms, we might expect it to mean information relating to our family life, personal relationships and that which we consider private. Wacks has proposed a relatively restricted definition:

"Personal information" consists of those facts, communications, or opinions which relate to the individual and which it would be reasonable to expect him (or her) to regard as intimate or sensitive and therefore to want to withhold or at least to restrict their collection, use, or circulation."[120]

The definition in fact reveals no concrete examples of personal information; rather, it relates "personal information" with the two components (subjective and objective expectation) of privacy, implying that personal information is, by its nature, an object of privacy regulation. However, in our daily casual talk, "personal information" covers a broader range than that falling into the privacy protection. It is this blurry between legally-protected information and loosely-disclosed information that results in some of the regulatory controversies over online public records. For the purpose of delineating privacy policies, the following reference of "personal information" takes the latter, more general, sense.

Let's first examine some accessible personal information in a most common public record – driver's license file. California Department of Motor Vehicles (DMV) driver's license file contains such personal information as: name, birth date, home and mailing addresses, license number, physical description, Social Security number, failures to appear in court, failures to pay traffic fines license status (valid, revoked, suspended, expired, major traffic convictions for the past seven years, minor traffic convictions for

---

(6)), and many other personal information that identifies or concerns a specific person is not necessarily covered, nor could be expected to be judicially construed so.

[120] Wacks, p.26.

the past three years. The DMV also keeps files of vehicle registrations which include: the name of the person who owns the vehicle, residential and mailing addresses of the registered owner, vehicle year, make and body style, year the vehicle was bought by the current owner and previous owners' names and addresses going back three years, license plate number, vehicle identification number, name of the lien-holder if the loan for the vehicle has not yet been paid in full.[121] With such a long laundry list of information, it seems that given little restriction in the FOIA requiring procedure, a California resident would be left little to his own had anyone make a casual request on his DMV files. There are, however, several commercial databases providing online interactive access to motor vehicles in many states of the U.S.[122]

Other types of common "public records" include Motor Vehicle Registration & Titles, Land Titles, Property Tax Records, Voting Registration Records, Occupational Licenses, Court Records, Bankruptcy, Civil Actions, Divorces, Law Enforcement Records, Compiled Criminal History Records, Political Contributions, Securities and Exchange Commission Filings, hunting/fishing licenses, Boat, Aircraft, and Other Vehicle Titles, Postal Service Address Records. A more extensive list of personal information contained in these commonly available public records is constructed below (parentheses indicate one possible source):

- Name and address (drivers license)
- Home ownership (land title)
- Mortgage loan (land title)
- Value of home (property tax)
- Size, price, physical description of home (assessments)
- Social Security Number (drivers license)

---

[121] From Cradle to Grave: Government Records and Your Privacy, available at http://www.privacyrights.org/fs/fs11-pub.htm (visited Dec.18, 1999).

[122] An example is TML Information Services, Inc., available at http://www.tml.com/ (visited Jan 23, 2000).

- Height, weight, use of vision correction, selected medical diagnoses (drivers license)
- Sex and date of birth (drivers license, vital statistics)
- Occupational status (occupational and professional licensing)
- Make, model, and loan for automobile (motor vehicle registration)
- Political registration and voting frequency (voter registration)
- Political contributions (federal or state election reporting)
- Hobbies (hunting and fishing licenses)
- Boat and airplane ownership (licenses)[123]

The list reveals the current permissible range of third party access to personally identifiable information in public records without violation of legally sanctioned privacy rights in the U.S. As more and more centralized registries are created, there may well come a time when the very concept of "public records" is brought into question. While people have all willingly disclosed their names and addresses, ages, and social security numbers to obtain driver's licenses in the past, they may not be quite so willing to do so when such information is stored in databases linked with hundreds of other pieces of information about their personal lives. Instead, one may question whether it would have serious consequences for the privacy of individuals if unrestricted access is allowed to those records collected for specific public purposes and maintained by government agencies. The on-line access to a variety of public records allows comparison of massive amounts of personal information in an unlimited number of public and private settings using direct on-line linkages. Citizens will have difficulty discovering where personal information is stored, knowing who has access, and making sure that the information is correct.

It should be noted that "public" as they are, public records may contain personal information of different degrees of confidentiality that is not always necessary subject to mandatory disclosure to the public. In many jurisdictions, "public records" are defined on

a spectrum from broad to narrow for the purpose of mandatory disclosure. It is recognized that zoning some personal information that once was public as involving privacy concerns is necessary. Regulations to establish the parameters of access to personally identifiable information in government files are increasing.[123] So are the limits on access to personal data contained in government-managed files. For instance, Pennsylvania's Open Records Law exempts records "which if disclosed would operate to prejudice or impair a person's reputation or personal security." In one case, the state used this exemption to withhold addresses, telephone numbers and social security numbers in firearms applications. The court said it was "not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files." However, the applicant's name, race, reason for requesting the license and answers to background questions could be disclosed because that information does not implicate privacy concerns.[124] In another case, the Michigan Supreme Court found that providing a computer tape containing names and addresses of students at a public university "was a more serious invasion of privacy than disclosure in a directory form" because "computer information is readily accessible and easily manipulated", even though the same information would later be published in a public directory.[125]

Another illuminating case is the online property records in the City of Victoria, Canada. In 1996, the City made available property assessment information to the public via its home page, allowing the public to search the database by property owner's name and address. Further search would yield the location of the property, assessed values, actual values, legal description, current year tax levy and "other related information about the property". When complaints from citizens about privacy concerns arose, the City removed the names of the homeowners. Acknowledging that obvious benefits accrue to

---

[123] For instance, California requires security check before providing driver's license records. In Virginia and Maryland, access to driver's license records is confined to insurance agents or brokers only.

[124] Times Publishing Co., Inc. v. Michel

[125] Kastenbaum v. Michigan State University

society through the availability of public databases such as the Assessment Roll and Land Title Registry, the BC Information and Privacy Commissioner's Office still decided that digital format of public records pose a greater challenge to the privacy rights of citizens for it is vulnerable to misuse.[126]

One piece of personal information was especially zoned out for privacy protection – the names of property owners. Accepting that the Assessment Roll is crucial to identifying properties, especially in rural areas, where parcels of land are generally referred to by name, (i.e., Old McDonald's Farm) rather than street address, and that a Roll without names would make accurate identification of rural properties more difficult, the Commissioner's Office questions the rationality of making the names and addresses of all property owners in the entire province available to anyone who wishes to browse through it.[127] One of the fundamental principles under the BC Freedom of Information and Protection of Privacy Act was invoked: the right information needs to reach the right person at the right time for the right purpose. Therefore, access for the purpose of property comparison should be limited only to properties within the taxing jurisdictions in which property is held. Since the Assessment Roll is made available for public inspection to permit the comparison of one property assessment to another, to evaluate whether a property has been equitably assessed, and the names of the property owners are included in the databases primarily to confirm the identification of the property, the Office reasoned that the personal information of the property owner is necessary but secondary to the property information. The Assessment Roll should not, therefore, be searchable by the name of the property owner, but only by property identifiers. Implicit in

---

[126] "Digital technology fundamentally changes the nature of public records as the paper record decomposes and becomes discrete pieces of information that can be searched, manipulated and reconfigured in ways that may improve efficiencies but were never intended by the legislature." An investigation concerning the disclosure of personal information through public property registries, available at http://www.oipcbc.org/investigations/reports/invrpt11.html (visited Oct. 20, 1999).

[127] As the commissioner put it, "Property owners in Saanich would never need to access the name and address of a homeowner in Kelowna or in Smithers to determine whether their own property in Saanich had been equitably assessed. The question remains as to the availability of the entire Roll Our office believes the Assessment Act is far too broad in this respect." Id.

this decision is the subtle privacy protections: If the system were not searchable by name it could not be used, for example, to run the names of all women working at a particular transition home, the name of an arresting police officer, a high profile politician or a doctor who performs abortions to determine where they lived. However, if you were appealing your property assessment and wished to examine the value of a home five doors down, the ownership information would be available, but only if you knew the address of the property.

This case reveals a delicate balancing test by zoning critical personal information in comparison with the appropriate purpose of data use. It exemplifies one policy choice: Where inappropriate usage of the Assessment Roll cannot be controlled, it should be discouraged. Since information from the Assessment Roll is used for confirmation of property values in the conveyance of properties and in the mortgage and insurance businesses, such critical personal information as name of the owner in the property registries should be accessed by the public or businesses on a case-by-case basis. The public should only be able to search real property registries by the address of the property. In the case of bulk sales of property registry data, the name of the property owner should be suppressed. This would prevent the Assessment Roll from being used as a locational device and protect, to a certain extent, those vulnerable people who have an interest in suppressing information which would reveal their home address.

Although zoning sensitive or critical personal information for privacy concerns is always a contextual test, the above principles – using data in its original purpose and discourage indiscriminating bulk sale of personal information – will serve as a useful tool.

2.2.4.2 Regulate Information Delivery Mechanisms in Private Sector

It is a highly political topic nowadays for the commercial dissemination of public records online. Information business representatives argue for market entrance on the grounds of both democracy and fair competition. They claim a commercial publishing motive does not disqualify anyone from the right to obtain basic government information. Further, government should not be allowed to monopolize its dissemination since it risks

censorship. Both government and private entrepreneurship have a role to play in realizing the advantages of information technology with respect to public information, because "no one supplier can design modern information products to suit the needs of all users."[128] Relying on the public sector alone will result in a much slower pace of innovation due to inadequate resources, while competition is an effective spur to reduced prices.[129]

However, some believes making public records available online for commercial purposes is a distortion of the original purpose of public records laws. "Public records laws were developed to keep government accountable to the people; to give the public the opportunity to examine government; not to create commercial services. Whenever personal information is put on a computer network, someone has to decide if requests for access to it are legitimate. The current process for requesting public records also serves a gate-keeping function. One of the down sides of speedy information is that it becomes harder to police unauthorized disclosure and distribution."[130] There are many queries about the "look-up service" selling public records.[131] In terms of privacy concerns, the question arises as how to regulate the information delivery mechanisms in private sector, whose very existence has circumvented some traditional privacy restrictions on the access, disclosure and use of public records. Should the private sector's dealing with information obtained from public records be mandated to provide equivalent privacy

---

[128] See Perritt, *Federal Electronic Information Policy*, p.240 (explaining why government suppliers are inadequate as sole or primary sources for public information).

[129] Henry H. Perritt, Jr. and Christopher J. Lhulier, Information Access Rights Based on International Human Rights Law, 45 Buffalo Law Review 899, 1997.

[130] Karen McGlone, supra note 113.

[131] Such as whether a private-sector competitor could use the FOIA to acquire at nominal cost and in convenient form information to be sold at a profit in the private sector. SDC Development Corp. v. Mathews, 542 F.2d 1116 at 1117 (9th Cir. 1976).

In another case, the court found that the public disclosure provisions of the FOIA were directed toward information dealing with the decision-making procedures of the various governmental agencies, whereas the primary purpose of the NLM was to collect medical information, organize it, and make it available to the public. Further, the issue of government secrecy, the issue that gave birth to the FOIA, was not involved

protection as in the public sector? If so, what measures can be taken to reach this policy goal?

The most prominent problem in commercial databases is its potential violation of fair information practice principles, as David Flaherty points out:

> "The continued automation of traditionally 'public' records, such as vehicle registration data and drivers' licenses, and their multiple uses and linkages to other information systems poses significant challenges to the traditional privacy interests of individuals and necessitate new rules of the road. The main result is that a set of records intended for a particular purpose, such as land title records, may now be used for novel and unintended purposes without full public awareness of the impact of these practices on the rights and interests of individuals."[132]

In fact, it is the very promise of this secondary use of personal information contained in public records that contributes to the input for the "look-up services", for businesses, as they always are, profit seeking. We can see lots of examples of illegitimate use of DMV records for stalking, private investigating and other identifying purposes that is beyond the permissible scope of law.

One possible solution is to require the information provider to conform to the regulations on disclosure. For example, while a landlord is restricted to access to detainer records of a potential tenant, he may access the records from a commercial online public records provider, thus undermining the legislature's goal of protecting the information privacy of tenants. Legislative measures should be taken to require the same degree of gate-keeping obligations observed by commercial public records providers in disseminating certain information to certain customers. But how to ensure and supervise businesses' observance of law remains a big problem.

The other, more fundamental, choice might be checking the government rules of initial sources. The existence of many "look-up services" depends, in part, upon an initial

---

[132] David Flaherty, The Information Highway (submitted to Industry Canada), available at http://www.oipcbc.org/publications/other/Industry-Canada.html (visited Dec. 10, 1999).

violation of the fair information practice principles[133] by government agencies and others. Government needs to review rules controlling access (either in paper or online) to personal information contained in public records. In one case, privacy advocates bring questions to the electronic accessibility of court records in San Diego County of California.

Here the balancing test is taken between convenient public access interest and the privacy interest. What these opponents argue is the absence of a compelling need for electronic access to these court records.[134] Granted, it might be more convenient for the community to search the full electronic record in order to monitor the court system. However, they ask, are Californians prepared to accept this dilution their right to privacy in the interest of mere convenience? Since personal information contained in court records is various and highly sensitive, and it won't surprise most people that those unregulated and unaccountable vendors would readily use and misuse the various types of personal information in court records,[135] the opponents outweigh privacy over the mere interest of convenience in this type of public records. They do recommend, though, an alternative choice of balance, which would make only index information available in electronic form. It alternative furthers the interest in public access by making summary court information available in a more convenient electronic form. Index information may be easily inspected and specific records identified, which may then be retrieved on a case-

---

[133] The most important is: There must be a way for an individual to prevent personal information obtained for one purpose from being used for another purpose without his or her consent.

[134] Often court records contain information about individual citizens which may be of a highly sensitive nature, and which usually is provided on an involuntary basis. A wide variety of sensitive personal information is routinely set forth in court records, including personal financial information, family histories, medical and health information, and many other private facts. Court records often reveal facts about individuals other than the parties of record, and may include sensitive information concerning third parties who have been deposed or summoned for jury duty. See Comments In Opposition to the Court Technology Committee Draft Rule: Access to Electronic Records, available at http://www.privacyrights.org/AR/ucan.html (visited Nov. 13, 1999).

[135] For example, in the case of paper records, it is not economically feasible for a medical marketing firm to compile a list of all parties in personal injury actions that have suffered specific types of injury, or for a securities firm to purchase a list, compiled from probate records, of relatives with new discretionary income. Yet, once such records become available in electronic format, it becomes economically feasible and even highly profitable to create these types of lists. Id.

by-case basis. At the same time, the mass cultivation of personal information from court records is discouraged, thus providing some measure of protection for such sensitive data. This results in a better balance between these two competing interests.

Some further suggest establishing a set of rules governing the access to "look-up services" – that government agencies, social service agencies, and private companies should submit comments spelling out the purposes for which they access "look-up services". The establishment of:

- a limited set of "permissible purposes" for which information can be accessed;
- auditing and accountability mechanisms to control and monitor access to systems;
- limits on law enforcement access to these systems;
- an individual right to review and correct information in these systems; and,
- remedies, including a private right of action, and stiff penalties for violations of such rules would begin to address privacy concerns, especially if coupled with a focus on the initial sources of the data as mentioned above.[136]

## 2.3 PROPERTY RULE FOR CONSUMER INTERNET PRIVACY

Privacy concerns in cyberspace transactions lie in several levels. Since e-commerce is relatively a new phenomenon, the law governing the use of the Internet is obscure. In the United States, while some courts have applied federal laws safeguarding consumer privacy to commercial transactions in cyberspace, the protection of consumer privacy on-line is limited.[137] Although Canada has established a voluntary national model standard

---

[136] CDT FTC Testimony, supra note 123.

[137] For instance, although Congress amended the Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510-2710 (1982 Supp. IV 1986) to prevent Internet service providers from releasing personal information of their members to a government agency absent a legal request, the Act does not explicitly prohibit Internet service providers from distributing the members' private information to any individual or entity outside of government. Furthermore, the Act fails to provide adequate remedies for those whose privacy was violated in cyberspace. For instance, the Act does not include any immediate punishments or

for the collection and use of personal identifiable information by the private sector, [138] it takes a similar approach as the US to protect the personal identifiable information of its citizens through industry self-regulation.

The tort liability theory of common law also fails to rectify invasion to consumer privacy in digital networks. In the first place, the difficulty of defining privacy and its underlying principles has impeded forming cohesive information privacy rules.[139] The formulation developed by scholars and judges perceives privacy in two components: the right to be left alone[140] and the right to control information of oneself. But in cyberspace transactions, I can be "left alone" while my privacy is invaded, and I have no control of my information once it is leaked out to the information market after the first transaction. Even the principle of "reasonable expectation" has been foiled on the Internet: The US

---

deterrents for violators of consumer privacy on-line. In addition, the law fails to establish a mechanism by which private information illegally obtained over the Internet can be excluded from civil or criminal court proceedings. As a result, consumers who use the Internet are not guaranteed true and complete protection of their right to privacy in cyberspace. See Nancy Lazar, *Consumer On-line: Your Right to Privacy in Cyberspace*, 10 Loyola Consumer Law Review, 1998.
There are, however, some legislative movements pending in the Congress addressing consumer privacy concerns, like H.R. 3685: Communications Privacy and Consumer Empowerment Act (require the FCC to study the impact of new technology on privacy rights and take collective action, if necessary, to protect consumer privacy rights) and H.R. 98: Consumer Internet Privacy Protection Bill (introduced early in the 105th Congress requiring the written consent of Internet service subscribers before the service provider can disclose any personal information about the user to third parties). See Nicholas W. Allard and David A. Kass, *Law and Order in Cyberspace: Washington Report*, Hastings Communications and Entertainment Law Journal (COMM/ENT), Spring 1997.

[138] The Canadian Standards Association (CSA) Model Code for the Protection of Personal Information ("CSA Code" or "Code") establishes ten practice principles that must be adopted as a whole by those who wish to participate: (1) accountability; (2) identifying purposes; (3) consent; (4) limiting collection; (5) limiting use, disclosure and retention; (6) accuracy; (7) safeguards; (8) openness; (9) individual access; and (10) challenging compliance. Although the CSA Code is essentially a guideline for a self-regulatory regime, it has allowed Canada to establish a national standard for on-line privacy protection of personal identifiable information. See Jonathan P. Cody, *Protect Privacy over the Internet: Has The Time Come to Abandon Self-Regulation?* 48 Catholic University Law Review, 1999.

[139] British Columbia Privacy Commissioner David Flaherty made such a remark of privacy as "You know it when you lose it", which reminds one of Supreme Court Justice Potter Stwart's infamous attempt to define obscenity in a First Amendment case: "I know it when I see it." *Visions of Privacy: Policy Choices for the Digital Age*, ed. Colin J. Bennett and Rebecca Grant (University of Toronto Press, 1999), p.112

[140] Warren and Brandeis, *The Right to Privacy*, 4 Harvard Law Review, 1890. Olmstead v. United States, 277 U.S. 438, 572 (1928) (dissenting opinion).

court has continually held that individuals have no privacy in information divulged to the private sector, even though modern society leaves citizens no other option but to disclose to others where disclosure is a condition of participation in society.[141]

While the existing legal framework did not envision a world where the private sector would collect and use information at the level it does today, current undertakings from self-regulation is similarly disappointing. One of such self-regulation is seeking consent to use consumer information for secondary purposes such as direct marketing solicitations. However, the debate over the opt-in or opt-out mechanism often shows conflicting interests of two sides: should businesses be allowed to use personal information unless and until the individual affirmatively "opts-out" or should they be required to receive an individual's prior permission or "opt-in"? The essence of this debate is who should bear the burden of protecting consumer privacy on-line: industry or the consumer? At present, industries insist that the maximum protection should only be the "opt-out" scheme.

TRUSTe is yet another self-regulatory privacy initiative intended to popularize the "trustmark", a "trademark of privacy policy" designed to enhance and simplify disclosure of the information-handling policies of participating Web sites.[142] Although the TRUSTe is welcomed to be a viable option for the protection of Internet privacy, many attorneys are advising companies against posting privacy policies on their Web sites just to avoid

---

[141] See Janet Goldman, *Privacy and Individual Empowerment in the Interactive Age*, supra note 140, p.105. "(T)he Supreme Court accepts as a given the apparently lowered expectations of privacy resulting from new technology."
In one bizarre case, the Court suggests that hidden audio bugs are to be expected. "According to the Court, we all know, after all, that anyone we talk with might wear such a device; thus, there can be no reasonable expectation of privacy in such conversations." See Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 Iowa L Rev (1995) at 573-74, citing United States v White, 401 US 745, 753 (1971).

[142] The Information Technology Practice Group of Cooley Godward, LLP, *Privacy Limits on Collecting Personal Information via the Internet*, 15 No.6 Computer Lawyer, 1998.

potential allegations of deceptive information practices.[143] The problem of conflict of interests in self-regulation even becomes evidential when TRUSTe is faced with disciplining its own sponsors.[144]

Perhaps the fundamental problem with self-regulation is its lack of enforcement of well-intended policies. Without a systematic management, it is difficult, if not impossible, either to monitor effectively the collection of personal identifiable information, or to redress harms done when a company violates self-regulatory principles. If the company cannot be held accountable and the individual cannot seek a remedy when a breach of self-regulatory policies occur, the incentive for a company to adhere to policy diminishes. As observed by one commentator, the principle that is mentioned least in the industry-specific guidelines is an enforcement mechanism to punish those who deviate from industry guidelines.[145] People seem to agree that the industry is motivated to self-regulation because of the threat of pending legislation that may be more burdensome than self-regulatory efforts. Consequently, the level of industry efforts to self-regulate is directly proportional to the seriousness of (or the perceived seriousness of) the legislative threats.[146]

---

[143] A recent settlement of a complaint against one of the most popular Web sites on the Internet, GeoCities. The complaint accused the Web site of engaging in deceptive practices in connection with its collection and use of personal identifiable information from its on-line customers. As a result of this complaint, companies are being advised not to post privacy policies on their Web sites, thereby hindering the possibility that Internet users will be provided with notice as to the companies' information collection practices.

[144] TRUSTe decided not to pursue an audit of Microsoft's privacy practices following a complaint about the personal identifying number on Microsoft products. Microsoft is a corporate sponsor of TRUSTe and has contributed $100,000 to the TRUSTe program. TRUSTe's decision not to pursue Microsoft's information collection practices adds currency to the argument "that these seals don't deliver the real privacy protection that people want and deserve, and self-regulation is sham regulation."

[145] Jonathan P. Cody, *Protect Privacy over the Internet: Has The Time Come to Abandon Self-Regulation?* 48 Catholic University Law Review, 1999.

[146] William E. Bandon, III, Summary of Technological and Self-Regulatory Responses to Internet Privacy Concerns, NETLAW 97, American Conference Institute.

### 2.3.1 QUESTION OF RIGHT

A pragmatic approach to consumer Internet privacy is thus needed to redress the current institutional failure. But first we should settle the basic question as Branscomb forcefully asked in the title of her book – " Who Owns Information?"[147] Should people be entitled property rights in their own information?

To give a loose definition, personal information is any data about an individual that is identifiable to that individual. You might wonder why your name, address, income, credit history, shopping interests should be given particular property protection. – Because they have value in the marketplace and are traded routinely nowadays. Strangely though, neither legislatures nor individuals themselves recognize the commercial value of this asset. The ignorance perhaps stems from a democratic tradition in North America that took privacy issue only seriously in the public sphere. As one scholar noted, "From a belief that the government's collection and use of information about individuals' activities and communications was the only threat to individual privacy and that a solid wall separated the data held by the private and public sector; to the notion that the Internet would be used primarily for a narrow slice of activities and that private and public spaces were easily demarcated, these vestiges of a pre-Internet, pre-networked world, stress our existing privacy framework."[148] Nevertheless, as the relative ease and low cost of collecting personal identifiable information has made it a commodity in private sector, concerns for privacy start to shift from a civil- and political-rights issue motivated by polemic ideology to a consumer-rights issue underpinned by the principles of data protection and by the law of trading standards. Privacy has metamorphosed from an issue of societal power relationships to one of strictly defined legal rights.[149] More consensus

---

[147] Anne W. Branscomb, Who Owns Information?: From Privacy to Public Access, Basic Books, 1994.

[148] Oscar H. Gandy, Jr., Legitimate Business Interest No End in Sight? An Inquiry into the Status of Privacy in Cyberspace, 1996 University of Chicago Legal Forum F.77, p.117-118.

[149] See Simon G. Davies, Re-Engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity, in Technology and Privacy: The New Landscape, ed. Philip E. Agre and Mark Rotenberg (The MIT Press, 1997).

has been reached that personal information is the property of the individual to whom it relates. "Our names and addresses and personal transactions are valuable information. Unless we assert these rights, we will lose them. If such economic value, we should receive something of value in return of its use by others."[150]

Current presumption about the ownership of personal information is, however, at issue with such a consensus. In fact, the property right to personal information is given to the collector of that information, and not to the individual to whom the information infers. It is argued that personal information like name, address and credit has no value *per se*, and the gathering agencies, by collecting and compiling information on individuals from a variety of sources, create the value in personal information and should enjoy the ownership of such "added value". This is not much different from the claim of a thief who professes to own a stolen car which he refurbishes later. In the United States, "the right to privacy" has its focus on *ex post* damages, not *ex ante* prevention. In comparing with EU data protection regulations, an American law professor admitted, "America does not have the general presumption that data should be used only for the purpose for which they are collected. It is roughly accurate to say that Americans are more concerned with wrongful decisions and harmful effect that with the wrongful processing of information itself."[151]

We should note that commercial power is a determining influence on the current assignment of rights in the realm of personal information. Because of the nature of relationships between individuals and companies, there is likely to be a substantial informational asymmetry in terms of what one actor "knows" about the other.[152] Empirical evidence shows that it is much easier for companies to amass information about individuals than for individuals to find out how their information is used by numerous companies. The imbalance of power in controlling personal information in

---

[150] Branscomb, supra note 148.

[151] Peter P. Swire and Robert E. Litan, supra note 78, p. 178.

[152] Gandy, supra note 149, p.117-118.

cyberspace, consolidated by the frustration of privacy laws and fallacy of self-regulations, has rendered some scholars to question the basis of privacy rights. They believe entitling individuals of property rights to their own information will compensate to some extent the market imbalance between consumers and marketers. A property rule is thus introduced to protect consumer privacy in cyberspace transactions.

### 2.3.2 Property Rule as Market Solution

The allocation of right, however, is only the beginning of a complex interaction in which concerns for privacy collide with competing interests. It is a static view that granting property rights to individual consumers means the end of the story, since transactions of personal information are inevitable if efficient and safe business is to continue. Different parties have different preferences on "information permeability" and need a way to synchronize these preferences. Privacy is thus an issue of control over information flows, with a much greater inherent complexity than a conventional "consumer versus business" analysis suggests.[153] The proposed property rule not only requires determining a baseline assignment of rights in the first place, but also allows individuals to trade those rights if they desire so,[154] which means interactive negotiation over the use of personal information would have a place in establishing and protecting consumer privacy on the Internet.

---

[153] Eli M. Noam, Privacy and Self-regulation: Markets for Electronic Privacy, in Privacy and Self-regulation in the Information Age, U.S. Department of Commerce, 1997.

[154] See James Rule and Lawrence Hunter, Towards Property Rights in Personal Data, in Visions of Privacy, supra note 140. Also see Richard S. Murphy, Property Rights in Personal Information: An Economic Defense of Privacy, 84 The Georgetown Law Journal, 1996. Hal R. Varian, Economic Aspects of Personal Privacy, in Privacy and Self Regulation in the Information Age, US Department of Commerce, June 1997. Jerry Kang, Information Privacy in Cyberspace Transactions, 50 Stanford Law Review, 1998. Internet Regulation through Architectural Modification: The Property Rule Structure of Code Solutions, 112 Harvard Law Review, 1999.

2.3.2.1 The Default Rule

In practice, consumers and companies do not always have explicit privacy agreements before engaging in each transaction. Although privacy notices have become more frequent on Web pages, it is a stretch to say that there is a "meeting of the minds" on privacy terms each time an individual browses a Web page.[155] A default rule is thus necessary absent explicit agreement to govern personal data collected in a cyberspace transaction.

The law and economic literature considers economic efficiency when setting the default rule. According to Coase Theorem, if there are no transaction costs in trading or negotiation, the initial assignment of privacy rights is arbitrary from the view point of economic efficiency, i.e., the parties will allocate the right to the party who values it the most. Consequently, a default rule should be set to minimize the costs associated with contracting out of the rule, thereby lowering transactional costs since fewer parties are forced to contract around the rule. So the question left is to determine which party in cyberspace transactions values its interests in personal information more – the company seeking disclosure or the consumer seeking non-disclosure?

Suppose the default rule is disclosure, the consumer who has stronger privacy preferences will be simply unable to contract out of the rule, since the research costs to determine what information is being collected and how it is used tend to be high. The company, on the other hand, has no incentive to restrain its own right to disclose such information. An efficient use of information will be resulted as the consumer who values privacy more than the company values the information is unable to acquire the rights to that information.

Conversely, in a non-disclosure default rule, if the company which values trading personal information more than the consumer values keeping it intact, the company could relatively easily realize its aim by placing a simple dialog box on the Web (the privacy

[155] Jerry Kang, Cyberspace Privacy: A Primer and Proposal, 26 Human Rights, Winter 1999.

contract) asking whether the consumer will allow some secondary use of personal data, in exchange for some benefit. The cost of contracting out of the rule is low since the company has no need to research its own information practices, and the cost of soliciting rights to the information will be cheap.

Therefore, from the consideration of economic efficiency, the default rule for transactional personal data in cyberspace should be non-disclosure: No personal information should be legally traded from data banks of commercial entities for any commercial purposes, without express permission from the person with whom the information is concerned.

2.3.2.2 Mechanisms Implementing the Property Rule

A royalty system has been proposed to implement the property rule for consumer privacy in cyberspace transactions.[156] The initiative creates a property right over the commercial exploitation of personal information, which defines the conditions for secondary use of personal information for any commercial purpose and requires the express consent of the data subject for any disclosure of personal data. With this right, individuals are able to collect royalties, through profit-driven information intermediaries, on the sale or exchange of his personal data. These information intermediaries, or data rights agencies, seeking to enroll clients on the promise of collecting royalties for the commercial use of their data and on the expectation of collecting an agreed commission, would find it in their own interests to monitor all sorts of unauthorized release of personal data and thus become entrenched force of privacy protection.

Although some privacy experts showed moral dislike for the notion that one should be allowed to sell one's privacy to the highest bidder, they don't deny that such a royalty system would have particular application in fields like direct marketing and credit reporting where personal information is used for free, and it would work as a supplement

[156] James Rule and Lawrence Hunter, Supra note 155.

to ensuring enforceable legal rights in both the public and private sectors.[157] After all, the present reality is that personal information is being freely used, without any remuneration to the individuals involved. A system of royalty payment will benefit all consumers whose personal information is used commercially. In addition, the allocation of property rights to personal information to the party whom the information concerns, rather than to the collector of the information, gives consumers grounds to insist on requirements pertinent to the fair information principles. It seems to be a viable market mechanism to fulfill the intent of privacy legislation and standards.

With the development of technology, data management and monitoring, the proposal can even be realized. A company in Cambridge, Massachusetts offers an on-line service that provides precise data about consumers' choices and pays royalties to consumers for the commercial use of their information. Although this system differs somewhat from the model proposed above, it is nonetheless a system where the personal preferences that consumers display towards a particular product or service actually bring in some cash.[158]

The Platform for Privacy Preferences (P3P), a technical standard for negotiating privacy practices while browsing on the World Wide Web, is another mechanism where the property rule is implemented through a combination of market and technological approaches.[159] P3P is designed to allow Web sites to express their privacy practices – including which data they collect from users, what they use the data for, and whether that data will be shared with other parties – in a machine-readable format that can be automatically parsed by Web browsers and compared with privacy preferences input by the user. If there is a match between Web site practices and user preferences, a P3P agreement is reached. Users are able to configure their browsers to reach agreement with, and proceed seamlessly through, Web sites that have certain types of practices; users are also able to receive browser prompts when encountering Web sites that engage in

---

[157] David H. Flaherty, Visions of Privacy: Past, Present, and Future, supra note 71, at p.54-55.

[158] Cavoukian, supra note 75, p.93.

[159] See <http://www.w3.org/privacy> for background information on the P3P project.

potentially objectionable procedures. For example, a user might request to be prompted when a Web site proposes to collect information that will be used for marketing purposes. Thus, users need not read the privacy policies at every site they visit to be assured that their information is going to be used only in ways they consider acceptable.[160]

By enabling the Internet user to control over the release and use of his personal information and to exchange part of personal information for payment or for access to a particular Internet site or service, the P3P standard offers a property rule protection for the privacy entitlement through the use of privacy enhancing technologies. Although the costs of negotiating privacy agreements in real-space may be prohibitively high, low communication costs and automated negotiations with "software agents" minimize transaction costs in cyberspace and enable privacy agreements to be reached efficiently. P3P permits Internet users to value privacy according to their personal preferences with this market feature of low transaction costs, thus resulting in, some scholars believe, the optimal level of privacy protection through a contractual implementation of the property rule.[161]

2.3.2.3 Normative Implications of the Property Rule

A property rule based on law and economic literature for consumer privacy in cyberspace transactions is not, of course, without skeptical examinations. Opponents often question it from a consideration of distributional justice, and the efficacy of the mechanisms that the property rule entails is also under scrutiny.

The social justice attack is directed at the part of the property rule that regards privacy as an alienable possession, presuming the value of privacy as a marketable commodity. One writer made a fair criticize that "to operationally define and institutionalize the

---

[160] Lorrie Faith Cranor, Internet Privacy: A Public Concern, available at http://www.research.att.com/~lorrie/pubs/networker-privacy.html (visited Nov. 23, 1999).

[161] Internet Regulation through Architectural Modification: The Property Rule Structures of Code Solutions, 112 Harvard Law Review, 1999.

commercial property aspects of the privacy interest show very little promise for reversing the trend toward the collapse of our reasonable expectations for privacy."[162] This insight is shed into three angles:

First, the theory that considers privacy interests as economic goods disregards the underlying moral and social value of privacy as a basic human right. A law professor rebutted, "We do not buy and sell civil liberties. This is commodity fetishism. It is capitalism run amok." Many believe that well-established rights as privacy rights cannot be peddled to the highest bidder. But at the same time some of them are hesitated to protest this pragmatic solution categorically since privacy is not well defined or protected in current legal system. Instead, they call for a safety net – a minimal level of personal information privacy that cannot be bartered away, such as privacy of children, the inalienable control over people's most sensitive material, medical and financial information for examples. The privacy market will require a concrete legal regime to protect what's being traded and the integrity of that trading. Besides, such a market can't supersede statutory protections for privacy.[163]

Second, the fundamental asymmetry between individual consumers and companies causes the market failure for fair trading of personal information, since the market's inefficiency "is systematically beneficial to the merchant"[164] and consumers cannot correctly assess the market value of giving up personal information. The problem of unequal bargaining power in information-related transactions is manifest: powerful companies tend to be monopolistic, presenting consumers with little real choice in the

---

[162] Gandy, supra note 149, p.127. Further he goes on, while the creation of a market in personal information might help establish some justification for informed consent for the use of personal information, it would not address the quite substantial problems of inequality that would distort such a market.
In Privacy in Cyberspace: Constructing a Model of Privacy for the Electronic Communication Environment, Katrin Schatz Byford also suggests that we should structure privacy protections so as to preserve privacy's personal and social value, rather than creating privacy rights by resorting to the fiction of ownership in personal data.

[163] Andrew L. Shapiro, Privacy for Sale: Peddling Data on the Internet, 26 Human Rights, Winter 1999.

[164] Bailey Kuklin, The Asymmetrical Conditions of Legal Responsibility in the Marketplace, 44 University of Miami Law Review, p.1004.

market. If you don't like the terms of the deal they offer, there's really nowhere else you can go to establish a reputable credit report that will allow you to obtain, say, a checking account or a mortgage.[165]

Third, the property rule renders privacy protection dependent upon individual wealth and disproportionally burdens the poor. As companies are able to charge increasingly higher rates for finer shades of privacy, poorer customers who can't afford these premiums will be left more exposed simply by dint of economic disadvantage. For those with little disposable income, the right to privacy is just a luxury that can be easily sacrificed for little if not neglectable financial gain solicited by companies. Do we really want to perpetuate such a system of first- and second-class privacy rights?

In terms of efficacy, people look into the societal goal of P3P that incorporates privacy policies in software technologies. It is hard for the technology to handle the negotiation process – How can such a technical device arrange communication that is not technical? The issue being negotiated is rather essential to individual consumers: the electronic release of personal data – names, addresses, bank accounts, credit card numbers, and other, often intimate, details. Therefore, a certain degree of transparency in its operation is required to ensure that users do not object to the activities of the software agent.

The problem for developers, however, is getting P3P-enabled software to set up comprehensible vocabularies for on-line privacy negotiation in the first place. But as the system is complicated for the general public to understand and fashion to their needs. Unsophisticated users don't seem to appreciate such warnings as "Your IP address may be used", or "This data is going to be used for survey purposes." That's why for some, the answer is to ease P3P in over several generations. Keep first versions simple, and once

---

[165] Shaprio, supra note 164.

users become more familiar with its powers, introduce more sophisticated negotiating abilities.[166]

While accepting the fairness and force of the above queries, it should be recognized that such a rule extending property rights to personal information is subject to many qualifications, both in terms of function and scope.

First, the focus of the property rule on privacy is confined to the mechanisms of transactions in the private sector, ignoring other aspects of privacy as a basic human right. Today, technology has escalated the collection of detailed personal information and enabled massive data sharing between companies for unrelated purposes – all without data subjects' consent, and privacy protection frequently takes the form of multiple-paged disclaimer waving any claim to privacy which the individual Internet user must agree prior to receive a service or benefit. It's fair to say that the use of technology to meet information needs of business has disempowered individual consumers. A property rule is then meant as a legal tool to add more bargaining power to individual consumers over the transaction of their personal information. As Noam noticed, whether we like it or not, people continuously trade in rights in return for some other benefits, as a person reconsider his freedom of religion to make his spouse's parents happy, or a student waive his right to read faculty letters of recommendation written in his behalf for greater credibility. When an informed, lucid, sober, and solvent citizen makes a choice freely, the objections are much harder to make.[167] The reality is that personal information is a marketable commodity in the information age, and through offers and counteroffers between individual and information collector, the market will move the correctly priced personal data to the party that values it most. Even to the argument that marketing privacy for sale burdens the poor disproportionately, a defense of economic efficiency can still be raised – the same poverty condition may also make a poor person an

---

[166] Chris Oakes, The Trouble with P3P, Wired News, June 25, 1998, available at http://www.wired.com/news/news/technology/story/13242.html (visited Nov. 2, 1999).

[167] Noam, supra note 154.

unattractive target for a commercial intrusion, which is especially true in direct marketing areas. It is in fact a matter of decision making – who should make the decision of the commercial use of personal information, government or citizens? Shouldn't the poor reserve the discretion over profiting from their own property? To insert well-intended government policy against privacy trading cannot help the poor financially; even worse, it will lead to inefficient use of personal information by business without any incentive to self-regulation. The property rule will, in contrast, change the default rule of disclosure in current privacy legal structure into a non-disclosure one, and put more incentives to business to restrain from misuse of personal information.

Cautions should be taken here, however, that the market approach does not reach the public sector, since "distribution of privacy rights on a free-market basis would provide no protection for citizens against the encroachment by the state."[168] The property rule, as a market solution to the current free commercial exploitation of personal information, does not exclude other available mechanisms as technological empowerment or liability rules imposed by law. Legislation should continue to protect those basic human rights aspect of privacy which are not negotiable between citizens and government, and restrictions on the use of personal information should continue to apply to government organization. So there should be two types of privacy rules: one for transactions among private parties, the other for transactions between private parties and the state. More importantly, the property rule generally does not constrain the collection and compilation of personal data, since such data has been divulged by individual consumers voluntarily as an exchange for services and products. What the property rule restricts is the secondary use of data, i.e., the unauthorized disclosure or release of personal data by data collectors after the initial transaction. Furthermore, the property rule is not absolute, just as the right to privacy is never absolute in the context of various competing interests. There are several situations under which individuals should waive their property rights to privacy, which is an empirical matter for legislative deliberation.

---

[168] Id.

To be sure, a property rule for consumer Internet privacy is by no means a panacea to every invasion of privacy in cyberspace transactions, but it's focus on current institutional failure to address the issue cannot be ignored. Because the United States has such a unique privacy culture unlike that of the Europe, which favors self-regulation instead of centralized and systematic regulations on data flow, and which seems to have a less adverse reaction to "automated individual decisions",[169] the property rule advocated by many economists and jurists is perhaps a compromise between the reluctance of government intervention and consumer outcry for privacy protection.

## 2.4 TOWARD A HOLISTIC REGULATORY SOLUTION TO INFORMATION PRACTICE

While concern about privacy in the online public records runs high, the prescriptions for treatment vary widely. Much of the current debate about online privacy focuses on the **tools** of regulation, rather than the **goals** for which regulation is sought. But essentially, a holistic solution to online information privacy depends on a balanced goal before formulating policy proposals.

For instance, in the U.S., the main privacy concern serves the good of business in order for the Internet to achieve its full potential. Policy aims to ensure that privacy fears – well founded or otherwise – do not impede the continued growth on online commerce.

In the "balancing" test of privacy against the American tradition of free transfer of information, the First Amendment, and the legitimate needs of business, representatives of the Internet industry and politicians play a dominant role. As a result, regulations of privacy focus on scandalous and controversial forms of privacy abuse that might impact public trust in the Internet or prompt legislative overreaction. Identity theft and child stalking would be at the top of the list, regardless of their actual prevalence in the society. One would expect to see little or no protection of neutral biographical data (other than

[169] Peter P. Swire and Robert E. Litan, supra note 78, at 178.

that useful for committing identity theft) or information related to consumer preferences and lifestyle, regardless of whether that information might have commercial value.[170] Protection seems to focus on those visible and reassuring areas. The most visible portion of the personal information spectrum is the nexus where information is gathered from or provided to the individual consumers. One would expect to see few or no restrictions imposed on the use of data outside public view.[171] Secondary use of personal information, therefore, is rarely regulated, and that opens great chance to information vendors. In short, as Branscomb puts it, "in its entrepreneurial spirit, the American public, as well as its venture capitalists, see the burgeoning world market for online databases as a natural magnet for Americans to maintain and expand their competitive edge."[172]

As a contrast, the European countries in general attach greater value to information privacy when formulating their policies. They seek to protect individuals and society from the effects of loss of privacy, including the loss of human dignity. Despite the pressure posed by technology and commercial markets in information, the 1995 EU Directive on Data Protection[173] features a relatively holistic perspective. Legislators realize the generally weak bargaining position of the individual when exercising his or her rights and try to equalize such relationship by strengthening the individual's power vis-à-vis the usually more powerful information gathering agencies.

---

[170] See Swire, Markets, Self-Regulation and Government Enforcement in the Protection of Personal Information, in Privacy and Self-Regulation in the Information Age, supra note 154, p.83. ("Privacy laws are likely to be significantly less important for bolstering consumer confidence if the security risk, and the accompanying risk of direct financial loss, is understood to be small").

[171] Karl D. Belgum, Who Leads at Half-Time?: Three Conflicting Visions of Internet Privacy Policy, 6 Richmond Journal of Law and Technology, 1999.

[172] Anne Wells Branscomb, Lesson from the Past: Legal and Medical Database, 35 Jurimetrics Journal, 1995.

[173] Council Directive of 24 July 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data. [hereinafter the Directive]

While the EU Directive does not specifically address the issue of freedom of information – it's main concern is the processing of information – it does try to balance competing interests of privacy and freedom of information by empowering Data subjects certain limited rights as well as imposing on Data controllers obligations in their conduct of Data processing.

The Directive limit its application to "personal Data",[174] and it does not apply "to the processing of personal data . . . by a natural person in the course of a purely personal or household activity."[175] Since "the expression 'purely personal or household activity' must not make it possible to exclude from the scope of the Directive the processing of personal data by a natural person, where such data are disclosed not to one or more persons but to an indeterminate number of persons."[176] Article 3(1) further provides, "This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a file or are intended to form part of a filing system. Limiting the Directive to filing systems of personal data and not applying it to files generally that contain personal data would reduce the burdens that the Directive imposes on freedom of information. This limitation means that the Directive would regulate only organized activities of data processing directed to particular individuals; organized activities that only incidentally affect individuals would remain unregulated. However, assuming that the Directive is to apply to "filing systems" and not to "files" generally, technological developments may overtake that limitation. If a database is searchable by an individual's name, one might argue that it is a filing system where there is easy access to personal data.

While Article 8(1) requires that Member States prohibit processing of certain special categories of data, such as those containing racial or ethnic information, political or

---

[174] Article 2(a) defines personal Data to mean "any information relating to an identified or identifiable natural person (Data subject)". Council Directive of 24 July 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data.

[175] Article 3(2)

[176] Common Position, Statements for Entry in the Minutes, 4730/95 (quoting Article 3 (2) of the Directive)

religious beliefs, and so on, the following Article 8(2)(e) permits processing when "the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defense of legal claims." In this way the Directive takes a generally applicable rule and suspends or limits its operation and, thus, intentionally or unintentionally promotes the interest of freedom of information.[177]

The EU Directive provides a more holistic solution to the conflict of information privacy and freedom of information interests than in the U.S. The reason may lie in the different goals in their policy formulation: the U.S. is more market oriented where the interests of privacy is more than often compromised; EU places more restrictions on the organized processing of personal data while making efforts not to hinder individual citizen's right to know. The key issue in the balancing test, though, is to prevent the improper use of public records rather than restrict access to this information. Compared with random searching made by curious individuals, organized private entities poses more threats to information privacy by providing online "look-up" services as well as other advanced information technologies. Such practices further assist the improper or unfair use of personal information contained in public records by interested parties, be it stalking, private investigation, or tenant-screening. Since it is difficult to design legal mechanisms either to categorily restrict releasing certain kinds of information or to ban the commercial use of public records as a whole, a more realistic solution can only focus on the way personal information is used in public-inspectable realm. Unavoidably this involves context-specific analysis to decide in which context it is improper to make decisions based on certain information contained in public records. Factors as efficiency, convenience, freedom of information, compellingness of online access and so forth must be considered in comparison with the privacy interest – and those other interests which will be enhanced by the protection of privacy. Professor Kreimer writes: "Constitutional values can be threatened by both disclosure and secrecy. Either choice may be a sacrifice

---

[177] James R. Maxeiner, Freedom of Information and the EU Data Protection Directive, 48 Federal Communication Law Journal, 1995.

of constitutional magnitude, and that decision cannot be made in the abstract. The crucial question is the degree of sacrifice in the particular context."[178]

Privacy may not deemed by some as severe or harmful as a physical attack, since the privacy-invaded person experiences no obvious loss or injury. But knowledge about a person is raw power which may be used to cause harm. The wounds, though not immediate, might result over time in a reduced ability to get jobs or loans, or other harm to that person's spiritual or emotional well-being. More and more agree that privacy is a necessary element of quality life in modern society. Some protection for identifiable personal information about individuals and institutions is an essential part of privacy. As information technologies spread and reliance on them increases, as the amount of personal information accrues in various records, and as the cost of processing those data declines, the perceived need to protect information privacy is growing.

There seems no doubt that in the future we shall experience more information – the issue is whether this can be both open and protected. In the "good society", public life should be open and private life should be private, but the fear with new technology is that we could end up with greater public secrecy and less personal privacy.[179] Currently, one important threat to controlling personal information comes from the "look-up services", who compile and sell customer profiles created not only from information solicited directly from the consumer, but also from data contained in public records and the data banks of third parties. So far no effort is made to incorporate market profiler practices into the proposed privacy protection model.[180] What public policy framework should control third party access to "personally identifiable information" contained in government files remains a tough question. But this has to be solved because its significance in the healthy development of both industry and human integrity in the

---

[178] See generally, Seth F. Kreimer, Sunlight, Secrets, and Scarlet Letters: The Tension Between Privacy and Disclosure in Constitutional Law, 140 U. Pa. L. Rev. 1, 77 (1991).

[179] Rowe, Christopher, 1942. People and Chips: The Human Implications of Information Technology. 3rd ed. London; New York: McGraw Hill. 1996, p.192.

[180] CDT FTC Testimony, supra note 123.

Information Age. In many situations it's not so much the release of data and the use to which it is put that upsets people. Unfortunately, it is extremely difficult to control what happens to data once it hits the street. Therefore, protecting privacy must start with an effort to restrict access to the kinds of personal data that simply should not be made public in the first place. Coming to some consensus on what should be included in the category is an important public policy priority.

In this pursuit of information privacy right, we need to develop a combined perspectives of both utilitarian and Foucaulian. As lawyers, we should be concerned about the operative feature of privacy as a legal right to make it meaningful in legislations; as social scientists, we shouldn't ignore those parallel social forces beyond law – technology, behavior pattern, private power, norms – and their implications and influences on the notion of rights, on the protection of rights, and on the evolution of rights.

# CHAPTER III CONTESTED COPYRIGHT IN CYBERSPACE

## 3.1 CHANGING POINT OF BALANCE

Copyright law strikes a precarious balance. On the one hand, it accords a bundle of proprietary rights to right owners to encourage creation and dissemination of original expression. On the other hand, it sets exceptions and limitations to copyright owner's exclusive rights to promote public education and creative exchange in the society. "Copyright law's perennial dilemma is to determine where exclusive rights should end and unrestrained public access should begin."[181]

Copyright law is said to disappear in cyberspace.[182] Traditionally, right owners succeeded in controlling the distribution of content by controlling the physical medium on which the content was delivered. Piracy was less attractive by the technological constraint that made inferior copies to the original. The use of digital technology has modified both production patterns and consumer habits. Digitization makes it possible to store any tangible subject matter in a binary format. Since strings of zeroes and ones can be reproduced with absolute fidelity, the cost of copying is greatly reduced compared with the Analogue world. Mostly notably, mass adoption of personal computers with DC-ROM drives, coupled with the Internet connection, has terrified the content industry –

[181] Neil Weinstock Netanel, Copyright and Democratic Civil Society, 106 Yale Law Journal 283, 1996.

[182] See generally, John Perry Barlow, Selling Wine Without Bottles: The Economy of Mind on the Global Net. Margaret Jane Radin, Property Evolving in Cyberspace, 52 Stan. L. Rev. 1125. See also, Eric Schlachter, The Intellectual Property Renaissance in Cyberspace: Why Copyright Law Could Be Unimportant on the Internet, available at http://cyber.law.harvard.edu/metaschool/fisher/ISP/cache2.html (visited March 11, 2004). The unique ways that the Internet poses threats to the enforcement of copyright are identified as: no loss of quality in reproduction, no meaningful marginal costs of reproduction or distribution, users' ability to act anonymously, and lack of copyright sense of users in both "real" space and cyberspace. Schlachter, id.

music and movies, making consumption of "free" content a widespread reality.[183] There is a significant growing of copying digital media for personal use and for sharing with friends. Use of online file-sharing is fairly well established for some consumers. The publicity of the Napster litigation and the peer-to-peer (P2P) technology is just one example showing how the business models and consumer practice in transition have contributed to breaking the equilibrium of the traditional copyright system.

Information users also change their traditional passive consumption model to a more active one. Due to the decentralized architecture of the Internet, anyone who possesses a computer that is linked to the Internet owns a part of the network, and anyone with access to the Internet can send data across the network. Not only can they easily reproduce works with a few clicks of a mouse and communicate them to every corner of the world connected with the Internet, but they can also manipulate data to create entirely new works without degrading the quality of the original data. The lack of central control in turn has certain implications for the legal system. Low reproduction costs means that small companies, even individuals, can make a perfect copy of the protected work without easy detection by the right owner. While copyright was traditionally enforced directly against the infringers, the same strategy is not effective to deter piracy on the Internet, because copying is widespread and direct threats of copyright infringement are not generally felt so imminent as in the real world. From the point of right owners, the difference between real world and cyberspace lies in the scale: the scale of private copying, and the scale of distribution of pirated materials over the Net. Consequently,

---

[183] By mid-2002, copying CDs was a relatively common act for one-third of online adults and nearly 40% of the online teens, by a survey of Internet users queried by GartnerG2. The survey revealed a relatively high level of ownership of digital technologies, for instance: 95% of Internet users reported owning a standalone CD player, 56% owning a PC with a CD burner. At the root of this high level of ownership is the continual enhancement of the PC platforms at ever-decreasing prices. In 1997 a mid-range PC with 3.2GB hard drive storage and a CD-ROM sold about $1,100-$1,400, while in 2006 a mid-range PC with 180GB hard drive storage and a DVD-CD-RW combo drive will cost only about $1489. Gartner Dataquest, April 2003. This price-performance progression is fixed in the consumers' mind and has arguably given rise to an important set of expectations: that with a mid-range PC and an Internet connection, virtually any type of digital content is available. GartnerG2 and The Berkman Center for Internet & Society at Harvard Law School, Copyright and Digital Media in a Post-Napster World, p.16.

even private copying activities are now deemed commercially relevant to the interests of right-holders as constituting competing activities. If unauthorized and widespread, such user activity could radically undermine traditional copyright markets. Some even remarks that "byte makes right in cyberspace".

Given the technological challenge, one might conclude that the balance favors users (or consumers) rather than authors (or copyright owners) in this control battle. However, the same technology also greatly enhances copyright owner's control of their works. Technologically, access control systems (Electronic Copyright Management System (ECMS)) function as a privatized alternative to law that can monitor and control the copies that are made on the Net. Digital technology provides copyright owners with the technical means to restrict access to, and uses of, digitized works to a far greater extent than is possible in the Analogue world.[184] For example, copy protection technology can be used to fence works that either would not be eligible for copyright at all or would enjoy only quasi-copyright protection.[185]

Legal measures are in addition more frequently sought to strengthen the private ordering and to protect against third parties circumventing such ECMS. Although contractual relations between authors and publishers and between authors and collective societies have long exited, there is no direct relation between the producer and the end-user of copyrighted material. However, when distribution of works becomes simpler in the

---

[184] Copyright management information (CMI) comprises all information that identifies a copyrighted work, information that identifies anyone who has a particular kind of involvement or interest in the work and any other information that would enable or facilitate the management of rights, such as conditions of use. The importance of CMI lies in the role it can play with regard to the on-line trade in content and the administration of rights, i.e. to enable or at least facilitate the creation and exploitation of multimedia works. See Protection of Copyright Management Information, Institute for Information Law, Amsterdam, Dec. 1998. http://www.imprimatur.alcs.co.uk/legal.htm (visited March 24, 2000).

[185] The most important example is databases – a "white-page" telephone directories; compilations of primary legal materials; etc. See Deborah Tussey, Owning the Law: Intellectual Property Rights in Primary Law, 9 Fordham Intell. Prop. Media & Ent. L.J. 173 (1998).

digital networked environment, more direct and complex contractual relationships between information producers, intermediaries and end users arise as a consequence.[186]

Through the use of click-wrap, or shrink-wrap, licenses, authors are increasingly demanding that purchasers, or licensees, waive rights that copyright law gave them. Copyright law is gradually being displaced, if not by byte then by the private power of counter-trickery systems and the private law of contract. A tendency worth nothing, albeit not new to the digital divide age, is that at the focus of the Internet copyright debate is the transition of protection of individual creation to industrial production. Some scholars have aptly observed that copyright in the wired digital world protects a system of production rather than the individual author. "It is copyright in its industrial capacity that is the second dimension of the law."

The rise of "code" modifying copyright law (promised as ECMS becomes more common) and the rise of contracts modifying copyright law (due in part to the falling costs of contracting) raise unprecedented questions. In real world, as copyright is in essence a statutory device, the control over the use of copyright work could only be achieved through the law, not private right-holder. Since copyright's internal limitations are deliberately prescribed to preserve a space for personal uses and discursive exchange, the replacement of "code" and contract could make copyright and its set of statutory limitations largely redundant, and may require an entire new body of information law to safeguard the public domain. Right-holders view their private ordering of copyright in the digital environment positively, deeming it promises more efficient resource allocation that gives them the capacity to channel their investments more precisely to meet newly articulated patterns of demand. End-users contend on the other hand, that the "free use zone" of the hard copy world must be maintained in the digital networked environment. Controversies arise over whether the traditional limitations to the exclusive exercise of

[186] See Lucie Guibault, The Exceptions and Limitations to Copyright: Limitations Found outside of Copyright Law, www.eblida.org/ecup/exceptions/excep.htm (visited 9 Feb 2000).

copyrights should apply to the digital environment; to which extent "private ordering" is tolerated and when is to be regulated.

Anti-circumvention legislations and recent case law also bring hot debates over the degree of legal protection afforded to ECMS. If the current access control battle tilts in favor of the right holders, why should the law add an extra layer of protection – and contributes to the privatizing "a large chunk of the public law of copyright"? Put in a broader perspective, information policy purporting to alter the open architecture of the Internet and limit access to some of its most valuable content – that protected by technological protection measures and contracts, backed up with legal penalties for "circumventing" – would invariably render the medium useless. Although new norms should by no means deprive just compensation for creators, public interests also abhor deprivation of access to public domain by unfettered control of copyright owners. The "balance of interests" analysis, presently throughout in all legal systems, shifts to a more nuanced aspect – what "center of gravity" is to be given to the interests of the various stakeholders as to the copyrighted content? The author is of the view that any "balance of interests" analysis should not only be sensitive to the interplay between changed market condition and consumer expectation and practices, but also with a technology-friendly mentality toward future development. When the facility of digital communications makes information access and distribution cost almost nothing, a "goods"-based concept of information production in the analogue world may encounter serious question on its underlying presumptions. Strengthening property right concept in cyberspace as cornerstone of the copyright policy may have unintended negative impact on the information market in the long run.

Since the scope of copyright limitations is indicative of these balances, this chapter will explore the way traditional limitations are applied to the increasing private ordering of copyright in the digital environment. Three aspects of online copyright issues will be examined: (1) copyright limitations as applied to the ECMS; (2) increased reliance on secondary liability for indirect copyright enforcement, and the legal prospect of the decentralized peer-to-peer file sharing architecture; and (3) private copying in the grey

area of fair use. The last two issues will be examined particularly in connection with the Napster litigation. The focal inquiry is: If any change of limitations is to be taken in respect of the technological change and market transformation, what will be the optimal choice? Starting with a historical review and comparison of copyright limitations recognized in two predominant copyright regimes (the Anglo-American copyright regime and the European continental *droit d'auteur* regime), it finds that recent legislating policies and relevant cases of the United States and the European Union shares common thread: despite the ideological dichotomy between the copyright and *doit d'auteur* regimes and varying preference in regulating the information market, there is a surprising common understanding among western liberal states on the limitations of copyright in the increasingly privatized cyberspace. In a highly hailed effort to "harmonize" copyright and related rights in the increasingly inter-connected information society, proposed legislation aimed at validating the private "fencing" rights has been crafted, without much concern of balancing the social costs of legal incentives to innovate against the benefits of free competition. Policing priority is given to the protection of copyright holders on the false assumption that their interests are severely weakened by the digital technology – just because they have more money to cry louder.

## 3.2 COPYRIGHT LIMITATIONS IN THE COPYRIGHT AND *DOIT D'AUTEUR* REGIMES

The Anglo-American copyright regime and the European continental *droit d'auteur* regime are well known as opposites. One is based on the utilitarian principles that pursue public interest objectives, while the other is based on natural law principles that focus on the author's personality rights.[187] The ideological divergence results in different fixation

[187] Leval states that the objectives of the American copyright regime is not an inevitable, divine, or natural right that confers on authors the absolute ownership of their creations. "It is designed rather to stimulate activity and progress in the arts for the intellectual enrichment of the public. This utilitarian goal is achieved by permitting authors to reap the rewards of their creative efforts". See P. N. Leval, Commentaries – Toward A Fair Use Standard, 103 Harvard Law Review 1105-1161, 1990.
Such utilitarian considerations play only secondary role in continental droit d'auteur regime, where copyright is seen as a positive right of ownership by the author in the fruits of his intellectual work. French authors like Desbois and Françon draw their findings from the text of the Déclaration des droits

of the scope of rights conferred to authors, and correspondingly, the extent of limitations imposed on right-holder's rights under the two regimes. This being said, there have been common understandings of certain categories of copyright limitations. Countries from *droit d'auteur* tradition have adopted measures more akin to public interest considerations, such as the protection of computer programs, and countries from the copyright tradition have recognized concepts, such as moral rights. The ongoing international harmonization of copyright law also helps to reduce the gap between different systems. In this respect, both regimes admit certain limitations to right-holder's exclusive rights, although such limitations vary in nature and scope from one country to the next. These limitations can be categorized into two types: those found within the scope of copyright law and those found outside of copyright law.

### 3.2.1 Limitations Found in Copyright Law

Copyright law limits right-holder's exclusive rights through many mechanisms, most notably the idea/expression distinction, the duration of copyright and related rights, first sale doctrine and the statutory limitations (like fair use, or fair dealing defense in common law countries). Generally, there are two major grounds underlying the limitations to copyright: public interest and market failure.

Among the limitations based on public interest considerations, some are meant to preserve the public's fundamental rights such as freedom of expression and privacy. Both the copyright regime and the *droit d'auteur* regime accept that copyrights should not be used to hinder the public's freedom of speech or freedom of information, nor to violate an individual's fundamental right to privacy, nor should they constitute an obstacle to a large dissemination of information. Many national and international instruments enact

---

de l'homme et du citoyen de 1793, and believe that the droit d'auteur system does not aim primarily at promoting creative activity for the public good, but rather at rewarding authors for their intellectual work. The public interest was not invoked as a ground for granting protection, nor was it suggested that authors needed rights as an incentive to creativity. See Contract and Copyright Exemptions, Institute for Information Law, Amsterdam, Dec. 1998, available at http://www.imprimatur.alcs.co.uk/legal.htm (visited March 24 2000).

measures designed to safeguard the public's freedom of information and freedom of speech, thus allowing for the personal reproduction of works for purposes of research, study, criticism, news reporting and even parody.[188]

However, due to the utilitarian approach and legal realism in the copyright regime, courts do not usually accept the argument of freedom of expression as a separate defense in copyright infringement proceedings. While the argument for free speech is sometimes invoked in defense of parody or other unauthorized use of copyrighted works, some courts find that this speech freedom is not "a freedom to use someone else's property to do so"[189]. In the United States, there's also concern that "maintaining the First Amendment privilege within the fair use doctrine leaves the impression that the interests found in the *Bill of Rights* can be balanced away every time the price to copyright holders is too high'.[190] Consequently, although courts may accept the argument for freedom of expression and right to information, their utilitarian approach to copyright infringement cases makes this limitation a marginal defense.

More frequently invoked limitations, however, are based on the objectives to promote other less crucial public interests such as education, research, or learning. Limitations based on these public interest considerations have long been an integral part of the copyright system, since the copyright system as a whole is believed to establish a balance between the interests of the creators and those of the public to further the common good. Legislatures enact provisions designed to relax copyright rules for particular categories of users, like educational institutions, libraries, archives and museums. Such limitations plays a more important role in the Anglo-American copyright system, where they are

---

[188] In the United States, parody has been admitted as fair use in Campbell v. Acuff-Rose, 114 S. Ct. 1164 (1994).

[189] Compagnie Générale des Établissements Michelin- Michelin & Cie v. National Automobile, Aerospace, Transportation and General Workers Union of Canada et al., [1997] 2 F.C. No. T-825-94 available at: http://www.fja-cmf.gc.ca/en/cf/1997/vol2/html/1997fca19917.p.en.html.

[190] Fraser, S., 'The Conflict Between the First Amendment and Copyright Law and Its Impact on the Internet', 1998 vol. 16:1 Cardozo Arts & Entertainment Law Journal 1-52, p. 51.

addressed mainly within the "fair use" (or "fair dealing") defense, and constitute a rule of judicial interpretation, especially in contractual matters. The traditional common law principle recognizes that certain terms of a contract may be unenforceable because they are invalid under a fundamental public policy that clearly overrides the fundamental policies supporting freedom of contract.[191] This is exemplified by the proposed provision of Article 2B UCC concerning the free expression and competition policy issues regarding information. It is stipulated that a contract term that violates a fundamental public policy is unenforceable to the extent that the term is invalid under that policy[192]. Such a provision has impact on the interpretation of standard contractual terms of use of copyright material, such as the license of software or other information. Public interest is also invoked as a basis for the adoption of other forms of copyright limitations, which in fact result primarily from the strong lobby exercised by the stakeholders. For example, the *U.S. Copyright Act* stipulates copyright exemptions where performances of musical works by a "nonprofit agricultural or horticultural organization, in the course of an annual agricultural or horticultural fair or exhibition".[193]

The limitations based on market failure considerations is said to alleviate the "public good" problem in the production and exploitation information. Information is a "public good" in the sense that its creator cannot efficiently exclude its use. Information is also non-rivalrous in the sense that once a work is created, it can be used by one user without detracting from the use of the same information by others.[194] Because technological developments make it impossible or at least very difficult for copyright owners to control effectively the use made of their works and to collect royalties for all authorized uses, such as home-taping and broadcasting, copyright law gives right-holders the right to remuneration: once a work is commercially released on the market, the rights owner

[191] Restatement (Second) of Contracts, § 178.

[192] Article 2B UCC, sect. 2B-105(b).

[193] US Copyright Act, Title 17 U.S.C. § 110 (6).

[194] Niva Elkin-Koren, Copyright Policy and the Limits of Freedom of Contract.

looses the possibility to prohibit its communication to the public but is entitled to monetary compensation.[195] A broader view of market failure includes private ordering of copyright through contracts, where the right-holders adjust their respective contractual terms to one prevalent term so that that particular term becomes dominant in all licensing contracts, to the extent that it effectively forms private legislation. Limitations based on such market failure considerations curb the exercise of a copyright owner's exclusive rights where it is thought neither practical nor socially desirable that authors fully exercise their rights over their work. The market failure consideration provides an economic analysis of copyright limitations, especially in the US system of copyright law. It is generally accepted that the extent and limitations of copyright law are based on economic efficiency and public interest functions.[196] Under the European *droit d'auteur* regimes this is not as clearly established, but, even though principles of natural law appear as their main foundation, economic efficiency and public interest considerations play a large role in the analyses of copyright matters under these regimes as well.

The problem with the market failure consideration in determining copyright limitations is that it will be hard to establish when it has actually disappeared, since the development of technology makes the conditions of market in constant change, sometimes to a workable condition. For instance, with the help of ECMS copyright owners are now able to collect fees for uses that used to be exempted because of market failure in the Analogue world. Would the creation of such payment mechanism within an ECMS eliminate any fair use pretension in cases where public interest is not at stake? The much-debated *ProCD* case in the United States raises this issue, where the court granted the validity of the

---

[195] US Copyright Act, Title 17 U.S.C. § 115.

[196] The US Supreme Court delineated this idea in Twentieth Century Music Corp. v. Aiken, 422 US 151, 156, 45 L. Ed. 2d 84, 95 S. Ct. 2040 (1975):
"The limited scope of the copyright holder's statutory monopoly, like the limited copyright duration required by the Constitution, reflects a balance of competing claims upon the public interest: creative work is to be encouraged and rewarded, but private motivation must ultimately serve the cause of promoting broad public availability of literature, music, and the other arts. The immediate effect of our copyright law is to secure a fair return for an "author's" creative labor. But the ultimate aim is, by this incentive, to stimulate artistic creativity for the general public good."

shrinkwrap license: fair use defense is not admissible since it is possible to comply with the terms in the shrinkwrap license. We can conclude that the elimination of market failure may make copyright limitations in this respect obsolete. Among the limitations of this category, the most commonly invoked are those relating to the limited right of lawful owners to reproduce computer programs. Under the *EC Directive on the legal protection of computer programs*[197], lawful owners of a copy of a computer program have the right to make, in the absence of specific contractual provisions, a permanent or temporary reproduction of the program as well as to make a translation, adaptation, arrangement or any other alteration. This is believed to be based on the market failure considerations because the right to a back-up copy may not be prevented by contract insofar as it is necessary for that use.

### 3.2.2 Limitations Found outside of Copyright Law

In both US and European nations there also exist legal rules beyond the scope of copyright law that pose limitations on copyright owner's exclusive rights. While originating from diverse sectors of the law (constitutional law, civil law, consumer protection law and competition law) and not designed primarily to deal with copyright matters, these restrictions nevertheless constitute additional safety net for users against rights holders who misuse their copyrights to the detriment of the public interest. Most important among defenses based on such grounds are violation of competition or antitrust law, abuse of rights and consumer protection.

The limitation based on competition or anti-trust law is more frequently applied in the United States, as administrations and courts have long been influenced by the Chicago School's neo-classical view about the economic impact of intellectual property rights on the competition process. It is generally not a defense to a copyright infringement claim in the United States that the rights owner is violating the U.S. federal antitrust laws. However, in recent years courts have granted approval for a number of antitrust lawsuits

[197] Council Directive of 14 May 1991 on the legal protection of computer programs (91/250/EEC), O.J.E.C. no. L 122, 17/05/91, p. 42, art. 5.

brought by the government on the grounds that a copyright holder has abused his monopoly grant through anti-competitive practices. One example is the case against Microsoft's abuse of dominant position by tying sales of 'other products' to its market-dominant PC operating system Windows 95.[198]

In the European Union the relation between competition law and the exercise of intellectual property rights involves an additional aspect besides competition policy, i.e. the free movement of goods within the Internal Market. Monopoly in certain copyright licensing practices is not only subject to certain Treaty rules, such as the rules on the free movement of goods and services (Article 36), and competition (Articles 85 and 86), but also to the general principle of non-discrimination as laid down in Article 6 of the EC Treaty, and have been challenged before national courts and the European Court of Justice. Competition law has proven to be an effective instrument in curing abusive behavior by dominant copyright owners, as in the *Magill*[199] decision delivered by the European Court of Justice. The key issue in this case was whether, and to what extent, an owner of copyright in advance listings of forthcoming television and radio programs can rely on his exclusive right to exclude potential competitors from the derivative market of TV guides without constituting an abuse of dominant position in the sense of Article 86 EC Treaty. The European Court of Justice held that by refusing to license a third party to publish the advance TV and radio listings, the applicants were abusing a dominant position contrary to Article 86 of the EC Treaty. A compulsory license was ordered as a remedy for the abuse.[200] Competition law considerations are also at the heart of the adoption of the restrictions to the rights granted under the *EC Directive on the legal*

---

[198] United States of America v. Microsoft Corporation, 56 F.3d 1448 (DC Cir. 1995).

[199] Radio Telefis Eireann v. E.C. Commission (Magill TV Guide Limited intervening), Decision of the Court of First Instance of the European Communities, July 10, 1991, Case No. T 69/89 reproduced in IIC 1993/24, p. 83, confirmed by RTE and ITP v. Commission, Judgement of the Court, 6 April 1995, joint cases C-241/91 and C-242/91.

[200] Lucie Guibault, The Exceptions and Limitations to Copyright: Limitations Found outside of Copyright Law. ALAI Study Days General Report, available at www.eblida.org/ecup/exceptions/excep.htm.

*protection of computer programs*[201], pertaining to computer system interoperability. It is specifically stated that these provisions are without prejudice to the application of the competition rules under Articles 85 and 86 of the EC Treaty, if a dominant supplier refuses to make information available which is necessary for interoperability as defined in the Directive.

The civil law concept of abuse of right raised in the *Magill* Case provides yet another source of limitation to copyright owners' exclusive rights. Abuse of right (*détournement de pouvoir*) is often invoked in civil liability cases as the intentional misuse of a right by its owner which results in a prejudice to others, thereby giving rise to damages. In copyright infringement defenses, such a limitation is often raised to limit a copyright owner's deliberate abuse of his rights to the detriment of users. For example, under French civil law, abnormal use of a right consists in the deviation from its intended use, either with the intent to cause prejudice, out of carelessness, without legitimate interest, or by diverting the right from its social function. The abuse of right has been included in the French *Code de la propriété intellectuelle* which deal with the "notorious" abuse in the exercise of rights, either economic or moral, by the representatives of a deceased author[202].

While there is no legal concept similar to the civil law notion of abuse of right in common law countries, in the United States defendants sometimes may raise the right-holder's own misuse of his rights as a defense in copyright infringement proceedings. Such a defense in the US courts is more closely related to antitrust law than to tort law. But unlike antitrust law proceedings, a defendant who invokes a copyright misuse defense does not have to prove that the market is adversely affected by the copyright owner's actions. Anti-competitive language inside a licensing agreement may amount to misuse of copyright if the licensing agreement attempts to use copyright to control

[201] Council Directive of 14 May 1991 on the legal protection of computer programs (91/250/EEC), O.J.E.C. no. L 122, 17/05/91, p. 42, art. 5 and 6.

[202] Code de la propriété intellectuelle, art. L. 121-3 (moral right) and art. L. 122-9 (economic right).

competition outside the scope of the monopoly grant. Misuse of a license bars recovery for infringement even if the misuse does not amount to an antitrust violation[203].

The third type of copyright limitation is found in consumer protection rules. With the ascendance of private ordering of copyright works in the digital environment, the relationship between copyright owners and end-users are becoming more like that of merchants and consumers in the market of commercialized information. It is recognized that today's production and distribution of copyright works are indeed far from the romantic view of authorship[204] or of the traditional philosophy behind the *droit d'auteur* regime, where exclusive rights are granted to physical authors of literary and artistic works as an extension of their personality and as a reward for their effort. Certain licensing practices, and particularly those unfair terms included in mass-market license do affect consumer's rights and need to be regulated under consumer protection law. Already in Europe some consumer lobby groups are advocating for the preservation of a digital private copying exemption on the grounds of fair trade practices and consumer rights[205]. The *Directive 97/7/EC of 20 May 1997 on the protection of consumers in respect of distance contracts* pursues this objective by protecting consumers obtaining information in the environment of "E-Commerce".[206] It decides to introduce at the Community level a minimum set of common rules to protect consumers in respect of distance selling,

---

[203] Lasercomb America, Inc. v. Reynolds, 911 F.2d 970 (4th Cir. 1990); and DSC Communications Corp. v. DGI Technologies, Inc., 81 F.3d 597 (5th Cir. 1996).

[204] See Mark A. Lemley, Intellectual Property and Shrinkwrap Licenses, 68 Southern California Law Review 1239-1294, 1995.

[205] See: 'The Consumer Fair Practice Campaign warns that Information Poverty could result from the new EU Copyright proposals', Press Release from the European Fair Practices in Copyright Campaign, 29 June 1998.

[206] Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts, O.J.E.C. June 4, 1997, Nr. L 144/19.

> "Whereas information disseminated by certain electronic technologies is often ephemeral in nature insofar as it is not received on a permanent medium; whereas the consumer must therefore receive written notice in good time of the information necessary for proper performance of the contract."[207]

In the United States the proposed Article 2B of UCC would apply to the licensing to consumers[208] of any form of copyright material, given the Article's broad definition of "information", which includes "data, text, images, sounds, mask works, or works of authorship". Although Article 2B deals with general contract law and commercial law principles instead of promulgating a consumer protection code, it nevertheless contains a provision granting consumers a right of refund in cases of contracts in certain applicable circumstances.[209] Further, a section was introduced in the draft to confirm the prevalence of State consumer protection rules over contractual provisions to the contrary, considering the implications of mass-market software licensing for the consumers and in view of the strong lobby exercised by consumer organizations.

In summary, both the copyright and *droit d'auteur* systems admit restrictions to the exercise of exclusive rights, either on the basis of public interest or of market failure. A number of copyright limitations based on public interest considerations pursue fundamental objectives of safeguarding user's constitutional rights and freedoms. Besides the rules of copyright law, several other limitations may be invoked to circumscribe the rights of authors and owners in favor of users of copyrighted material. These limitations

---

[207] Art.13.

[208] Article 2B UCC, sect. 2B-102, where "consumer" is defined as follows: "an individual who is a licensee of information or informational rights that are intended by the individual at the time of contracting to be used primarily for personal, family, or household purposes. The term does not include an individual who is a licensee primarily for profit-making, professional, or commercial purposes, including agriculture, business management, and investment management other than management of the individual's personal or family investments."

[209] For a contract concluded between a distributor and an end-user, the end-user has a right to refund if the his right to use the information or informational rights is subject to a license from the publisher and there was no opportunity to review the license before the end-user became obligated to pay the distributor. See Article 2B UCC, sect. 2B-617.

are also founded on a notion of public order or public interest, where it is believed that the exercise of a person's right should not prejudice that of others.[210]

## 3.3 ELECTRONIC COPYRIGHT MANAGEMENT SYSTEMS (ECMS)

Mentalities change with the development of technology, so do manufacturing patterns and consuming habits. The new balance of copyright law being sought in the digital networked environment combines the functions of law and code. Copyright owners, the modern day "romantic author", now presents itself as a major computer software enterprise or a powerful publisher and "builds their own fences"[211] by the use of technology as "code" in the online market.

Generally referred to as "Electronic Copyright Management Systems (ECMS), the content protection technology lets a content provider to "wrap" a set of rules around the content, and to define how control can be manipulated and shared by the purchase of the copyrighted content. ECMS come in many shapes and can be distinguished in different ways.[212] Information technologies may fulfill various functions: the *conditional access systems* control access at the online outlet; anti-copying devices prevent the unauthorised reproduction and/or further use of certain information products; *Digital Object Identifier* (DOI) [213] plays a similar role as the ISBN to identify copyright protected works and trace the copyright owners; metering or tracking measures can further facilitate the trade in copyrights or copyrighted works in cyberspace. At the heart of all ECMS technology is a

---

[210] Contract and Copyright Exemptions, Institute for Information Law, Amsterdam, supra note 188.

[211] E. Mackaay, 'The Economics of Emergent Property Rights on the Internet', in: P. Bernt Hugenholtz (ed.), The Future of Copyright in a Digital Environment (The Hague: Kluwer Law International, 1996), p. 20.

[212] Smith classifies technological measures into two broad categories. The first contains measures that prevent interception of a work by unauthorized recipients, and the second contains measures that limit the use and/or further distribution of works. See N A Smith, "United States of America", in M Dellebeke (ed), Copyright in Cyberspace, ALAI Study Days Amsterdam, 4-8 June 1996, Amsterdam: Cramwinckel, 1997, p.425.

[213] See http://www.doi.org.

rights model. Set in the rules of ECMS software, such rights model defines the right of a user to content in consideration for the user's payment of money, registration or agreement to the content provider's privacy policy, for instance. Typically, encryption of content is involved. To get the decryption key a user must satisfy the conditions by the content owner. Thus, with the help of encryption technology, right holders are able to condition access to and use of the protected content, thus maintaining complete control over every interaction between the user and the content.[214]

Such ECMS measures would be useless if circumvention of the conditions were possible and users were even allowed to make the protected content available on the Internet without control. As a result, ECMS has been subject to legal protection by legislatures on both national and international levels. Anti-circumvention law backs up the code so that certain circumventing act is prohibited with the threat of legal sanction, which in turn, reinforces the private ordering by content providers.

It is to these entities and their licensing practices that the individual user is now confronted when he wants to "consume" copyright protected works on the Internet.[215] Private ordering featured by the combination of ECMS and contract poses a major challenge to the existing body of limitations to copyright owners' exclusive rights. How nations apply the copyright limitations to such private ordering practices? Should the current set of limitations be automatically transposed into the digital networked environment, or should there be any differentiation to determine which limitation is relevant in the information highway?

---

[214] Mark Stefik, Shifting the Possible: How Trusted Systems and Digital Property Rights Challenges Us to Rethink Digital Publishing, available at http://www.law.berkeley.edu/journal/btlj/articles/vol12/Stefik/html (visited Nov.11, 2003).

[215] Lucie Guibault, The Exceptions and Limitations to Copyright: Limitations Found outside of Copyright Law. ALAI Study Days General Report, available at www.eblida.org/ecup/exceptions/excep.htm (visited March 12, 2000).

### 3.3.1 Copyright Limitations to Contractual Arrangements

One major concern over the ECMS rights model is the contractual arrangement, most often substantiating in the click-wrap licenses: if content provider's power to condition access and use of the content is left unbundled, a significant portion of the copyright limitations will be "bargained" away. The structure of the Internet facilitates the establishment of a multitude of contractual relationships between information producers and end users, either directly or through intermediaries, and creates challenges to the equilibrium of copyright law. While in the analogue world regulation over copyright contracts was focused on protecting the weaker party to the negotiations – the author, in the digital environment the interests of users of copyright material have become prominent, since copyright owners have greater power to unduly extend their rights through mass market licenses.

Under both the copyright regime and the *droit d'auteur* regime, the freedom of contract is subject to the bounds of public order. A contract whose object is prohibited by law or contrary to public order is null and invalid. However, norms of public order take many faces and vary from one country to another. Except for the widely accepted notions on the protection of fundamental rights and on the safeguard of the freedom of competition, public interest matters are mostly a question of national policy: what is in the public interest in one country, is not necessarily in the public interest in another.[216] The question then becomes to what extent copyright limitations and exceptions based on public interests considerations may or may not be overridden by contract. Does an information producer have the right to contractually subject a user to restrictions that go further than copyright law prescribes? May, e.g., the license prevent the user from copying the work for private purposes, to quote from the work or to make copies for educational or scientific purposes?

---

[216] Lucie Guibault, Pre-emption Issues in the Digital Environment: Can Copyright Limitation be Overridden by Contractual Arrangements under European Law?, available at http://www.ivir.nl/Publicaties/guibault/ARTICLE2.doc (visited April 11, 2000).

In the United States this is directly linked to the constitutional doctrine of pre-emption. Since copyright is a federal law and contract law is state law and because federal law is supreme when the two bodies of law conflict, there is much consensus among scholars that copyright law should not be overridden by contracts that try to undermine the statutory limitations such as fair use, first sale and some other user exemptions. While freedom to contract is an important legal principle, it is not absolute. "Allowing parties to enter into contracts is not synonymous with granting them a license to enforce all of the terms of such contracts, no matter how onerous or how much at odds with public policy they may be."[217] In the European Union pre-emption issues have rarely been examined since copyright rules are not subject to constitutional pre-emption in any of the Member States. Nevertheless, as I will examine below, regulation of contractual arrangements in copyright matters is not unusual.

Whether in the US or EU there is consensus that distinction should be made between negotiated licenses and for mass-market licenses. Freedom of contract is the rule, and stricter requirement based on public interest considerations is placed on less "free" – non-negotiated standard contract.[218] What differs is that in the United States, the software industry has long developed a practice of licensing products with prohibitions to decompile or reverse engineer, and the question of overridability of user freedoms has drawn scant attention. Consequently it is uncertain whether restrictions on the use of a computer program in an explicitly negotiated license should be overridden by copyright limitations. This question has been definitely settled in Europe by the adoption of the *EC Directive on the legal protection of computer programs*, which explicitly invalidates that

[217] Maureen A. O'Rourke, Copyright Preemption After the ProCD Case: A Market-Based Approach, 12 Berkeley Tech. L. J. 53 (1997).

[218] According to O'Rourke, parties to a negotiated agreement are usually informed parties, who understand the nature of the rights they are granting and obtaining, respectively, including the rights that the licensee agrees to forego. Neither party would enter the agreement if it did not think it were receiving something worthwhile in exchange. Unless some overriding policy justification can be asserted, there is no persuasive reason to preempt particular provisions of these deals. However, the situation may be different in the case of non-negotiated license agreements, often presented on a "take-it-or-leave-it" basis. Legitimate concerns arise when one party to a transaction is uninformed, thereby rendering the transaction itself both inefficient and unfair.

any contractual agreement preventing a lawful user from decompiling the program for private purposes.

In the case of non-negotiated mass-market license, it is more likely for courts to override restrictions that run afoul with statutory copyright rules. Besides limitations found in copyright law, both the US and EU nations have developed rules found in competition law and consumer protection law. What's at issue is to find an optimal mechanism: whether the fine tuning with regard to mass-market licenses should take place within consumer law or whether it should take place within copyright. In Europe, the enforcement of intellectual property rights is considered to have a possible affect both on competition and on the free movement of goods within the Internal Market. Legislating initiatives are based on the need to "combine [our] efforts in Europe and make a greater use of synergy in order to achieve as soon as possible objectives aimed at building efficient European information infrastructure"[219]. The exercise of intellectual property rights is therefore mainly subject to a series of specific treaty rules[220] that shape the legal framework as a response to the challenges brought by information technologies. In the US, Article 2B of the *Uniform Commercial Code* regulates the licensing of information in general, including the licensing of software and other copyrighted works. Framed as "a cyberspace contract statute", Article 2B is said not to "*create* contract law – it merely provides a more coherent base for contracting".[221] It takes a liberal direction to validate broad range of shrinkwrap contracts, allowing for unreasonable terms in mass-market licenses to be enforceable as long as there is separate assent to the unreasonable term. It

---

[219] Commission of the European Communities, White Paper on Growth, Competitiveness, Employment: The Challenged and Ways forward into the 21st Century; COM (93) 700 final, Brussels, 5 Dec. 1993.

[220] Council Directive 91/250 on the legal protection of computer programs;
Council Directive 92/100 on rental and lending rights and certain rights related to copyright in the field of intellectual property;
Council Directive 93/83 on the coordination of certain rules concerning copyright and rights related to copyright applicable to satellite broadcasting;
Council Directive 93/98 harmonizing the term of protection of copyright and certain related rights.

[221] Uniform Commercial Code Article 2B: Software Contracts and Licenses of Information, with notes, available at http://www.law.uh.edu/ucc2b/.

is thus feared that the Article encourages a free licensing system that could end up displacing copyright law. When widespread contractual arrangements set asides the longer term interests, like consumer protection issues, freedom of expression issues and innovation policy in competition policy issues, copyright law is in fact being made obsolete. There are concerns that copyright law would become a kind of consumer protection or a public policy system so that copyright policy gets invoked when there's been an override of public policies that are embodied in copyright.[222]

In the US the question of the enforceability of mass-market standard software license agreements, such as shrinkwrap licenses, was examined in *ProCD v. Zeidenberg*[223] case. The plaintiff sought to enforce a mass-market software license agreement on a CD-ROM telephone listing that prohibited making the content available to any other user in any networked or time-shared environment. Although telephone listing is not covered by copyright protection in the US[224] and the ProCD found to effectively expand his copyright monopoly over uncopyrightable material through the enforcement of the license agreement, the validity of this license was upheld. The reason for the decision, according to the Court of Appeal, was that the contract was duly formed when the software was used. By recognizing the enforceability of the shrinkwrap contract, the decision of *ProCD v. Zeidenberg*[225] case implied that software producer can expand his monopoly beyond the terms of the Copyright Act. It is recognized that, however, the court's analysis in this case was determined by a geographical factor and by the nature of the product involved: the American computer industry follows specific licensing practices. The conclusions of the Court of Appeals for the Seventh Circuit could have

---

[222] Contract and Copyright Exemptions, supra note 188.

[223] 86 F.3d 1447 (7th Cir. 1996).

[224] Feist Publications Inc. v. Rural Telephone Service Co. Inc., 737 F.Supp. 610, 622 (1990).

[225] 86 F.3d 1447 (7th Cir. 1996).

differed if the contract had purported to restrain a user's fundamental rights, such as his freedom of speech or his freedom of information. [226]

European courts seem to take more restrictive approach to copyright owner's monopoly in mass-market licenses. In the well-known *Leesportefeuille* case a magazine publisher had put a notice in his publications prohibiting the legal acquirer from re-using the printed material in subsequent "reading portfolio", known as *leesportefeuilles*. The defendant disregarded the notice, published a portfolio and distributed it to its clients. Plaintiff filed suit on the grounds of copyright infringement. The Dutch Supreme Court found in favor of the defendant, considering that the plaintiff's copyrights were exhausted as soon as he had made his magazines available to the public and had therefore no right to restrict the user's subsequent actions. The notice prohibiting further reproduction was contrary to the exhaustion doctrine found under the Dutch Copyright Act.[227]

Legislation also makes some copyright limitations mandatory in certain specifically prescribed fields, like computer programs and databases. The *EC Directive on the legal protection of computer programs* contains four of such exemptions. According to Article 5 (2) of the Directive "the making of a back-up copy by a person having a right to use the computer program may not be prevented by contract insofar as it is necessary for that use". Also, the observing, studying or testing of a computer program (Article 9(1) and Article 5(3)), running a program and to error correction (Article 5(1)), as well as "decomplation (or reverse engineering, Article 9(1) and Article 6) may not be contractually restricted. Similarly, the *EC Directive on the legal protection of databases* contains a number of mandatory exemptions (Article 15). The legitimate user may perform acts inherent to normal usage (Article 6 (1)); the right to re-utilise non-substantial parts of a Database may not be overridden (Article 8). These restrictions do not aim at preserving any fundamental right or freedom on the constitutional level. Rather, they have been implemented on the basis of competition law considerations, to

[226] Contract and Copyright Exemptions, supra note 188.

[227] Id.

prevent any abuse of dominant position within the software and database industry. In contrast, restrictions implemented in favor of libraries, archives and museums are not immune to contractual overrides. Perhaps it is felt that limitations of this type do not pursue objectives so fundamental to the defense of individual freedoms and the free flow of information that they should be considered imperative rules from which parties may not deviate by contract, under any circumstances.

In the absence of specific stipulation in legislation, the assessment of whether other statutory copyright limitations override contractual provisions to the contrary must follow a careful examination of their grounds for adoption. Some limitations may find their justification in competing bodies of law, such as the European Convention on Human Rights or the competition rules of the Treaty of Rome, while others may be implemented on the basis of national public interest considerations or as a remedy to market failure. Public policy reasons may thus warrant the mandatory application of a number of these limitations, for fear of disrupting the balance struck by copyright law.

### 3.3.2 Copyright Limitations Preserved by Anti-Circumvention Laws

As Hugenholtz points out, on top of the existing copyright layer the technological measures provide an extra layer of protective armour.[228] Under copyright law a right-holder cannot statutorily control each use of a protected work, while the introduction of technological measures may upset the balance that copyright law has achieved between the interests of right-holders and the interests of users. Right-holders will be tempted to exercise their factual monopoly (as opposed to the limited statutory monopoly that copyright grants) by fencing in more material, and precluding more uses by technical means than copyright law enables them to. Thus, the countervailing effect of the copyright limitations is undermined. Although some authors insist that "the answer to the

---

[228] P. Bernt Hugenholtz, Code as Code, Or the End of Intellectual Property as We Know It, Maastricht Journal of European and Comparative Law, Volume 6 (1999), No.3, p.308-318, available at http://www.ivir.nl/medewerkers/hugenholtz.html.

machine is in the machine"[229], unrestricted use of technological protection has led to concerns over information block-out on the Internet. Some over-restrictive measures may even vitiate fundamental rights such as privacy and right to information by monitoring and tracing users' reading particular reading habit. In view of the tendency of copyright expansion, it is necessary to examine whether general rules of copyright limitations can be invoked in support of the copyright balance.

The statutory source in this regard, ironically, is to be found in a series of documents that provide legal protections of technological protections of copyrighted works. This is understandable because ECMS is accepted more as a positive measure and is expected to play an increasingly important role in the future on-line trade in content and the administration of rights. However, legislators and policy makers are not unaware of the need to check the unbundled use of private power that runs afoul against copyright limitations. All legislative bodies that have taken on the protection of technological measures stress that the balance that is struck in copyright law between the interests of the right-holders and of copyright users must be maintained. Consequently, legal protections of ECMS are designed to incorporate certain limitations to these technological measures, thus maintaining the copyright balance in the digital environment to more or less extent.

Major instruments include the 1996 WIPO Copyright Treaty (WCT)[230] and WIPO Performances and Phonograms Treaty (WPPT), the proposed EU Directive on the Harmonization of Certain Aspects of Copyright and Related Rights in the Information Society (hereinafter referred to as the proposed EU Copyright Directive)[231] and the

---

[229] Ch. Clark, 'The Answer to the Machine is in the Machine', in: P. Bernt Hugenholtz (ed.), The Future of Copyright in a Digital Environment, supra note 212.

[230] Article 11 of the WIPO Copyright Treaty requires the contracting states "[to] provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this treaty or the Berne Convention and that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law."

[231] Article 6 (1 and 2) of the amended proposal reads:

Digital Millennium Copyright Act (DMCA)[232]. All contain provisions which protect copyright management information by making it illegal to remove or change it. Although the purpose of these legislation is to protect technological protections of copyrighted works, they make efforts to keep some copyright limitations in the design of the mechanisms of legal protection. This is exemplified in the following several aspects.

Firstly, all three provisions stress in general the necessity to maintain certain limitations to technological measures that make private ordering of copyrights. The Preamble to the WCT states that the Treaty is drafted while:

Recognizing the need to maintain a balance between the rights of authors and the larger public interest, particularly education, research and access to information, as reflected in the Berne Convention.

Similarly, in Recital 21 of the proposed EU directive it is considered that a "fair balance" must be safeguarded. Also, the US legislature underscores that a balance between the interests of both parties must be struck where the protection of TMs is concerned.[233]

---

"1. Member States shall provide adequate legal protection against the circumvention without authority of any effective technological measures designed to protect any copyright or any rights related to copyright as provided by law or the sui generis right provided for in Chapter III of European Parliament and Council Directive 96/9/EC, which the person concerned carries out in the knowledge, or with reasonable grounds to know that he or she pursues that objective.
2. Member States shall provide adequate legal protection against any activities, including the manufacture or distribution of devices, products or components or the provision of services, carried out without authority, which: a) are promoted, advertised or marketed for the purpose of circumvention of, or b) have only a limited commercially significant purpose or use other than to circumvent, or c) are primarily designed, produced, adapted or performed for the purpose of enabling or facilitating the circumvention of, any effective technological measures designed to protect any copyright or any right related to copyright as provided by law or the sui generis right provided for in Chapter III of European Parliament and Council Directive 96/9/EC."

[232] Section 1202 of Title I, which constitutes one of the five sections of chapter 12 that will be added to title 17 of the US Code, implements the obligations contained in Article 12 of the WCT and Article 19 of the WPPT and protects the integrity of copyright management information.

[233] See House Report 1998b: 24-26: "[the provisions concerned] prohibit certain actions and create exceptions to permit certain conduct deemed to be in the greater public interest, all in a way that balances the interests of copyright owners and users of copyrighted works."

Secondly, legal protection is given to defined subject matter instead of covering all kinds of copyright management measures. Leaving some technological measures "unprotected" by law, the provisions thus implicitly permit certain copyright limitations to the use of such measures. The technological measures protected under Art.11 of WTC are those that restrict acts not authorized by the authors or permitted by law. This means circumventing for the purpose of performing an act permitted by copyright law or other areas of the law (e.g., the right to privacy or the freedom of information) need not be outlawed. Apparently, technological measures that only meter usage or merely enable a transaction to take place are not covered, since they do not necessarily "restrict acts". Both the US and EU protect copyright management information (CMI), which is defined to encompass information that identifies the work, the author and the owner of any right in the work, information about the terms and conditions of use and numbers or codes that represent any of the aforementioned information. In the proposed EU Copyright Directive, CMI also includes information in connection with a work or subject matter covered by the *sui generis* right of the Database Directive. According to the DMCA, only measures that that "effectively" protect copyrights are protected, so access prevention to non-copyrightable material like databases does not fall within the scope of the provision. In DMCA, CMI that identifies information about a user is explicitly excluded, which is probably due to the concern for the conflicting interests of protecting the right to privacy.[234]

Thirdly, not all circumvention-enabling devices are prohibited, so that the balance between the interests of right-holders and users can be maintained through enabling certain supposedly lawful circumvention. Under both the EU and US protection scheme there is a "purpose requirement" in order to establish infringement liability for

[234] In response to concerns that copyright management system might be intrusive on privacy interests, the legislative history of DMCA makes clear that copyright management information (CMI) does not include digital information used to track or monitor usage of copyrighted works: "It would be inconsistent with the purpose and construction of this bill and contrary to the protection of privacy to include tracking and usage information within the definition of CMI." Section-by-Section Analysis of H.R. 2281 As Passed By the United States House of Representatives on August 4, 1998, 105th Congress, at 20.

circumvention-enabling devices.[235] The proposed EU Copyright Directive takes an objective criterion of "purpose": It provides that dealing in devices or providing services that "have only limited commercially significant purpose or use other than circumvention" is covered. That means if a device coincidentally has an unintended use besides circumvention, it will not be outlawed. The DMCA takes a similar approach by requiring that the device is "primarily designed or produced for the purpose of circumventing", which is understood as an objective standard. To satisfy producers of general-purpose electronics, it is expressly added that it is not required to design consumer electronics, telecommunications or computing products to provide for a response to any technological measure.[236]

Finally, not all circumventing activities are targeted under the three protection schemes. As recognized in the Explanatory Memorandum of the propose EU Copyright Directive,

"the real danger for intellectual property rights will not be the single act of circumvention by individuals, but the preparatory acts carried out by commercial companies that could produce, sell, rent or advertise circumventing devices."

If taking the market failure considerations of limitations in ECMS, existing statutory technological measure protection schemes should target only the preparatory activities to circumvention rather than the actual act of circumventing, since the former activities have greater impact on the potential market for or value of the material protected while it will be economically infeasible [237] to prohibit and detect private use. However, it is unclear whether the act of circumvention is actually covered by Art. 6 of the EU Copyright Directive, which covers "any activities, including the manufacture or distribution of

---

[235] The WCT does not contain any purpose requirement. Art.11 only states that the remedies provided for must be "adequate", thereby leaving regulations at the discretion of Contracting States.

[236] Proposed section 1201(c)(3) of the DMCA. However, in section 1201(k), it is specifically prescribed to include certain copy-preventing technologies in analogue video recorders.

[237] 296 Litman 1997b: text near note 49; Landes & Posner 1989: 358 ("the potential fee (or damages) per user might be so small [...] that enforcement proceedings would be infeasible").

devices or the performance of services, which have only limited commercially significant purpose or use other than circumvention". The only thing clear is that it prohibits the commercial dealing in circumvention devices. On the other side, the DMCA expressly deals with preparatory acts of circumvention. In respect of the actual circumvention activities, it only prohibits circumvention of technological measures that control access, but leaves circumventing measures that protect a copyright uncovered. Some authors therefore conclude that the DMCA deliberately create a "right to control access to technological measures-protected works".[238] Perhaps the rationale is that, as Smith states, controlling access is important for controlling copying, while it prevents many infringements from ever taking place, and it is easier to control copying by authorized, known users, either by contract or by identification of the duplicated copy.[239]

Compared with the EU Copyright Directive and US DMCA, the WIPO treaties seem to be more restrictive in the sense that it includes the actual circumvention of a technological measure that protects a copyright.[240] On the implementation level, however, most commentators are correct in observing that DMCA provides a much stronger standard for protection of technological measures. The focus of WCT is on the act of circumvention, and not the technologies which might make circumvention possible. In contrast, while DMCS focuses on outlawing circumvention for the purpose of obtaining access to the underlying work, it prohibit not only the act of circumvention of access control, but also device or service which would serve to facilitate access.[241] It is noteworthy that the prohibited circumvention of access control is not limited to infringing purposes, but includes acts traditionally permitted by copyright limitations.[242] There is

---

[238] N A Smith, "United States of America"; see Protection of Technological Measures, Institute for Information Law, Amsterdam, available at http://www.imprimatur.net/legal.htm.

[239] Id.

[240] It is observed that the final wording of the provision has been the result of the successful lobbying of producers of (consumer) electronics. Protection of Technological Measures, supra note 239.

[241] 17 U.S.C. § 1201(a) (Supp. V 1999)

[242] Although the DMCA authorizes the Librarian of Congress, in consultation with the Register of Copyrights, to assess the impact of the circumvention ban on traditional fair use practices and, if

concern that unfettered use of ECMS will supplant fair use and other exceptions. Content providers may successfully prosecute a violation of the anti-circumvention law against users who attempt to access materials that lay in the public domain. Many scholars point out that the first sale doctrine has been in effect eliminated by the pay per view/listen business models – different levels of enjoyment of works set up by the ECMS.[243] As copyright until now did not grant a right to control access, it is not surprising that the fair use doctrine did not limit the possibility to prevent access or set conditions upon access to published works. It is suggested that to keep the equilibrium of interests, copyright law should prohibit the application of technological measures that prevent acts permitted under copyright law or block access to non-protectable material.[244] Then, the copyright limitations would affect the extent to which uses may technologically be blocked.[245]

## 3.4 THE NAPSTER INTERPRETATION OF SECONDARY LIABILITY AND FAIR USE

The ECMS is based on the presumption that rampant copyright infringement in cyberspace can be curbed by access rules that condition the use of the protected material at the control of content owner. It is thus deemed as an effective two-party deal through the digital incorporation of contractual agreement into the technological measures. If a user tries to violate certain access/use conditions, he may be blocked by the built-in "fences" of the ECMS, or he may be sued for breach of contractual terms of the license agreement. Further, acts or attempts of circumvention of ECMS are outlawed by anti-

---

necessary, to issue rules exempting certain uses of certain categories of works from the ban, the statute makes it clear that any such exemptions will not provide a defense to the prohibition on circumvention technologies. 17 U.S.C. § 1201-1205.

[243] Jane C. Ginsburg, Copyright and Control over New Technologies of Dissemination, 101 Colum. L. Rev. 1613, 1632.

[244] See J E Cohen, "A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace", available at http://38.222.224.75/sol3/paper.taf?ABSTRACT_ID=17990.

[245] Protection of Technological Measures, supra note 239.

circumvention laws with various levels of exemption. In short, code backs up law, which, in turn, backs up code.

The strength in the individual-targeting "code plus law" approach will be drastically limited if, however, tracking of unauthorized use is virtually impracticable due to the open nature of the Internet, or the effect of enforcement is counter-productive. Certain copyrighted works generally contain no copyright management system, such as MP3[246] files, thus they offer no protection against unauthorized copying, use, or distribution. Because MP3 files are sound recordings protected by copyright law, and most people uploading such files rarely have permissions from copyright owners to make digital copies of their music and distribute them on the Internet, direct infringement of music copyrights is a common practice in cyberspace. Nevertheless, it is financially and socially impracticable to pursue all the individual infringers directly through the process of litigation. The image of big incorporation prosecuting poor student hacker also has the effect of alienating consumers. Therefore, there is incentive for right holders to enforce copyright law indirectly by placing those in a position to control the use of the copyrighted works liable, as small-scale copyright infringement that occurs within a small group of friends or music fans is a reality that owners have to live with in cyberspace as well as in real space. What worries right holders most is large-scale infringement, made possible by new services of file sharing that does not fit comfortably within the traditional doctrines for secondary liability. Where the ECMS does not work, traditional copyright protection needs to be expanded, through legislation or case law, to accommodate the changed power balance in cyberspace. Greater emphasis is placed on the control by third-party intermediaries; at the same time, fair use defense has been

[246] MP3 is a compression digital technology which stands for MPEG-1 audio Layer 3. It allows audio data (generally requires large files) to be compressed into relatively small files that are easily transferred on the Internet and downloaded onto a personal computer or portable player. These files are digital, so they retain the near-CD quality sound no matter how many copies are made, and once downloaded can be played any time the user whishes. See MP3 technology rocking the music world, CNN March 1, 1999, available at http://www.cnn.com/TECH/computing/9903/01/web.music.ants/ (visited August 2, 2000).

subject to more restricted interpretation. The Napster litigation[247] provides such an example.

Napster is an Internet-based company that employs the peer-to-peer (P2P) technology to facilitate the copying of MP3 files form one user's hard drive to another's, by hosting a centralized directory that responds to searches for particular songs by identifying the matching holdings of Napster users currently online. After downloading the "swapping" software (Musicshare) from the Napster website, a subscriber is then able to locate an MP3 file by an automatic connection to one of the 150 servers operated by Napster and downloading the file directly from the computer of another subscriber who has the file. Since Napster subscribers "traded" MP3 files within such a sharing system and they do not give up the copy on their computers, any copy residing on one subscriber's computer has the capacity to turn into as many additional copies as there are other Napster subscribers. Napster states that it does not make any copies of MP3 files on its own servers.

A suit initiated by the major five record companies charged Napster with contributory and vicarious liability. The District Court for the Northern District of California granted a preliminary injunction after finding that Napster would very likely to be found liable. On appeal, the 9th Circuit Court of Appeals held that there was a likelihood that Napster was both vicariously and contributorily liable for its users' copyright infringement, but remanded for modification of the scope of the injunction by placing the burden on the plaintiffs to notify Napster of the specific infringing files in question.[248] Based on the reformed order of the district court, once Napster received a list of copyrighted works owned by the plaintiffs, it is required to block transmission and remove all complementary search ability for the named files within three days.[249]

---

[247] A&M Records, Inc. v. Napster, Inc., 114 F.Supp.2d 896 (9th Cir. 2001)

[248] Id.

[249] A&M Records, Inc. v. Napster, Inc., 2001 U.S. Dist. LEXIS 2186 (N.D.Cal. Mar. 5, 2001).

Napster is not a case of anti-circumvention, because Napster was not charged with circumventing access control by the plaintiffs.[250] But it raised three related issues: the development of secondary liability theory for intermediaries; the legitimacy of copyright-defying devices under anti-circumvention laws; and the scope of copyright limitations in respect of novel file-sharing systems.

### 3.4.1 Secondary Liability for Intermediaries

#### 3.4.1.1 Pre-Napster test

In the Untied States, contributory liability is codified in the Patent Act but not in the Copyright Act. However, the concept of secondary liability for copyright infringement grew out of tort and master servant liability principles and out of the grant of the exclusive right "to authorize" under Section 106 of the Copyright Act.[251] Under the theory, providers of technology that can be used to infringe copyright may be liable for the infringement of users in certain circumstances.

In essence, contributory liability is found when the third party: (1) knows of the infringing activity; and (2) induces, causes or materially contributes to it. Actual knowledge is not required as long as the contributory infringer has reason to know the direct infringement.[252] On the other hand, a third party is vicariously liable for harm done by a person who infringes on copyright owner's exclusive rights if it: (1) has the right and ability to supervise the infringer; and (2) derives a direct financial benefit from the infringer's actions.

---

[250] The Napster subscribers who were held to have directly infringed plaintiffs' copyright did not "circumvent" any technological measures either, because MP3 files shared within the Napster system do not contain any ECMS.

[251] 17 U.S.C. §106 (1999). In Sony Corp. of America v. Universal City Studios, Inc. 464 U.S. 417 (1984), the Court recognized that:
"[T]he lack of clarity in the area [of vicarious and contributory copyright infringement] may, in part, due to the fact that an infringer is not merely one who uses a work authorization by the copyright owner, but also one who authorizes the use of copyrighted work without actual authority from the copyright owner."

[252] See Sega Enters. Let. v. MAPHIA, 948 F.Supp. 923 (N.D.Cal. 1996).

The United Supreme Court in Sony case[253] established the Staple Article of Commerce Doctrine (hereinafter "Sony defense"), which granted conditional immunity to developers of new technologies: the mere sale by a manufacturer of a staple article of commerce capable of substantial non-infringing uses that consumers may use for, among other things, does not necessarily render the manufacturer contributorily liable for its buyer's infringing use. Thus, the key issue turns on whether the new technology has a non-infringing use, or at a minimum, the capacity for such use. The rationales for the Sony defense was that copyright owner's desire to prevent unauthorized use of works should not tramp valid public interest in the development of new technologies.[254]

3.4.1.2 Contributory Liability under Napster

Upon appeal, the Ninth Circuit held that Napster was likely to be contributorily liable for its users' infringement not only because Napster made the direct infringement of its users possible, but also because "Napster had actual knowledge that specific infringing material is available using its system."[255] The court declined to apply the Sony defense, reasoning that it is merely a tool for imputing Napster constructive knowledge of its users infringing actions, while Napster had actual knowledge of infringement. This was viewed as a clear departure from the pre-Napster interpretation and from the Supreme Court's actual decision in Sony.[256] It seems to imply that so long as the defendant knows about infringing activities on its system – or even, the infringing purpose for which its

---

[253] Sony Corp. v. Universal City Studios, 464 U.S. 417 (1984).

[254] Id. at 441.

[255] 114 F.Supp.2d. Two reasons were cited by the Ninth Circuit for finding actual knowledge of Napster: (1) a document written by Napster co-founder Sean Parker mentioned "the need to remain ignorant of users' real names ... 'since they are exchanging pirated music'" and (2) the Recording Industry Association of America (RIAA) notified Napster of more than 12,000 infringing files. Id. at 1022.

[256] Bruce G. Joseph, Dineen P. Wasylik, Copyright Issues on the Internet and The DMCA, Practising Law Institute, Patents, Copyrights, Trademarks, and Literary Property Course Handbook Series, May and June 2003. See also, Matthew Fagin et al., Beyond Napster: Using Anti-Trust Law to Advance and Enhance Online Music Distribution, 8 B.U.J.Sci. & Tech.L. 451, 480.

system/product would be used, at least constructive knowledge will be found against defendant.

Noteworthy in this departure is the distinction that the court drew between the Sony case and Napster. The technology of video recording in Sony is free-standing, i.e., once sold the video recorders are no longer under the control of the developer, who could not monitor the ways consumers utilize the product. Thus, to penalize the developer by contributory liability would yield an "all or nothing" result: Either no video recorders were to be put into the market under the threat of indirect copyright infringement, or producer be granted immunity for distribution despite the capacity of infringing uses of his product. As will be discussed below, the video recording technology could be used for substantial non-infringing purposes, and had even proved to spur a new market for dissemination of copyrighted works that benefited both the copyright owners and consumer, balance of interests tilted in favor of the producer. As the case for Napster, the Music share software was an integrated part of an ongoing service. The software was frequently updated by Napster. Although it refused to transmit date protected by copyright law, Napster did provide directory services to help its subscribers to locate such works. Most important, Napster had the control capacity to remove or block access to the infringing directory listings, thereby limiting its service to locating only non-infringing content. As a result, the Napster case did not present an "all or nothing" choice for new technology because the particular mode of implementation by developers like Napster can be regulated. The legal rule of secondary liability should show more flexibility given the complex control capacity of developers of new technology.[257]

However, this distinction raised more questions than it purported to solve. The crucial factor in finding contributory liability for infringement is defendant's (actual or constructive) knowledge of infringing activities on its systems. Napster holding arguably tightened the standard of knowledge for intermediaries or providers of technology.

[257] Jane C. Ginsburg, Copyright and Control over New Technology of Dissemination, 101 Colum.L.Rev. 1613, 1641.

Justification was based on Napster service's ability to exercise certain amount of control over its subscribers' activities, for instance, by terminating users who are found to transmit infringing materials, or by removing the infringing content from the system. But even with the centralized server structure of Napster, proving the requisite control may be difficult. A terminated user can always log on with different IP addresses and register with another ID. Should Napster still be held liable if such control is of limited help?

Secondly, the analysis of the nature of Napster's on-going service has significant implication for decentralized peer-to-peer systems. Recognizing the legitimate purposes that P2P systems serve and the danger of over-restrictive copyright enforcement may have on the development of technology, the Ninth Circuit cautioned, "We are compelled to make a clear distinction between the architecture of the Napster system and Napster's conduct in relation to the operational capacity of the system."[258] (*emphasis added*) Napster's "architecture" is presumably the P2P system, and it was not the source of Napster's liability. The Ninth Circuit warned that it would "not impute the requisite level of knowledge to Napster mere because peer-to-peer file sharing technology may be used to infringe plaintiffs' copyrights."[259] From the standpoint of intermediaries who provide either service or technology that facilitates unauthorized sharing of copyrighted works, they would invariably invoke the Napster distinction and claim that the challenged service/technology is "free-standing" as the video recorder in Sony. However, to what extent of the control such intermediaries would retain that they can be shielded from imputation of constructive knowledge? It is unclear whether the court's reference to "operational capacity of the system" means that Napster is liable only to the extent that it can control its system. Suppose, a file sharing service is deliberately designed to make the

[258] 907 F.Supp. at 1373.

[259] As most observers of the case noted, it was not the peer-to-peer technology itself that was infringing, but the particular manner in which Napster used the peer-to-peer technology to implement its service. The court thus avoided discussing the infringing versus non-infringing uses under the Sony structure, but instead, found Napster's actual knowledge based on its capacity to control and its material contribution to infringement by providing the site and central indexing services. See Aric Jacover, I Want My MP3! Creating A Legal and Practical Scheme to Combat Copyright Infringement on Peer-to-Peer Internet Applications, 90 Geo.L.J. 2207.

provider unable to control users activities while allowing substantial infringement take place on the system, as long as its executives keep their mouth shut on any "knowledge" of the existence of infringements, it would be difficult for copyright owners to sue under the Napster secondary liability theory. Be that as it may, a service provider is very likely to be held liable for infringing activities of its subscribers, under the Napster reasoning, if its relationship with such activities or infringers is shown to be not accidental or tenuous.

If generalized knowledge of infringing uses was not enough to justify holding it liable as a contributory infringer, it is natural to require plaintiff to present evidence of specific acts to show defendant's special knowledge. Hence, the district court was ordered to remand the injunction mandating Napster to act only in instances where it has specific knowledge of infringing activities.[260] Implicit evidentiary requirement in this holding is a similar "notice and take down" procedure to that enacted under the DMCA, i.e., upon receiving notices from copyright owners alleging that specific copyrighted music files are being traded on the system, service provider must act expeditiously to remove or block access to the allegedly infringing material.[261] Such documentary notice serves as a factor of actual knowledge if a suit is later brought against the service provider. In effect, however, it creates adverse incentives for intermediaries to censor speech completely on grounds of copyright infringements, before they can reasonably determine whether the alleged infringer has a fair use defense. After all, copyright law should not suppress speech but only control the commercialization of certain types of speech. Mere refusal to censor users is not equal to intentional facilitating infringement, an element of material contribution. Given the fact that copyright owners can easily create "actual knowledge" by sending a letter, it is also doubtful whether voluminous files of notice by copyright holders has any significant difference from the general fact that the operational capacity of defendant's system contains infringing uses as well as non-infringing uses. The issue of "specificity" remains in the factual findings by courts.

---

[260] 239 F.3d at 1027.

[261] 17 U.S.C. §512(c)(1)(A)(3) and 17 U.S.C. §512(d)(1)(C).

3.4.1.3 Vicarious Liability under Napster

Napster's downfall was also attributable to its central indexing service and the right to block access at its discretion, evidencing Napster's ability to supervise and control users' activities. Moreover, though lacking statutory basis, U.S. courts in deciding vicarious liability for copyright infringement have traditionally followed the market impact analysis, based on the tort law principles of respondeat superior and entrepreneur liability. It is reasonable, under the respondeat superior theory, to hold a person who has the right and ability to supervise an infringer and who in addition benefits from the infringer's conduct, responsible for any damages resulting from that infringer's activities.[262] Napster was held to likely be held vicariously liable, because it enjoyed a direct financial benefit from the structure of its service.

But how "direct" must the financial benefit be? Some courts hold that the ISP's flat fee price structure gives it no marginal benefit from carrying infringing posts.[263] Obviously Napster broadened the view. Direct financial benefit from the current trading of infringing files on Napster's system was established by a prediction into the future: that Napster's future revenues will depend on the size of user base, and copyrighted music "act as a draw" to increase the size of the user base. More users register with the Napster system as the "quality and quantity of available music increases."[264]

As to the element of supervision, consensus in case law was that the ability to block infringers' access to a particular website/service is evidence of the right and ability to supervise.[265] In Napster, the court found that Napster has an express reservation of rights policy, stating on its website that it expressly reserves the "right to refuse service and

---

[262] Gershwin Pub. Corp. v. Columbia Artists Management, Inc., 443 F.2d 1162 (C.A.N.Y. 1971)

[263] See Religious Tech. Center v. Netcom On-Line Communication Servc., Inc., 907 F.Supp. 1376 (N.D. Cal. 1995), and Marobie-FL, Inc. v. National Ass'n of Fire Equip. Distribs., 983 F. Supp. 1179 (N.D. Ill. 1997).

[264] Napster, 114 F.Supp.2d at 902.

[265] See, for example, Netcome, 907 F.Supp. 1376.

terminate accounts in discretion, including, but not limited to, if Napster believes that user conduct violates applicable law...or for any reason in Napster's sole discretion, with or without cause." It is noteworthy that Napster system does not "read" the content of indexed files other than to check that they are in the proper MP3 format. Nevertheless, since it ahs the ability to locate infringing content listed on its central index, and the right to terminate users' access to the system, the failure to exercise its reserved right to prevent the exchange of copyrighted material leads to imposition of vicarious liability on Napster for copyright infringement. Thus, from the rationales of Napster court, to escape vicarious liability, the reserve right to police must be exercised to its fullest extent.

Turning a blind eye to detectable acts of infringement for commercial advantage gives rise to liability.

3.4.1.4 The Interplay of Secondary Liability and the DMCA

From the part holding on secondary liability of Napster, as discussed above, we may come to a summary of the rule. Three conditions must be met for an Internet intermediary to avoid contributory and vicarious liability for third party's infringing act: (1) it must have no actual or constructive knowledge of subscribers' infringement on its system/service; (2) it lacks the right and ability to control user behavior; and (3) it does not derive a direct financial benefit from the third party's infringement.

One twist in the Napster litigation is the statutory limitation defense raised under the Safe Harbor provisions in DMCA.[266] The provisions are a response to copyright owners' preference to enlist intermediaries as "copyright police" with the threat of infringement actions and the fact that ISPs are particularly vulnerable to such claims because of the sheer volume of content they process, the automated nature of their systems and the relative anonymity of many of their users.[267] The DMCA defines "service provider" as:

---

[266] 17 U.S.C. §512.

[267] Bruce G. Joseph, Dineen P. Wasylik, Copyright Issues on the Internet and The DMCA, Practising Law Institute, Patents, Copyrights, Trademarks, and Literary Property Course Handbook Series, May and June 2003.

(1) "an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing;" or (2) "a provider of online services or network access, or the operator of facilities."[268]

The district court dismissed Napster's claim as an "ISP" under the safe harbor, because it did not satisfy the requirements under §512, i.e., not performing the applicable functions "through" its system as a conduit. Instead, infringing material is transferred directly over the Internet from user to user, "not through the Napster server."[269] Arguably this reading too narrow to comport to the legislative intent of DMCA, which intends to cover wide range of Internet intermediaries not limited to ISP. In essence Napster's functions are analogous to that of a search engine, albeit with higher level of control. And one type of safe harbor is available to ISPs that either host material for someone else or that operate search engines which point to infringing material. Upon appeal, the Ninth Circuit correctly rejected any "blanket conclusion" that §512 was inapplicable, while finding that "significant questions" regarding the applicability of the safe harbor to Napster remain.[270] The court, however, did not deliberate on this issue, but went on to affirm district court's injunction, on the ground that the balance of equities supported the injunction at this stage of the litigation in plaintiffs' favor.[271] Hence, the court was ultimately unwilling to allow Napster the protection of the safe harbor provisions in DMCA.

One might wonder: would Napster escape secondary liability if DMCA had been applied to the case? It is not difficult to find the negative answer from the holdings of district court and the Ninth Circuit. Sections 512(c) and (d) closely paralleled the common law theory of contributory and vicarious liabilities as construed in the Napster case: (1)

---

[268] 17 U.S.C. §512(k)(1).

[269] Napster, 54 U.S.P.Q.2d 1746 (N.D.Cal. 2000) at note 9.

[270] Napster, 239 F.3d 1004 (9th Cir. 2001).

[271] Id.

Qualifying ISPs must neither have "actual knowledge," nor are "aware of facts or circumstances from which infringing activity is present," and (2) such ISPs must not derive "a financial benefit directly attributable to the infringing activity, in a case in which it has the right and ability to control such activity."[272]

Furthermore, the threshold for invoking the safe harbors provisions is much more stringent than mere lacking elements of a finding of secondary liability. The district court held that Napster failed to meet the condition of §512(i) requiring a service provider to have "adopted and reasonably implemented, and informed subscribers and account holders" of a policy for terminating accounts of users who are repeat infringers.[273] It is clear that to find shelter under §512's safe harbor, the Internet intermediary has to comply with additional conditions than what is needed to avoid secondary liability under a conventional common law analysis. Apart from policy of control announcement, the service provider must designate an agent to receive notifications of infringement from concerned copyright owners, and upon receiving such a notification, "respond expeditiously to remove, or to disable access to" the allegedly infringing material.[274] (so-called "notice-and-take down" procedure) As discussed above, to require service providers to act as private censor of users' speech raises free speech concerns. While ISP's failure to act upon notice does not affect its ability to invoke other defenses of copyright law,[275] as a practical matter they have the economic incentive to comply with such conditions in order to avail the protection of the DMCA safe harbors, because risk aversion is prevalent in Internet business under the current unsettled and controversial views scattered in case law toward ISP's liabilities.

---

[272] 17 U.S.C. §512(c) and (d).

[273] Despite Napster's claim that it had such a policy prior to the litigation, the court found that Napster did not inform users of the policy until after the lawsuit was filed. So such self-serving policy should not protect Napster from liability for past conduct. Napster, 54 U.S.P.Q.2d 1746 (N.D.Cal. 2000).

[274] 17 U.S.C. §512(c)(1)(A)(3) and (d)(1)(C).

[275] 17 U.S.C. §512(1).

Therefore, contrary to the impression that §512 of DMCA functions as limitation to Internet intermediaries' strict liability, the conditions and procedures attached to the various safe harbors have the practical effect of compelling intermediaries to assume a much more active role in the enforcement of copyright law than they would be required under the common law secondary liability theory. Given the express legislative intent to protect ISPs from liability, Napster's defense raised an interesting dilemma: where an ISP makes available file sharing software that facilitates unauthorized copying and distribution of copyrighted works, and designs its system in such a way that no central control is possible, but otherwise complies with the attached conditions under §512, should it be allowed to invoke the safe harbors as a preliminary issue to any case in which the DMCA is implicated? This looks like yet another "anti-circumvention" case at which the DMCA is directly aimed, only it is now the law, not the technological measures, is "circumvented."

3.4.1.5 The Legal Prospect of Decentralized P2P systems

Increasing reliance on Internet intermediaries as an indirect means to enforce copyright law presuppose the ability of control by an identifiable local center. When transmission of files steps aside the control center, the legal enforcement of copyright law becomes questionable. This the case for decentralized peer-to-peer (P2P) technology such as Gnutella and its numerous software clones.[276] In such a P2P network, information and contents are transmitted between users in the network, and each individual computer has equivalent capabilities and responsibilities by maintaining both distribution functions and receiving functions (server plus client). This differs from client-server architectures in which some computers primarily function as servers, or, a local control center.

The important distinction made by the Napster court between "the architecture of the Napster system and the Napster's conduct in relation to the operational capacity of the system" has stirred ample controversies over peer-to-peer files sharing systems. Napster

[276] See John Borland & Mike Yamamoto, The P2P Myth, CNET News.com (Oct. 26, 2000), available at http://news.cnet.com/0-1005-201-3248711-2.html.

created a distinction between the underlying technology (P2P) and the Napster service that utilized the technology. It was not the P2P technology itself that was infringing, but the particular manner in which Napster used the P2P technology to implement its service. Thus, although music industry plaintiffs gained their first victory against Napster, they have not yet won their war. If service providers can employ the P2P technology in such way as not to implicate secondary liabilities as Napster did, copyright owners will find it more diffuclt to establish infringement under the current law.

In one file-sharing case filed in October 2001, 28 of the largest music and entertainment companies sued Grokster, StreamCast Networks and Sharman Networks for operating the P2P file-sharing services Grosker, Morpheus and KaZaA, respectively.[277] The defendants successfully argued that their software which enabled P2P sharing of copyrighted works functioned differently from that of the Napster service. Unlike indexing files in a central server as Napster, Groskter and other P2P users connect and upload their files lists to "Supernodes" – other users on the network who have fast connections. Although noting the fact that the file-sharing services did have sufficient knowledge of and profited from the users' infringing activities through their services, the court held that defendants did not have control over users sufficient to impose vicarious liability for users' infringement, as the service would continue even if the companies shut down. The court also agreed that the defendants did not materially contribute to users' infringement, finding "substantial non-infringing uses" of the file-sharing software.[278]

In contrast, in the Aimster case[279], which involved a similar service by defendant that allowed users to identify other users with desirable files and then transfer copies of those files using P2P technology[280], the Northern District of Illinois determined that Aimster's

---

[277] MGM, Inc. v. Groskter, Ltd., 259 F.Supp.2d 1029 (C.D. Cal. 2003).

[278] Groskter, 259 F.Supp.2d 1029.

[279] In re: Aimster Copyright Litigation, 252 F.Supp.2d 634 (N.D. Ill. 2002).

[280] The service included chat rooms and bulletin boards, and included a "tutorial" that explained how to transfer and copy copyrighted works over the system. Aimster, Id.

technology subjected defendants to secondary liability. The court reasoned that Aimster met the requirements of contributory liability because it received several cases and desist letters warning it of alleged infringement, and since Aimster designed and provided the encryption technology, it should not deny knowledge by its own hindrance. The Sony "staple article of commerce" defense did not apply because Aimster's service was not primarily used for non-infringing purposes. Vicarious liability was also found against defendant, based on Aimster's ability to control its users and receiving of a financial benefit from the infringing activities. The court stressed that Aimster had the required right and ability to supervise infringing activities given its statement in the Terms of Service to take down infringing materials, and retaining the right to terminate users.

These cases show the current commotion under existing law with respect to P2P service providers after Napster. Courts diverge not only on the ultimate finding of secondary liability, but also on establishing the elements of them, such as the application of Sony defense, the knowledge requirement of contributory liability, willful ignorance, the requisite level of control needed to establish vicarious liability.[281] For instance, while the Grokster court required specific knowledge of infringement by defendants before imposing contributory liability, the Aimster court held that specificity of knowledge was not required. While Aimster court imputed knowledge by defendant's willful ignorance and held that encryption use alone did not prove lack of knowledge, the Grokster court rejected such a deduction of willfulness despite its acknowledgment that defendant likely designed its technology and business model purposefully to avoid liability. The Grokster court agreed that defendants had no ability to control users, even if defendants could have modified their software to restrict copyrighted materials, as the case in Aimster.

It should be noted that the DMCA ISP safe harbor provisions do not apply to decentralized P2P software providers or distributors, because they do not fit into any of

[281] Robyn Axberg, File-Sharing Tools and Copyright Law: A Study of In re Aimster Copyright Litigation and MGM, Inc. v. Grokster Ltd., 35 Loy.U.Chi.L.J. 389, 435.

the protectable categories under §512.[282] Even in the case where P2P service providers have a policy reserving certain right to terminate users like Aimster, merely having the policy without effectuating its purpose does not meet the requirement of the DMCA safe harbor shelter.[283] Similarly, the right to delete certain links pointing to infringing materials does not equal to the right to control any underlying infringing activities.[284] Unlike Napster, providers of decentralized P2P service usually do not have the ability to remove or disable access to the infringing materials. The flip side of the lack of control, paradoxically, is that it would be difficult to hold them contributorily or vicariously liable for any direct infringement of their users under existing law.

### 3.4.2 Private Copying in the Gray Area of Fair Use

Since secondary liability of Napster was hinged on its subscribers' allegedly infringing activities, Napster's principal defense was that there was no direct infringement by the users. Direct infringement occurs when one violates any of the copyright owner's exclusive rights. Plaintiffs claimed that their exclusive rights to reproduction and distribution, by downloading music files and sharing with other users on the Napster system. Napster claimed that its users were not infringing, but making "fair use" of the copyrighted works.

Not all unauthorized copying and sharing of copyrighted material is prohibited as infringement; many types of personal use are sanctioned under the doctrine of fair use in the United States, or under compulsory license scheme in certain other copyright regimes. Whether unauthorized sharing is characterized as copyright infringement depends on the treatment of private copying and the scope of personal use rights reserved to the public.

---

[282] 17 U.S.C. §512(k)(1).

[283] Aimster, 334 F.3d 658 (7th Cir. 2003).

[284] The Aimster standard of the control element has been criticized as too harsh for establishing vicarious liability, as it allowed the mere contractual retention of a right to terminate a user to satisfy the control element, without any showing of an ability to monitor the networks to gain knowledge as to specific infringers' activities. See Robyn Axberg, File-Sharing Tools and Copyright Law: A Study of In re Aimster Copyright Litigation and MGM, Inc. v. Grokster Ltd., 35 Loy.U.Chi.L.J. 389, 447-448.

Earlier sections of this Chapter briefly discussed the fair use defense as a limitation to the exclusive rights of copyright owners. However, fair use has been a notorious grey area in the case of private copying (or, personal use),[285] the controversy hotly debated in the Napster litigation. It is therefore necessary to examine to what extent the Napster holding clarified this grey area in connection with the new music distribution technologies.

3.4.2.1 Genesis of the Private Copying Controversy

There are mainly two reasons for the indefiniteness of the concept and application of fair use defense in the context of personal use. First, theoretical grounds for accepting private copying differ. One view considers the market failure of implementing stricter copyright law against individuals, because while personal use amounts to a de minimus infringement, requirement of owner authorization for an individual's personal use of protected works has high social cost antipathy to owner's interests. Thus neoclassicists applaud the development of ECMS which greatly reduces transaction cost by automated billing and individualized licensing agreements, thereby arguably eliminating the market failure problem (so the scope of the fair use defense should shrink).[286] Another view, however, deems private copying exception as an unavoidable result of priority of rights: copyright enjoyed by right owners as a statutory grant should not tramp constitutional protection of people's right to privacy. Since enforcement of a strict law prohibiting private copying will invariably intrude one's physical seclusion, one exception must be made as a result of the unenforceable prohibition. Therefore, even the advent of tracking digital technology has the ability to detect unauthorized use, serious privacy concern limits the feasibility of subsequent evidence collection.

---

[285] Matthew Fagin et al., Beyond Napster: Using Anti-Trust Law to Advance and Enhance Online Music Distribution, 8 B.U.J.Sci. & Tech.L. 482.

[286] See Mark Stefik, supra note 215 (discussing the technical possibility to transfer legal aspect of right to commercial aspect of remuneration: "With low overhead, it is practical for publishers to establish very low fees for simple and even rare uses. With automated billing, they can make compliance relatively inexpensive and convenient. Since the fee to exercise a right can be large or small, the gap between fair use (free) and paying to exercise a right (possibly expensive) can be populated by many positions in between: nominal fees, low fees, medium fees, pretty high fees, and so on.").

Second, different copyright regimes allowing fair use have divergent "centre of gravity" as to the point of balance.[287] Private copying as one category of fair use may apply implicitly because of the author's monopoly and "acts subject to restriction," such as the case in French Intellectual Property Code. In this so-called "closed" system, exceptions to author's exclusive monopoly are explicitly defined, and the freedom to make private copies is included in the list of exceptions to copyright as set out by legislators. For example, in France, private copying is defined to apply in two narrow situations: (1) private and gratuitous performances carried out exclusively within the family circle; and (2) copies or reproductions reserved strictly for the private use of the copier and not intended for collective use, with the exception of copies of works of art to be used for purposes identical with those for which the original work was created and copies of software other than backup copies made in accordance. Although under the second exception, it is technically possible to make an unlimited number of personal copies as long as they are all for private use, courts have considered that the fact that the user ends up with a "CD-like product" means that the copy is not "private."[288] The exceptions for private copying do not apply to databases or computer programs, and users first of all must have legally acquired the underlying work.

In common law copyright regimes such as the United States, fair use has been in large part a judicially-created doctrine. It is allowed as a general exception by law while the court is entrusted to determine its application. Loosely defined by statutes, a court will finally balance the value of the allegedly infringing act against the harm to the copyright owner before finding liability. In the United States, Section 107 of the U.S. Copyright Act sets out four factors to determine the existence of fair use: (1) the purpose and character of the use, (2) the nature of the copyrighted work, (3) the amount and substantiality of the portion used, and (4) the adverse impact of defendant's activity on

---

[287] Pierre Sirnelli, Workshop on Implementation Issues of the WIPO Copyright Treaty (WTC) and the WIPO Performance and Phonograms Treaty (WPPT), Geneva, December 6 and 7, 1999, p. 9.

[288] Daniel J. Gervais, Transmission of Music on the Internet: An Analysis of the Copyright Laws of Canada, France, Germany, Japan, the United Kingdom, and the United States, 34 Vand.J.Transant'l L. 1363.

plaintiff's potential market for the work.[289] In addition, private copying is permitted through the Audio Home Recording Act of 1992 (AHRA). Section 1008 of the Act states that "[n]o action may be brought" alleging infringement of copyright "based on the *noncommercial use* (*emphasis added*) by a consumer of such a [recording] device or medium for making digital musical recordings or analog musical recordings."[290] In return, royalties on digital audio devices and all media blanks used in the device are collected and distributed to music publishers and artists. Thus, the Act provides a safe harbor for consumers' personal use with the compensation of the royalty system. Consumer home recording from VCR devices for later playback is protected under the fair use doctrine as the Supreme Court's ruling in Sony.[291] However, since Napster failed to argue that its file-sharing service fell within the scope of the AHRA, the Act has become irrelevant to legal conflicts involving the digital distribution of music.[292] With the establishment of technological fences like ECMS and the anti-circumvention sanctions in DMCA, private copying of digital files is in effect threatened with total ban, because the far-reaching protection of DMCA seriously undermines the basis of fair use defense.[293]

Canadian law is somewhere in-between the "open" and "closed" systems: Unlike U.S., there is no general exception for fair use; private copy and use are more specifically defined in legislation before courts are empowered with the flexibility to evaluate the degree. A private copy can be made both of a work already existing on a material

---

[289] 17 U.S.C. §107.

[290] 19 U.S.C.A. §1008.

[291] Sony, 464 U.S. 417 (1984).

[292] See GartnerG2 and The Berkman Center for Internet & Society at Harvard Law School, supra note 184, p.5.

[293] Many scholars read the stricture of DMCA as failing to provide a fair use defense for circumvention activities, see, for example, Pamela Samuelson, Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to be Revised, 14 Berkeley Tech.L.J. 519 (1999), and Jane Ginsburg, Copyright Legislation for the Digital Millennium, 23 Colum.-VLA J.L. & Arts 137 (1999).

medium and a work not yet fixed on such a support (e.g., broadcast). A private copy means one single reproduction of the work and genuinely private use, which excludes any reproduction for the purposes of distribution to the public or for profit.[294]

Whatever the scope of exception and flexibility allowed to courts, current common trend around world indicates a sweeping outlaw of the private copying in the digital environment. Since private copying is not affirmative right as the exclusive rights enjoyed by copyright owners, but rather an exception to copyrights, content providers have come close to eliminating it by narrowing it scope.

3.4.2.2 The Napster Decision on Fair Use

Since personal use limits certain exclusive rights of a copyright owner, such as the rights of reproduction and distribution, one nightmare for content providers in the digital age is that private copying will lead to rampant small-scale, informal sharing and copying that will devastate their business. That was the position of the recording companies in the Napster litigation. Napster contended that there was substantial non-infringing character in its users' activities, such as space-shifting[295] between office and home computers and sampling before purchase (defenses accepted in Sony), and such activities actually benefit copyright owners in the long run. The Ninth Circuit was not receptive to the argument. Instead, it responded that it is up to the copyright owner to decide how to exploit the work; the decision to authorize sampling, for instance, remains with the copyright owners rather than Napster. Noting that MP3 files contain sound recordings, which are highly artistic creations, and downloading MP3 files for whatever purpose,

---

[294] Pierre Sirnelli, Workshop on Implementation Issues of the WIPO Copyright Treaty (WTC) and the WIPO Performance and Phonograms Treaty (WPPT), Geneva, December 6 and 7, 1999, p.12-13 and 17-22.

[295] Space-shifting was argued as analogy to time-shifting in Sony. In Sony the Court was persuaded that recording television programs to view at a more convenient time was fair use, and should not be subject to remuneration. The Napster rejected this analogy, holding that space-shifting by Napster users automatically released any MP3 files copied onto their computers for potential download by millions of other users.

including space-shifting and sampling, is not transformative, the court found against the fair use defense.

An important aspect to note in the holding is court's determination of "commercial" use. The first factor in §107 – the purpose and character of use – takes into account the commercial nature of the activity, and the AHRA even sets out "non-commercial" as a denominator justifying personal use. Napster claimed that the file sharing constituted a fair use because its subscribers did not "gain a commercial advantage" from at least some of the uses.[296] The district court admitted the non-for-profit motive of Napster users, nevertheless, it went on to define the standard of "commercial" with a focus on the fourth factor – adverse impact to the market. First, "given the vast scale of Napster use among anonymous individuals," such activities as downloading and uploading MP3 music files with the assistance of Napster were deemed not private use. Second, the fact Napster users received for free something they would ordinarily have to buy suggested that they "reap economic advantages."[297] Relying on plaintiff record companies' expert witness on the lost of sale as a result of Napster users' file-sharing activities, the court further reasoned that Napster's service impaired the ability of copyright owners to commercialize their product, based on Supreme Court's rule that widespread use would adversely affect the potential market for the copyrighted work.[298]

The economically-focused analysis is not very surprising, given the reluctance of most U.S. courts to accept fair use defense for private copying in the context of digital distribution of music. What's striking in the case is the similar pattern of argument as when VCRs first came out on the market. Copyright owners back then also argued that the widespread private copying would harm the potential market for movies. In the end, however, the movie industry turned out to benefit from the sale of VCR because it developed a second market for home video playing. In the Napster litigation, both the

[296] Napster, 114 F.Supp.2d 896 (N.D.Cal. 2000).

[297] Napster, 219 F.3d 1015.

[298] Sony, 461 U.S. 451.

district court and the Ninth Circuit referred to expert reports for the plaintiffs which claimed that the record companies had sustained as much as 300 million dollars of damages due to lost CD sales, and that damages would continue to accrue as long as Napster users continued to make unauthorized copies of plaintiffs' copyrighted works. Napster's expert report, on the other hand, claimed that the service actually stimulated sales of CDs for the recording industry by increasing consumer interest in music. The courts dismissed Napster's report in favor of plaintiffs' data, adding that even if plaintiffs' sales in certain areas might be enhanced, "courts have rejected the suggestion that a positive impact on sales negates the copyright holder's entitlement to licensing fees or access to derivative markets."[299]

If the holding was less attackable on asserting copyright owners' right to develop a derivative market, it seems more intuitive a judgment on the economic side, i.e., the adverse impact on plaintiffs' current market, the measure of harm to a "potential market," etc. Despite the hype and rhetoric about the linkage between decreased CD sales and piracy, no true accounting of the financial impact of file-sharing exists.[300] Personal use cuts sales revenue because a user does not make a commercial purchase if he can obtain its analogue or digital copy for free from a friend. But one may also argue that many of the users who would not obtain the free copy from a friend would not otherwise buy it in any way, either. The sales decline might be offset by favorable personal advertising from the circle of fans that increases the demands in turn, or be offset by a higher sales price by the monopoly of the few recording companies in the market. One French author compared the sales of sound recording in the world in 2002: while the industry sales in the U.S. lost 9.2% of their value during the first quarter of the year, sales in France actually rose for that same period by 5.2%, and sales in Brazil rose by 7.1% and sales in Chile rose by 29% compared to the previous quarter. Since private copying of music files

---

[299] Napster, 114 F.Supp.2d 914.

[300] See the survey of GartnerG2 and The Berkman Center for Internet & Society at Harvard Law School, supra note 184, p.18.

and distribution over the Internet are worldwide, the data shows that the impact of piracy can be minimal depending on the country and the year examined. In the author's opinion, the variability in CD sales has more to do with the quality and price of the music industry's product than private copying.[301]

Perhaps it is better to view the Napster analysis of negative market impact simply as declaratory. With easy copying prevalent on the Internet and no technological measures available for MP3 files, more and more copyright owners come to realize that it is important to prevent entitlement to private copying from being transformed into a right to copy. They want to send the message that they will go after those acquiring music for free without proper authorization, as well as sources distributing unauthorized copies of digital works, including ISPs, if the provider does not act to stop infringing transmissions once given notice. The fact that Napster is now engaged in the process of signing license agreements with music companies in the increasingly pay-per-view/hear world concedes the efficacy of this strategy. Most copyright regimes are in the process of gradually shrinking the scope of personal use in the context of digital transmission of music files, based on the concept of "private" in a medium capable of widespread dissemination of protected works. The rights discourse predominating in most legislatures demands stronger protection of copyright owners' control over exploitation of content. Therefore, even a digital transmission devoid of making commercial gain in the traditional sense (such as sharing music with a small circle of music fans) is deemed commercia, because the potentially numerous copying of the same file makes this act for personal use no longer "private," but a public performance.[302] It is observed that "[a]s the public's

---

[301] Tricia Moham, Freedom v. Control: Private Copying and Technological Protection Measures, citing Michel Alberganti, CD, DVD: les vertus du piratage privé, available at http://www.lemonde.fr/web/recherche_resumedoc/1,13-0,37-791262,0.html?message=redirection_article. (visited on Nov. 23, 2003).

[302] In Napster, the Ninth Circuit did not touch the right of public performance by finding that "at least" the right of reproduction and the right of distribution were infringed. Napster, 239 F.3d 1004. Although public performance right was not directly mentioned in Napster, the court's ruling on the issue of derivative markets of copyright owners was in consonant with the WIPO treaty. Article 8 of the WTC grants a right concerning "the making available to the public of their works in a way that the members of the public may access these works from a place and at a time individually chosen by them." WIPO Copyright Treaty, Dec. 20, 1996, Article 8. The WIPO explained this right to cover "in particular on-

easement in the public domain are transformed into piracy, into trespass, independent Web publishing will be steadily displaced by intensive exploitation of established works. The Oversoul that is cyberspace will give way to the Celestial Jukebox, to the corporate synergies of the diminishing number of publishers, networks, and studios."[303]

3.4.2.3 Alternative Remuneration Structures

With the advent of online distribution of copyrighted materials, the distinction between mass market infringement and personal use appears to break down. Debates about private copying have led many countries to expand ways to define digital property beyond the concept of the fair use doctrine.

Despite the varied treatment of private copying in different copyright regimes, in general most countries recognize the need for protecting right holders' revenue in view of the significant economic importance of private copying of copyrighted materials. One mechanism is to impose a blank media levy as price for private copying of individual units of copyrighted works, which has been adopted by eleven EU Member States and Canada. In France, authors' revenues are protected by a remunerative tax on blank materials used for copying purposes. Taxed devices include blank audio and video cassette tapes, and with the widespread Internet copying, materials used in digital copying such as CD-RW are also covered. The proceeds from the tax are allotted to artists' societies, which then redistribute the money to their members. The yearly rate of taxation is established by the Brun-Buisson commission, a group composed of copyright holders, representatives from the industry, and consumers. Presently, the tax can amount to 50% of the price of blank copying materials.[304] Similarly, the fees due to UK writers

---

demand, interactive communication through the Internet." WPPT 1996, available at http://www.wipo.int/eng/general /copyright.wppt.htm.

[303] Matthew Fagin et al., Beyond Napster: Using Anti-Trust Law to Advance and Enhance Online Music Distribution, 8 B.U.J.Sci. & Tech.L. 451, 538.

[304] Tricia Moham, Freedom v. Control: Private Copying and Technological Protection Measures, available at http://theorem.ca/~yaacov/tricia_mohan.php (visited Nov. 23, 2003).

are collected by sister societies and sent to ALCS for onward distribution.[305] Canada imposes a levy on blank audio recording device to compensate authors and other right owners for private use. To adapt to the digital market, effective January 1, 2001, CD-RW and CD-RW audio and MiniDiscs are levied, or have increased levy rates. The Canadian Private Copying Collective (CPCC) is designated as the collecting body for the private copying levy, and for distributing the funds generated by the levy to the collective societies. The proceeds from the tax are allocated to authors, performers and product makers. The member collectives of CPCC consist of agencies representing right owners but not consumers.[306] The United States does not have a comparable blank media levy as provided in France or Canada, whose legislation made no distinction between analogue and digital technology.[307] The AHRA allows digital copying for personal use as long as manufacturers and distributors of digital recording devices and recording medium pay royalties to a fund for all products imported and distributed in the United States.[308] The fund is then distributed to recording artists, copyright owners, music publishers, and music writers. However, the coverage of AHRA was interpreted to exclude computer hard drives, therefore private copying of copyrighted works distributed on the Internet is not compensated by the blank media levy mechanism.[309]

---

[305] Blank Tape Levy (private copying), available at http://www.alcs.co.uk/royalties/main.asp?tablename=royalties_tape (visited Nov. 23, 2003).

[306] The organizations include: Canadian Mechanical Reproduction Rights Agency (CMRRA) , Neighbouring Rights Collective of Canada (NRCC) , *Société de gestion des droits des artistes-musiciens* (SOGEDAM) , Society for Reproduction Rights of Authors, Composers and Publishers in Canada (SODRAC) , and Society of Composers, Authors and Music Publishers of Canada (SOCAN). Copyright Board of Canada: Copyright Board's Decision, Private Copying 2001-2002. available at http://www.cb-cda.gc.ca/news/c20012002fs-e.html (visited Nov. 23, 2003).

[307] In the United States, only digital tapes are subject to the blank media levy. See Joseph S. Papovich, NAFTA's Provisions Regarding Intellectual Property: Are They Working as Intended? – A U.S Perspective, 23 Can.-U.S. L.J. 253, 259.

[308] §1004(a)(1) of the Audio Home Recording Act provides: "The royalty payment due under section 1003 for each digital audio recording device imported into and distributed in the United States, or manufactured and distributed in the United States, shall be 2 percent of the transfer price. Only the first person to manufacture and distribute or import and distribute such device shall be required to pay the royalty with respect to such device." 17 U.S.C. §1004(a)(1) (1992).

[309] Recording Indus. Ass'n of Am. v. Diamond Multimedia Sys., Inc., 180 F.3d 1072, 1076 (9th Cir. 1999).

It seems natural that the other alternative remuneration is through the market force itself, i.e. entrusting private copyright owners the power of self help. This is accomplished by the pay per view/listen scheme under the rights management system. Earlier sections have examined ECMS to detail, the point to add here is that proponents credit at least two advantaged of ECMS over the compulsory fixed levy: (1) It takes full account of the degree of use by establishing the link between the loss suffered by copyright owners and the act of private copying; and (2) it would prevent consumers from paying twice for their personal use, i.e., once in respect of an act of electronic commerce and secondly via a levy on the recording medium. Further, it is argued that the technological measures would give the creator better control over his work to the extent that he himself can control the number of copies he authorizes, receiving a remuneration exactly in proportion to this authorization. "This true price of the work will be at the heart of the link between the consumer and the author, and would help to raise awareness of the value of intellectual property."[310]

Nevertheless, if the administrative levy system is short of democratic legitimacy, the one-handed ECMS similarly raises the question of legitimacy of private ordering in the individualized license scheme: Have the copyright holders reached agreement among themselves? Would consumers accept such measures had the terms been negotiated at arm's length? There have been numerous complaints about the intrusion of fair use and first sale doctrine on account of the conditions inserted in the code of, or shrinkwrap contracts in accompany with the ECMS, as discussed earlier. More nuanced balance is called for to ensure new equilibrium of welfare of all stakeholders on the market.

Taking digital distribution of music for example, roughly four categories of stakeholders can be identified. First, the major record companies own most of the copyright to the sound recordings of music and control most of the distribution channels for music by selling CDs to record store chains. Second, artists own the underlying music

[310] Marc Mossé, Author's Rights and Exceptions for Private Copying in the Age of the Internet, available at http://droit-internet-2001.univ-paris1.fr/pdf/ve/Mosse_EN.pdf (visited March 28, 2004).

compositions who generate income mainly from the enforcement of the reproduction, distribution and performance rights. While they artists are similarly concerned with protecting their rights, some are frustrated with the unfair leverage resulting from the monopoly of record companies and welcome technologies that potentially may change the status quo. Third, technology developers and providers like Napster and Grokster are creating new access to music, and who are burdened with license fees that must be paid to provide content for the service. Fourth, consumers support the above entities by purchasing music and using new technologies. While they are supposedly have nothing to lose with the novel music distribution channels that at least reduces purchase price, if not for free, they are also concerned with protecting user freedom traditionally enjoyed under the fair use doctrine but which may be threatened by both the ECMS and more stringent copyright law. Now the control battle seems to be unbalanced in favor of only the first category stakeholder, major record companies who has the monopoly over price setting and who designs the code of ECMS in collecting remuneration for online use. Not only consumers are alienated by the over-extensive use of ECMS in addition to the price scheme set unilaterally on the analogue world, the other copyright holders – composers and performers doubtfully benefit from the scheme at all. The current power structure in the music industry is such that record companies have used questionable tactics in distributing royalties to artists. Suppose, for example, the unfairly-paid artists can instead benefit from alternative distribution services like that of Napster by collecting a royalty directly from individual users, arguably corporate giants (who owns copyright to the sound recordings) will have a much weaker claim to the digital property then, and the "effect on the market" analysis will turn out to be over-limited as to protect the system of production but not the individual author. If such is the case, would Napster be outlawed for harming the potential market of a section of copyright owners but not that of the creative authors?

Therefore, it is the dimension of industrial production of copyright law that is at the center of focus of current Internet copyright debate. The Napster litigation not only raises moral issues such as whether copyright should kill technological innovation, but more

profoundly, the request for a more just and fair compensation system in the spirit of copyright law in the digital age. Whatever remuneration system is chosen by various governing bodies, it is time to leverage the market forces that are presently threatening fair use into positive developments that can assure its future. Instead of trying to control consumers' behavior with copyrights and technological protection measures that are inevitably circumvented, the industry should be trying to develop new economic models that will actually appeal to consumers' tastes, and to find an economic model that strikes a balance between consumers' need for flexible, convenient access to works and content owners' need to make a profit. The ultimate purpose for legislative intervention should be to increase individual creation, not to maximize profit for a small section of monopoly holders by maintaining the *status quo*.

# CHAPTER IV THE "BIGGER PICTURE": FREE MARKET AND THE INFORMATION SOCIETY

## 4.1 CODE AND THE STATE

This thesis is not to be ended in a limited discussion of certain concrete legal rights that the Internet and digital technology have so far influenced. We live in an interesting time that machine automation takes configuration of people's everyday life. The Internet collapses our traditional notions of location and the significance of geography for sovereignty and regimes of law. Search of personal information is just a matter of click of mouse; with the increasing digitalization of documents and on-line profiling, data venders collect and process such valuable assets for marketing purpose and for licensing to third parties. User license for digital content has become the rule on the Internet through the click-wrap contract and technological measures that constitute the electronic copyright management system (ECMS). In his brilliant book "Code, and other Laws of Cyberspace," professor Lawrence Lessig observed that the regulation of behavior in cyberspace is imposed, not through a statute, but primarily through the code of software, technical protocols, and network architectures. He argues that, in cyberspace, code is particular powerful because it operates so directly. Code can more subtly control and discipline behavior.

There are two assumptions about the governance of code. One is that code is value neutral, and is capable of growing up as the result of market interactions, that is, without a governmental regulatory structure other than a general state-backed background regime

of property and contract.[311] Like the flip side of a coin, the other assumption relies on the fact that no territorially-based jurisdiction is powerful enough to exert sole control over the Internet, consequently the efficacy of cyberspace regulation turns mainly on the self-ordering of its constituents, that is, information users, content providers, software developers, service providers and other intermediaries.

One major task of the thesis is to respond to these two faulty assumptions about the Internet governance. From the discussion of privacy enhancing technologies to electronic copyright management systems, we can see that more subtle problems arise from private implementation of code that constrains behavior. Code can directly affect market structure by making personal information as a valuable and exchangeable commodity, or by limiting the public sphere of copyright law in the digital medium. The architecture of code may conflict with the rules established by the legal system, as exemplified by the copyright preemption debate over the ECMS. Furthermore, code is buttressed by law for its validity and enforcement, when legislatures around the world add an extra layer of anti-circumvention law above the technological fences built by content providers. The bigger picture is portrayed by Lessig by identifying the four "modalities" of regulation in cyberspace: Law is an ex post sanction by the state. Social norms are ex post sanctions imposed by a community. Markets offer the pricing structure. And Code, the software and hardware that makes cyberspace, combines and interacts with the other three modalities in its surreptitious regulation of cyberspace, as well as the real space.[312] While regulation modalities like law and social norms are more obvious targets for people to evaluate their regulatory legitimacy, Lessig cautions, as most technorealists do, about the often-ignored value choice in code:

---

[311] Margaret Jane Radin & R. Polk Wagner, The Myth of Private Ordering: Rediscovering Legal Realism in Cyberspace, 73 Chi.-Kent L. Rev. 1295, 1307 (1998).

[312] Lawrence Lessig, *Code: And Other Laws of Cyberspace* (New York: Basic Books, 1999), p.88-93.

> "We should worry about a regime that makes invisible regulation easier; we should worry about a regime that makes it easier to regulate. We should worry about the first because invisibility makes it hard to resist bad regulation; we should worry about the second because we don't yet have a sense of values put at risk by the increasing scope of regulation."[313]

To the extent the "private" ordering in cyberspace depends on rules of property and contract, it is relying upon norms created and enforced by the state. In fact, as James Boyle pointed out years ago, cyberspace self-governance implicitly supports indirect government regulation of the Internet. Governments can shape and develop the Internet through "privately developed, materially biased, technological methods of surveillance and censorship."[314] A state's effective enforcement mechanism does not have to touch all actors as long as it touches actors who can impact everyone else's behavior. The obvious strategy is to "seek out private actors involved in providing Internet services who are not quite as mobile as the flitting and frequently anonymous inhabitants of cyberspace."[315] In particular, the Untied States government has frequently eschewed direct regulation in favor of subsidizing filtering software and hardware to achieve privately what it lacks the constitutional power to achieve directly.[316] Rights are contested in cyberspace, not because they are novel issues unprecedented in real space, but rather because they expose a grey area the interaction of new technology with the real space requires a clearer resolution. For instance, to what extent private copying and sharing of copyrighted material on the Internet are to be outlawed, by shifting the burden of surveillance to third-party intermediaries? What will be a "reasonable" expectation of privacy in view of the massive digital date mining and profiling as prevalent commercial practice? "The fact that the background regime becomes contentious so often when it must come into play in order to enforce a contested interaction is the reason why the libertarian 'minimal state' cannot be put uncontroversially into practice in order to create a background scheme of

---

[313] Lessig, p.99.

[314] James Boyle, Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors, supra note 42.

[315] Id.

[316] Justin Hughes, The Internet and The Persistence of Law, 44 B.C.L.Rev. 359, 368.

certain and strong property rights."[317] In the end, almost unavoidably it is the state, rather than the market or code, that is entrusted with the task to define such contentious area, or at least in some respects of it.

## 4.2 MAPPING: CONCEPTUALIZING PRIVACY AND COPYRIGHT IN DIGITAL AGE

Recognition of state power in regulating cyberspace directs us back to Judge Esterbrook's metaphor "law of the horse."[318] No one theory is suitable for all cases of contested rights. The purpose of legal metaphor is to reconstruct the notion of rights to facilitate more nuanced balance in legal policy. States (mostly developed countries with mature commerce and legal systems) are in fact mapping real space law against relationships in cyberspace.[319] The definition of rights and obligations in cyberspace, not surprisingly, involves both top down implementation of rules through legislative enactment or judicial decision and bottom up rule making process and development of customs based on the concepts of contract and property law of that jurisdiction.

However, translation[320] of real space law is a process that decides the present in the past, which brings concerns for the value choice behind certain particular metaphor. While some sort of legal solutions tailored to the cyberspace will bring clarity and predictability to the rules attending cyberspace activity, some policy underlying real space law might not be apt application to cyberspace conduct. Existing legal rules are designed to enforce laws within a given technology. "As the form of information changes from something

---

[317] Radin, supra note 312.

[318] Frank H. Easterbrook, Cyberspace and the Law of the Horse, supra note 51.

[319] See Anne Wells Branscomb, supra note 48, for the cases of metaphors that previous case law has been applied to the computer-mediated communication.

[320] The technique that is familiar to American constitutionalists in cases where constitutional law confronts changed circumstances, called 'translation' by Lessig. 'Its aim is to choose in a way that is faithful to the choices of the past, to translate the commitments of the past into a fundamentally different context.' Lessig, supra note 313, p.109.

tangible to something electronic, changes will occur in legal institutions and processes that have been oriented around particular physical spaces, and in legal concepts and doctrines that have depended upon a relationship with a particular space."[321] If we probe into the background factual assumptions about the existing law, the ambiguous value in the original context will loom out as questions of political choice. Therefore Lessig observes, "The institutions most responsible for articulating constitutional values today are the courts. My sense is that they will step back because they feel...that these are new questions that cyberspace has raised. Their newness will make them feel political, and when a question feels political, courts step away from resolving it."[322] Metaphors of law promote *order* rather than *justice*.[323]

Reconceptualizing the right to privacy and copyright in cyberspace thus helps better understanding of the power structure of current Internet regulation; moreover, it pushes popular attention to focus on the ends rather than the means of regulation: for what purpose are we addressing certain concerns associated with cyberspace conduct? Is the regulatory objective to main the *status quo*, or to reach a new balance of interests among various stakeholders?

### 4.2.1 PRIVACY

The mapping of real space concept of privacy employs a deeply flawed rhetoric. Privacy in the pre-digital world was a clear-cut status or domain. Information is either private – the violation of which incurs tort liability and the exploitation of which promises economic compensation, or public – scattered in accessible public records and free for

---

[321] M. Ethan Katsh, Cybertime, Cyberspace, and Cyberlaw, 1995 J. Online L. 1, paragraph 11.

[322] Lessig, supra note 313, p.120.

[323] Milner S. Ball, *Lying Down Together: Law, Metaphor and Theology* (Durham, North Carolina: Duke University Press, 2000), p.22.

every interested party to check out. The "secrecy paradigm"[324] has been completely outmoded with the advent of digitization and Internet connection. The dichotomous notion of public and private collapses when an ordinary citizen with a search engine can search another citizen's personal information from online public records, let alone date marketing companies offer more complete personal profiles for sale, most time unknowing to the identified citizen himself. It is the degree of accessibility of information rather than particular categories of the sources, and the totality of the aggregated information rather than the scattered bits, that poses threats to individuals.

A holistic approach is thus needed to understand privacy in the new context. With the aggregation and profiling reality, people's reasonable expectation of privacy should rest on the limit of the degree of accessibility of information. At the same time, the center of debate about regulatory preference should shift: rather than stuck on the alternatives between industry self-regulation and formal legal response from the state, it is more imperative to consider the whole picture of data profiling, and seek to regulate both the public and private interaction concerning the use of personal information. It is not that comparing the two representative Internet privacy regulation models – the EU strict comprehensive regulatory regime and the US "self-regulation" model – is practically of marginal help on account of different cultural and market conditions of the two regimes. The binary notion of the private as opposed to the state simply misses the purpose of regulation by replacing the means as the central controversy, which in fact, is not.

The comparison of U.S. and EU models shows not only a methodological divergence but more importantly, the underlying purpose of the Internet privacy regulation. The American preference of market-based solution to personal data protection can be traced back to the lack of clarity in this country about the interest that individuals have in information about themselves. Is it a commodity interest, a consumer protection interest, a personal dignity interest, a civil right interest, all of the above, or no interest at all? As

[324] See generally, Daniel J Solove, Access and Aggregation: Public Records, Privacy and the Constitution, 86 Minn.L.Rev. 1137, 1170-71.

Pamela Samuelson observes, one of the strengths of the EU Directive is that the regulatory regime it embodies is consistent with its underlying conception of information privacy as a fundamental human right. Without a coherent conception about the nature of a person's interest in personal data, it is difficult to design a legal regime to protect this interest appropriately.[325]

Probing of ends necessarily leads to analysis of means. Like the copyright management system, privacy control can also implement code that combines technological measures and the institutional backup, that is, develop privacy-enhancing technologies (PET) and amend commercial access and use restriction law in general. The law would empower individuals to negotiate over their privacy rights and entitle them to privacy as a default. A property rule is proposed in substitution of the liability rules underlying the common law privacy rights. While the liability rules merely compensate after privacy is invaded, a property regime requires negotiation before taking, so it give the individual more choice instead of encouraging transfer. "That is the property's purpose: it says to those who want, you must negotiate before you can take."[326] It also declares the distrust of industry self-regulation, as "privacy polities tend to be self-indulgent."[327] The argument that the market is already providing the optimal level of privacy protection fails because there are vase inequalities in knowledge and much data collection is clandestine. The aggregation problem severely complicates the valuation process. A market solution will also experience difficulty because information transactions are often grossly unfair and unequal. [328]

But we also need to be wary of the normative implication for propertizing privacy. Will privacy become a new branch of intellectual property, as Pamela Samuelson suggests?

---

[325] Pamela Samuelson, Privacy as Intellectual Property? 52 Stan.L.Rev. 1125, 1171.

[326] Lessig, supra note 313, p. 160-161.

[327] Daniel J. Solove, Privacy and Power: Computer Databases and Metaphors for Information Privacy, 53 Stan.L.Rev. 1393, 1451.

[328] Id., 1454.

The proposal to commodify personal information in essence conflicts with the purpose of privacy law to ensure individual integrity and autonomy, "in part because a key mechanism of property law, namely the general policy favoring free alienability of such rights, would more likely defeat than achieve information privacy goals."[329] Considerable reasons exist to doubt that the current privacy market functions well. Over-zealous entrepreneurs tend to maximize information disclosure and sharing while having little incentive to take measures to protect consumer data. The greatest problem is not consumer does not have an option to trade his personal information. What is troubling is the unfettered ability of companies to do whatever it wants with this information. Personal information databases are often a company's most valuable asset and could be sold to third-parties at bankruptcy to pay off creditors.[330] The government's regulation of the privacy market should focus on both the valuation process and after-sale surveillance, so that information asymmetries can be curbed and attempts to bargain around objectionable norms can be facilitated.

### 4.2.2 COPYRIGHT

In a disturbed equilibrium, the rights of different parties in a copyright regime are determined by the intricate play of the private ordering and law.[331] Right-holders stress that stronger protection, be it technological or legal measures, is essential because copyright is vulnerable in the digital environment; end-users, on the other hand, argue for more public domain in cyberspace that they used to enjoy in the analogue world, because over-restrictive private ordering is menacing the very purpose of copyright law

---

[329] Samuelson, supra note 326, 1125.

[330] See Susan Stellin, Dot-Com Liquidations Put Consumer Data in Limbo, N.Y.Times, Dec.4. 2000, at C4.

[331] In the context of digital works, Trotter Hardy has argued that the scope of intellectual property protection afforded the publisher of a copyrightable work is a function of four things. First is the extent of the protection afforded by the formal, public legal regime. Second is the extent to which the publisher can secure protection via bilateral contract. Third is the sophistication of the technology available to inhibit unauthorized reproduction of the work (anti-free riding technology). Finally, the fourth is the sophistication of reproduction technology itself (the technology of piracy). See Trotter Hardy, Contracts, Copyright and Preemption in a Digital World, 1 Rich. J.L. & Tech. 2, available at http://www.urich.edu/<<tilde>>jolt/v1i1/hardy.html.

recognized in most jurisdictions – the promotion of literature, artistic work and useful arts. As Ejan Mackaay forceful asks, "If everything is "up for grabs" by whoever can come up with a fence for it, will we not slide into "undue information lock-up?"[332]

Current private ordering in the digital environment is in fact an expansion of copyright. Limitations based on traditional principles of copyright protection are not only necessary, but essential, although many agree that it would be simply too facile to recommend a mere restatement of existing limitations and exemptions in digital (or media-neutral) terms. But in any case, they serve to the right holders' exploitation rights. They are the tools for "fine-tuning" the rights protected under copyright[333], and therefore, are an integral part of the copyright regime, an essential "balancing tool", instead of mere exceptions to a rule. Further, consumer rights and technology advocate groups are increasingly concerned with the broader implication to information market brought by anti-circumvention laws: whether a technological innovation should be penalized as "illegal conduct" so as to protect right owners' ECMS depends on stakeholders' perspective. In an effort to protect copyright on the Internet, it is indispensable to consider the underlying purpose and effect of the measures to be taken: Is continuance of the *status quo* justified in view of the changed circumstances? Will the development of technology and compensatory mechanism provide opportunities to create a more efficient and just information market, as did the invention of video tape recorders?

It is intriguing that while the US has a broader extent of statutory copyright limitations, the dominance of private power in its information market coupled with a neoclassical policy preference restricts the effects of such limitations and shrinks the scope of users' rights. In contrast, while the Europe has a strong inclination to the strong author's rights and restricted copyright limitations, the policy consideration for harmonizing the internal

---

[332] Ejan Mackaay, The Economics of Emergent Property Rights on the Internet, in P. Bernt Hugenholtz ed. *The Future of Copyright in a Digital Environment*, supra note 212.

[333] P. Bernt Hugenholtz , Copyright Exemptions: Towards Extinction?, in Rights, Limitations and Exceptions: Striking a Proper Balance, IFLA/IMPRIMATUR Conference, 30-31 October 1997, Amsterdam, The Netherlands.

market and the traditional limits on contract subject the "digital privatization" to a relatively more definite and pro-user copyright limitations. The interplay between copyright law and regulations on market power complicates the real degree of limitations to the increasingly privatized information highway in different regions.

One may ask, is there any common denominators of copyright limitations on the Internet, an increasingly interconnected, borderless space? Can limitations to copyright be harmonized on an international level? Common denominators do exist, as revealed by comparative study of existing national laws. In many cases, limitations are drafted as outright exceptions to the copyright owner's exclusive rights. Sometimes, limitations take on the form of statutory or compulsory license schemes. Most copyright acts contain limitations for the following purposes: personal use, news reporting, quotation, criticism, science, classroom teaching or other educational uses, archival storage, library and museum privileges, administration of justice, other government uses. In addition to these "dedicated" exemptions, copyright laws of the Anglo-American tradition provide for general fair use or fair dealing provisions. Further more, Article 9 (2) of the *Berne Convention* and Article 13 of the *TRIPS Agreement* take a three-step test to impose certain limits on the freedom of Union countries to allow exemptions. And the WIPO Copyright Treaties contain similar language. Thus, new limitations would only be introduced (a) in a special case; (b) if they do not conflict with a normal exploitation of the works, performances or phonograms, respectively; and (c) if they do not unreasonably prejudice the legitimate interests of the owners of rights.

This been said, harmonization of limitations in the digital environment is at most a well-intentioned hope. Even if existing minimum Berne rights adapt to the digital environment, applying the existing Berne limitations is problematic since they are vague and open-ended, subject to further defining crucial terms as "normal exploitation", "unreasonably prejudice", and "legitimate interests", etc. In addition, the right of distribution is variably subject to the first-sale doctrine or exhaustion, and it is not clear

whether or at what point in network dissemination this right or limitation should come into play. As long as Berne countries are free to characterize rights at different phases of network dissemination, their respective legal systems and cultures will push their lawmakers to limit these rights, or provide exceptions to them, differently. There seems to be little choice, at this juncture in Berne harmonization, but to let law-makers follow their respective methodologies of characterizing rights and, accordingly, of conditioning the scope of these rights.[334]

With cases like Napster and follow-up companies employing controversial P2P technologies, there will be a continuing technological struggle between content providers, their customers, their competitors and future creators. The shaken copyright kingdom still provides some relief for right holders to claim in cyberspace. Digital fences can be backed up by anti-circumvention laws. Third-party intermediaries, such as ISPs, can be listed as semi-public copyright law enforcement agencies with various degree of expansion of secondary liabilities. Nevertheless, when one witnesses the strong outcry by copyright owners (who worry about the unbridled piracy online) and the massive civil disobedience by end-users (who think there's nothing wrong with copying digital content for personal use or sharing with others), one may question the legality of the present system that favors the right holders. In fact, many people do not share the value of overprotecting copyright in the digital world at the expense of users and other interested parties. It is even dubious that the strictest copyright law would benefit the creators (that is, artists, authors) in particular. Copyright law, after all, is based on the assumption that protection spurs invention and creation, that is, by an individual author (most case) or by entrepreneur through employment of authors. In the modern world copyright protects a system of production rather than the individual author. "It is copyright in its industrial capacity that is the second dimension of the law."[335] Furthermore, there is difference

---

[334] For example, while legislators in Europe might limit some rights definitionally by applying them only to "public" communication or access, judges in the United States might experiment with the exception of "fair use" for all rights on the network. See Paul Edward Geller, Conflict of Laws in Cyberspace: Rethinking International Copyright in a Digitally Networked World", 20 Colum.-VLA J.L. & Arts 571.

[335] Mackaay, supra note 333.

between real property and intellectual property. "The law has a reason to protect the rights of authors, *at least insofar as doing so gives them an incentive to produce.* With ordinary property, the law must both create an incentive to produce and to protect the right of possession; with intellectual property, the law need only create incentive to produce."[336] This distinction affects fundamentally the scope of the exploitative rights that copyright owners should be granted. Perhaps the right question to ask is: does copyright law provide an incentive for corporations to innovate? There is need to consider whether it is really in the public's interest to prohibit private copying and give content providers complete control to authorize every use of their work, or whether consumers should have the right to use legally acquired works more flexibly and simply provide compensatory remuneration.

### 4.2.3 The Right Level of Abstraction

The difficulty in formulating an issue in cyberspace arises because of the tension between conflicting desires. Information plays a central, if not defining, role in both the public and private worlds of the liberal political vision. In the privacy domain of family and home, information is most commonly defined as "privacy." Information economics also views the market as "private," an invisible hand capable of self-sufficiency that justifies freedom from state intervention. In the public world of politics, defined in the liberal vision by the information-centered ideas of debate, exchange, and decision – the free flow of information is a prerequisite for atomistic citizens first to form and then to communicate their subjective preferences in the great marketplace of ideas. At the same time, the availability of information to citizens is thought to be as important a check on governmental activity as that provided by the rule of law. Information, loosely defined, is central to our conception of the family, the market, and the democracy. There are tensions "between spheres" in the roles we expect information to play.[337] While

---

[336] Lessig, supra note 313, p.140.

[337] James Boyle, *Shaman, Software, and Spleens: Law and the Construction of the Information Society* (Cambridge: Harvard University Press, 1996), p.28-29.

individual desires seclusion from public intrusion of his personal information, exclusive control of such information is antipathy to the needs of democratic society. Similarly, while copyright owners have vested interests in protecting the fruit of their creations, such interests are not absolute as to be independent from public domain. In an open, transparent democracy, there is vertical relationship between the individual and the state for access to personal information from the government. However, horizontal relationship between private citizens for information has not been recognized as a property right except limited copyright limitations set by the law. By naming one right or entitlement to information we necessarily implicate an overlay or two or more sets of conflicts, in the matrix of conflicts between the theories of justice that are applied to the family, the market, and the liberal state.

This conflict, consequently, requires a right level of abstraction in characterizing the issue raised. As to the contested privacy and copyright in cyberspace, the teaching is that we should not merely look at the "law of horse" itself by a mechanical mapping of real space regime to Internet activities. Instead, it is conducive to form a bigger picture of the architecture of the Internet, with a progressive perspective of information society in general. "Reliance on essentialized notions of 'contract,' 'market,' and 'property' elides important empirical and policy questions about the extent of the monopoly that society should afford creators of digital works – questions that a more sophisticated model would consider." [338] Rather than undertaking haste endeavor to extend familiar laws and regime into the new territory, we need to consider questions like whether the existing consumer mass market offers the best forum for defining information policy and establishing the cope of entitlements in digital works, what is the relationship between creative and informational works and social welfare, and what are the potential asymmetries of power that may inhere in technologically-mediated transactions in usage rights, etc. Often a "right" question promises half success of the problem solution.

---

[338] Julie E. Cohen, Lochner in Cyberspace: The New Economic Orthodoxy of "Rights Management", supra note 69.

## 4.3 LIBERTARIAN MEANS OF GLOBALIZATION?

Over the last few years the Internet is no longer what it was in the 1970s or 1980s; it has become a contested space with considerable potential for segmentation and privatization. "The social and economic fabric of the information society has been unevenly woven by the warp of commercial innovation seeking competitive advantage and the weft of social action militating its realization. Thus the technological development driving the current changes can only be understood when placed within a wider political context of an unequal and changing pattern of power relations."[339] Digital space has emerged not simply as a means for communicating, but as a major new theater for capital accumulation and the operations of global capital.[340]

It is not surprising that, despite the "global" rhetoric of the Internet, domestic implementation of new legal norms by the United States and the European Union has played a significant role in shaping the actual content of international legal norms. The provisions of the DMCA and the European Union Copyright Directive on "technological measures" are sufficiently consistent that they de facto fill the "content" of these WCT/WPPT legal norms, although a few countries, like Burkina Faso and Australia, believe that they can meet the treaty obligations with much less normative content.[341] Because the initial research and utilization of the Internet were predominantly by the American, American courts were usually the first to address novel legal issues about the Internet (although parallel fact patterns have quickly appeared in other countries), grounded, naturally, on the legal concepts and values of this country. Even today, novel cyberlaw problems statistically arise first in either the United States or another common-law jurisdiction. Survey information for 2002 puts Americans at 42.65% of Internet traffic, dwarfing number two China (6.63%) and number three Japan (5.24%). Adding Britain, Canada, and the United States, a bare majority of Internet traffic still comes from

---

[339] Brian D. Loader, supra note 18, p.7.

[340] Saskia Sassen, On the Internet and Sovereignty, 5 Ind. J. Global Legal Stud. 545, 1998.

[341] Hughes, supra note 317, 376.

common-law, English-oriented countries (50.52%).[342] This reality of the Internet has forced and will continue to produce significant amount of convergence of legal system, because the interconnectivity of the Internet poses the same or similar problems to the geographically bordered jurisdictions. Notably, online businesses desire a coherent or uniform set of rules to facilitate movement of goods widely through the Internet, which form strong support for the private ordering of *lex informatica.*

The prevalence rhetoric of private ordering, that cyberspace should avoid coercive rules laid by sovereign governments and welcome a laissez-faire network of contracts and customary norms, covers the factual assumptions of these norms. To the extent the "private" ordering in cyberspace depends on rules of property and contract, it is relying upon norms created and enforced by the state, that is, the dominating legal cultures of the developed countries whose norms have already supplanted the formative-stage international law. The present debates over the definition and scope of various private rights to information, though mainly through domestic courts and academic forum, are in fact foredawn of future international arena of political and economic control battle between the information abundant and the information poor. While it is hard to predict, at this moment, to what extent harmonization will be achieved among nation-states, it is relatively certain to say that the Internet politics is heading for a libertarian globalization that favors the free market and private ordering.

[342] Id, 361.

# BIBLIOGRAPHY

## CHAPTER ONE


Edward Twitchell Hall, *Beyond Culture* (Garden City, New York: Anchor Press, 1976).

Thomas S. Kuhn, *The structure of scientific revolutions* (2rd ed., Chicago: University of Chicago Press, 1970).

Brian D. Loader, *Cyberspace Divide: Equality, Agency, and Policy in the Information Society* (Routledge, N.Y. 1998).

Mike Featherstone & Scott Lash, eds., *Spaces of Culture: City, Nation, World* (London: SAGE Publication Ltd, 1999).

Claire Cutler, Virginia Haufler, and Tony Porter, eds., *Private Authority and International Affairs* (State University of New York Press, 1999).

Milner S. Ball, *Lying Down Together: Law, Metaphor and Theology* (Madison, University of Wisconsin Press, 1985).

Egbert J. Dommering and P. Bernt Hugenholtz eds., *Protecting the Fact: Copyright, Freedom of Expression and Information Law* (Deventer & Boston: Kluwer Law and Taxation Publishers, 1991).

H. L. A. Hart, Legal Rights, in *Essays on Bentham: Studies in Jurisprudence and Political Theory* (Oxford: Clarendon Press, 1982).

O. W. Holmes, Jr., *The Common law* (Boston: Little, Brown, and Company 1881).

Michael Heim, *Electronic Language: A Philosophical Study of the Word Processing* (New Haven: Yale University Press, 1987).

George P. Landow, *Hypertext: The Convergence of Contemporary Critical Theory and Technology* (Baltimore: The Johns Hopkins University Press, 1992).

H.J. Chaytor, *From Script to Print* (Cambridge, England: Heffer and Sons, 1945).

CHAPTER TWO

Carole A. Lane, *Naked in Cyberspace: How to find personal information online* (CT: Pemberton Press, 1997).

Ann Cavoukian, *Who Knows: Safeguarding Your Privacy in a Networked World* (Random House of Canada, 1995).

Peter P. Swire and Robert E. Litan, *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive* (Brookings Institute Press 1998).

James Madison, *The Complete Madison* (S. Padover ed. 1953).

James Rule et al., *The Politics of Privacy: Planning for Personal Data Systems as Powerful Technologies* (New York: Elsevier, 1980).

Schoeman eds., *Philosophical Dimensions of Privacy* (Cambridge University Press, Cambridge, England, 1984).

Priscilla M. Regan, *Legislating Privacy: Technology, Social Values, and Public Policy* (Chapel Hill & London: The University of North Carolina Press, 1995).

Privacy Protection Study Commission, *Personal Privacy in an Information Society* (Washington, D.C.: Government Printing Office, 1977).

Terry Thomas, *Privacy & Social Services* (Aldershot, Hants, England: Arena, 1995).

Wacks, R., *Personal Information* (Oxford: Clarendon Press, 1989).

Philip E. Agre and Marc Rotenberg eds., *Technology and Privacy: The New Landscape* (Cambridge, Massachusetts: The MIT Press, 1997).

Colin Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (Ithaca: Cornell University Press, 1999).

Ellen Alderman and Caroline Kennedy, *The Right to Privacy* (New York: Alfred A. Knopf, 1995).

Mary P. Mack, *Jeremy Bentham: An Odyssey of Ideas*, 1748 – 1792 (London: Heinemann, 1962).

Laurence Tribe, American Constitutional Law, § 15-16 (2d ed. 1988).

Colin J. Bennett and Rebecca Grant eds., *Visions of Privacy: Policy Choices for the Digital Age* (University of Toronto Press, 1999).

William E. Bandon, III, *Summary of Technological and Self-Regulatory Responses to Internet Privacy Concerns*, NETLAW 97, American Conference Institute.

Anne W. Branscomb, *Who Owns Information?: From Privacy to Public Access* (Basic Books, 1994).

U.S. Department of Commerce, *Privacy and Self-regulation in the Information Age*, 1997.

Christopher Rowe, *People and Chips: The Human Implications of Information Technology* (3rd ed. London; New York: McGraw Hill. 1996).

CHAPTER THREE

*Copyright and Digital Media in a Post-Napster World*, GartnerG2 and The Berkman Center for Internet & Society at Harvard Law School.

*Protection of Copyright Management Information*, Institute for Information Law, Amsterdam, Dec. 1998.

*Contract and Copyright Exemptions*, Institute for Information Law, Amsterdam, 1999.

M Dellebeke ed., *Copyright in Cyberspace,* ALAI Study Days Amsterdam, 4-8 June 1996, Amsterdam: Cramwinckel, 1997.

P. Bernt Hugenholtz ed., *The Future of Copyright in a Digital Environment* (The Hague: Kluwer Law International, 1996).

Lucie Guibault, *The Exceptions and Limitations to Copyright: Limitations Found outside of Copyright Law*, ALAI Study Days General Report, 1997.

Commission of the European Communities, *White Paper on Growth, Competitiveness, Employment: The Challenged and Ways forward into the 21st Century*, COM (93) 700 final, Brussels, 5 Dec. 1993.

Pierre Sirnelli, *Workshop on Implementation Issues of the WIPO Copyright Treaty (WTC) and the WIPO Performance and Phonograms Treaty (WPPT)*, Geneva, December 6 and 7, 1999.

CHAPTER FOUR

Lawrence Lessig, *Code: And Other Laws of Cyberspace* (New York: Basic Books, 1999).

Milner S. Ball, *Lying Down Together: Law, Metaphor and Theology* (Durham, North Carolina: Duke University Press, 2000).

P. Bernt Hugenholtz ed., *The Future of Copyright in a Digital Environment* (The Hague: Kluwer Law International, 1996).

*Rights, Limitations and Exceptions: Striking a Proper Balance*, IFLA/IMPRIMATUR Conference, 30-31 October 1997, Amsterdam, The Netherlands.

James Boyle, *Shaman, Software, and Spleens: Law and the Construction of the Information Society* (Cambridge: Harvard University Press, 1996).