8 Va. J.L. & Tech. 6 (2003), *at* http://www.vjolt.net

VIRGINIA JOURNAL *of* LAW *and* TECHNOLOGY

UNIVERSITY OF VIRGINIA	SUMMER 2003	8 VA. J.L. & TECH. 6

The Invisible Handshake: The Reemergence of the State in the Digital Environment

Michael D. Birnhack[*] and Niva Elkin-Koren[**]

[*] Assistant Professor, University of Haifa, Israel. J.S.D., 2000, New York University; LL.M., 1998, New York University; LL.B., 1996, Tel Aviv University.

[**] Associate Professor, University of Haifa, Israel. S.J.D., Stanford University, 1995; LL.M., 1991, Harvard Law School; LL.B., 1989, Tel Aviv University.

We wish to thank Yochai Benkler, Robert Brauneis, Julie Cohen, Amitai Etzioni, Michael Froomkin, Ellen Goodman, Irit Haviv-Segal, Orin Kerr, Neil Netanel, Dawn Nunziato, David Post, Joel Reidenberg and the participants at the Public Design workshop at NYU School of Law, Rutgers Law School Faculty Colloquium, the Dean Dinwoodey Center for Intellectual Property Studies at George Washington University Law School, the Telecommunication Policy Research Conference (September 2002), and the joint colloquium of the faculties of law at Haifa University and Tel Aviv University, Israel. We are grateful for able research to Rachel Aridor, Avihay Dorfman, and Edo Eshet. All Web sites cited were last visited February 2003.

I. Introduction

1. Back in the 1980s and 1990s the information environment was associated with a general notion of the decline of the State.[1] The borderless nature of the Internet challenged the use of force by national states, which normally enforce their laws within their territories. The Internet was conceived as a decentralized network that derived its resilience from the absence of a central command, and seemed hard, if not impossible, to govern. Many commentators noticed the introduction of alternative private ordering schemes,[2] describing the Internet as a post-national situation,[3] either mourning or celebrating what they perceived as an inevitable sidelining of the State.[4] This misconception is now backfiring.

2. The State never left the scene. The Internet was initiated by the State, and soon after was privatized. The State minimized its direct involvement in the information environment and increasingly abandoned its role in running the Internet. Instead, it focused on its regulatory role of shaping the rules that govern Internet-related activities, and refrained from actually operating the Internet. In the State's absence, the field was left to the *invisible hand*. Market powers, assisted by the law, facilitated the rise of new players, such as Internet Service Providers (ISPs), search engines, content producers, application designers, and other Online Service Providers (OSPs), who gained power and control in the information environment. In the 2000s, we witness the *Comeback of the State*: the State takes over these ready-made, often quite-centralized, private nodes of power. These nodes of power and control are now being recruited, or co-opted, to serve the State and in fact, many powerful private entities are volunteering to join the State's efforts. A convergence of interests seems to be developing among players such as copyright owners and service providers on the one hand, and the State's growing interest in the digital environment, on the other hand. Law enforcement agencies seek to enhance their monitoring capacity and online businesses seek to prevent fraud and combat piracy while strengthening their ties with authorities. This convergence might lead to an unholy alliance with potentially troublesome results. The *invisible hand* turned out to be very useful for the State, and it is

[1] We use the term "State" in its political science meaning, i.e., to include all branches of government — the executive, legislature, and judiciary, unless otherwise indicated. Occasionally, we use, interchangeably, the term "government." Though this article has an emphasis on American law and politics, the term State should not be understood in the federalist context, i.e., the federal government vis-à-vis the several states, unless otherwise indicated.

[2] LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999).

[3] David R. Johnson & David G. Post, *Law and Borders: The Rise of Law in Cyberspace*, 48 Stan. L. Rev. 1367 (1996).

[4] *But see* CHRISTOPHER MAY, THE INFORMATION SOCIETY: A SCEPTICAL VIEW 114-48 (2002) (arguing that "the suggestion that states are likely to decline in importance in the information age is mistaken").

now being replaced with a handshake, which, likewise, is invisible. This is the *Invisible Handshake*.

3. The most explicit example of the State-private sector handshake is reflected in a presentation by Joseph E. Sullivan, director of compliance and law enforcement relations at eBay. Addressing law enforcement agents at a conference on cybercrime, Sullivan offered to hand over information, when requested, without a subpoena.[5] eBay is one of the largest online e-commerce businesses, and the owner of PayPal, which provides clearing services for online financial transactions. eBay controls access to a colossal amount of information, including financial records, names, user IDs and passwords, affiliations, e-mail addresses, physical addresses, shipping information, contact information, and transaction information (i.e., bidding history, prices paid, feedback rating). But eBay is not alone in implementing law enforcement-friendly policy. The emerging regime of recent years facilitates cooperation between the State and the private sector in law enforcement efforts, beyond the reach of judicial review. Whether the Big Brother we distrust is government and its agencies, or multinational corporations, the emerging collaboration between the two in the online environment produces the ultimate threat.

4. This new mode of State involvement is due to some extent to a shift in the way the digital environment is conceived. It is now increasingly thought of as an arena where alongside positive activities there are also terror-related activities. Therefore, the Internet increasingly becomes a target for intelligence activity. The tragic events of September 11 and its aftermath have strengthened this trend as they changed the way people thought about the State and its responsibilities and highlighted the traditional role of the State as custodian of personal security. It has also emphasized the significance of nationality and affiliation with a national State.[6] This shift in attitudes is strongly reflected by the comprehensive legislation that followed September 11, such as the USA PATRIOT Act in the United States,[7] as amended in 2002 by the Homeland Security Act,[8] the Antiterrorism Act in the United Kingdom,[9] and the Convention on Cybercrime, initiated by the Council of Europe.[10] These laws mark a shift in the State's policies to the Internet: from a "hands-off" attitude

---

[5] *See* Nimrod Kozlovski, *eBay to Law Enforcement – We're Here to Help* (Feb. 17, 2003), *available* at http://research.yale.edu/lawmeme/modules.php?name=News&file=article&sid=925.

[6] The development of the Internet as we know it today was not an inevitable consequence of inherent logic or natural forces. It was shaped by the people and the institutions that initiated and advanced it, as well as by its users and those who dwell in it. The Internet is further affected by ideologies, perceptions, cultural environment, socio-economic context, and the legal regime in which it emerges. The tragic events of September 11, 2001, unsettled many of these aspects. September 11 undermined many of the fundamental beliefs shared by Americans regarding their country, the State, and the role of the State in their everyday lives. It also affected attitudes toward the digital environment. Political and economic changes certainly have a life of their own, but one could predict that these changes will also fashion the Internet in a new way.

[7] USA PATRIOT Act of 2001, Pub. L. No. 107-56, §§ 105, 201-202, 204, 212, 814, 115 Stat. 272 (2001).

[8] Homeland Security Act of 2002, Pub. L. No. 107-296, §§ 223, 225, 235, 116 Stat. 2135 (2002).

[9] Anti-Terrorism, Crime and Security Act of 2001, 2001, c. 24 (Eng.).

[10] The Convention was initiated in the late 1980s, but was concluded shortly after September 2001, and has not yet entered into power. *See* discussion *infra* Part IV.A.

to one of "close-watch and control."

5. This article examines the shifts in the role of the State in the information environment, focusing on the recent innovative cooperation between the State and private parties, whether voluntary or forced. We closely explore the legislation that enables the State to seize control and exercise power in the decentralized borderless information environment. The article traces this intriguing process of recruiting private parties for governing tasks and analyzes its ramifications for the digital environment. Part II sets the theoretical stage, by outlining several functions and roles of the State in the information environment. Governments may opt for one of two main models of information technology (IT) policies or a combination thereof: they may *own* the IT infrastructure or opt for the role of a *regulator*. During the short history of the Internet, the State has assumed both roles. While assuming the relatively less intrusive role of a regulator, the State has allowed private nodes of control to emerge and develop in what appeared to be an exceptionally decentralized environment. In Part III, we describe how the regulatory regime of the 1990s facilitated the rise of these nodes of control. When the State now seeks to seize control in the information environment, it utilizes these private nodes of control at its service.

6. Part IV takes a closer look at the legal framework that allows the State to seize control in the information environment by using the private sector. We analyze a few main pieces of legislation in the United States, the United Kingdom, and Europe. We begin by analyzing rules regarding technological capability requirements, *i.e.,* requiring private powers to design their technology so it may serve the government's needs, as well as data retention, data preservation, and production orders — aimed both at online players and offline actors, such as libraries and bookshops. We also discuss rules that provide OSPs with incentives to cooperate voluntarily with the State. The use of private parties for executing government roles may create an *unholy alliance* between governments that wish to exercise their power and large online players that seek to maintain and strengthen their dominant role in the market.

7. Part V offers possible ways of conceptualizing the cooperation between government and private control nodes in the information environment, pointing at possible consequences of this *Invisible Handshake*. One such avenue we explore is the effect on constitutional law. The State relies on private nodes of control for executing its policies regarding the Internet. One might argue that this should not be too worrisome, since our constitutional law provides us with a readymade toolkit for responding to the State's abuse of power. Yet, when the State executes its powers indirectly, through private parties, standard constitutional analysis may fall short of providing a remedy. Section V.A discusses these constitutional aspects.

8. The *Invisible Handshake* may have some further implications for information policy. A vigorously debated issue regarding the appropriate regulation of the digital environment often reflects fundamentally different assumptions regarding the best way to guarantee liberty and democracy. While some believe that individual freedom would be best secured by the decentralized nature of the Internet, others maintain that liberal democracy requires at least

some concentration of private expressive power, capable of standing up to the government as well as the economic superpowers. The re-entry of the State raises some doubts as to the usefulness of relying on private powers for guaranteeing freedom. Not only has the private sector failed in mitigating the power of the State, it now joins forces with it (or is forced to join it). Section V.B discusses the implications for information policy.[11]

9. Another possible effect might be that of design, *i.e.*, the factors that influence the design of code. There is a dynamic interaction between code and the law: while the law attempts to adopt itself to the fast-changing technology and offer new "rules" that would govern the new information landscape, it is not a one-way relationship. Code is not created out of thin air. Programmers and — no less important their corporate employers — live and operate within a social environment. The law affects the technology they develop: they might wish to adapt the technology so it complies with legal requirements, or they might try to defy the law in the name of what they believe is imperative. Section V.C offers some thoughts on the consequences of the *Invisible Handshake* for the design and architecture of the digital environment.

II. The State and the Digital Environment

10. The State has a complex and dynamic relationship with the digital environment. Even though the Internet is often dissociated from the State, the State never really abandoned it. The State initiated the Internet, releasing it to the private sector, but always keeping an open eye on the network, which grew, unpredictably, into a multinational network of networks, challenging the State's ability to govern. The following discussion tracks the various roles of the State in regard to the digital environment. We begin by unfolding various models of government policies towards information technology (IT), and then turn to examine the policies affecting the Internet. The State in the Internet environment functioned as either an owner or a regulator. When the Internet was privatized, the State still regulated or deregulated the behavior of people related to the Internet as the State regulates many other aspects of human activity. Yet governing the Internet was never trivial. Attempts to regulate the Internet and related activities were widely criticized and often challenged in courts. Consequently, we observe the rise of a third model, which we label the *Invisible Handshake*: this is a regulatory framework that facilitates an alliance between nodes of control of the private sector and the State.

[11] Before we delve into the details of the argument, let us make few important reservations. Our argument does not purport to explain all legal rules that regulate the information environment, nor does it purport to explain all practices that have developed. Our argument is limited to a narrow — though highly important — segment of the information environment. The digital environment is a highly complex space, where many ultra-dynamic factors and forces are at constant work. We offer one possible view of a particular phenomenon, not of all phenomena. This is not an all-encompassing explanation, an option which we doubt is possible, at least not at this point of the development of the digital environment. Finally, this is not a comprehensive survey of all the laws passed in recent years, and it does not provide a full description of the Internet regulatory regime. We simply wish to draw attention to several examples we have identified as significant and believe should be studied.

A. Models of IT Policies

11. Generally, the State might affect the information environment in one of two roles: as a *participant*, exercising its authority through its agents to execute state action, or as a *regulator*, creating a legal order or a system of rules, through the legislatures and the courts. The history of government policies on information and communication technologies reveals two functions of governmental intervention: one is state ownership and the other is regulatory.

12. The first type of policy is governmental provision of services. The postal system is one example.[12] Postal systems began as governmental monopolies, coordinated through the Universal Postal Union.[13] Although in recent years postal markets around the world were partially privatized and increasingly opened to competition, governments retained a monopoly over at least some aspects of mail delivery. The government's role in establishing and then privatizing some aspects of the postal system is similar to its role in designing and providing Internet services during the early days of the Internet.

13. Several rationales are often raised to justify governmental provision of communication services. The standard economic justification points to the nature of communication services that is characterized by economies of scale. These services require a large investment in establishing the infrastructure, but once the infrastructure is set — as in the postal example — the marginal cost of delivering an additional letter is very low.[14] This would normally create a natural monopoly.[15] The natural monopoly argument might explain why a single monopolist should provide a service, but it does not justify the provision of services by the State.[16] The justification for that stems from the fact that information services are essential for the functioning of the market. Therefore, governments will support these services when they are concerned that they will not be sufficiently provided by the market.

14. Other explanations for retaining governmental monopoly over communication services emphasize its significance as a governing tool. Governments may seek to preserve ownership over information exchange systems so as to maintain their control over channels of exchanging and disseminating

---

[12] The postal system is a communication system that allows individuals to send letters or small parcels to any addressee at low cost, usually prepaid by sender. Even though some sort of postal systems, designed to deliver exclusively official mail, existed in ancient times, modern postal systems emerged only during the nineteenth century. *See* Larry Willmore, *Government Policies Toward Information and Communication Technologies: A Historical Perspective*, 2 J. INFO. SCI. 89, 90-92 (2002).

[13] Established in 1875, by the governments of 22 countries, the Universal Postal Union (UPU), now a United Nations agency, was established to coordinate international delivery. *See id.* at 91.

[14] *See* ITHIEL DE SOLA POOL, TECHNOLOGIES OF FREEDOM 75-79 (1983) (classifying the postal service as a common carrier).

[15] *Id*. at 79-84.

[16] Consider for instance the development of telegraph services, which took opposite directions in England and in the United States. While in the United States, Western Union acquired most telegraph companies during the second half of the nineteenth century, in England, the government nationalized the telegraph companies in 1868, handing over control to the Post Office. Willmore, *supra* note 12, at 92. Similarly, while the American model of radio broadcasting was based on licensing commercial stations, many countries followed a model of state ownership (such as Great Britain's BBC) or a mixed model of government-owned and commercial broadcasting.

information.[17]

15. Another model of governmental policies toward information and communication systems is that of regulation. Even though telephone services are usually provided by private companies, these providers and their services are heavily regulated. The rationale for regulation is often the monopolistic nature of communication services.[18] A monopoly is not exposed to competition, and it therefore tends to set its prices and services in such a way that maximizes its own profits, leading to social inefficiencies. Under such circumstances, the State is called upon to secure the public interest by restricting the monopolist behavior and setting standards of price and service that would benefit the public at large. This rationale could explain regulation of telephone services before the introduction of microwave technology. The regulation transformed the monopolistic nature of telephone services and facilitated entry by competing companies and technologies, such as MCI (Microwave Communications Inc.).[19] Another rationale for regulation is the use of scarce resources. The most evident example is the regulation of broadcasting that is justified by the need to allocate wavelengths to broadcasters.[20]

16. These rationales do not apply to the Internet. The decentralized technological feature of the Internet ensures that everyone who abides by the technical standards can connect to the Internet and become not only a user but also part of its reservoir of computing and content resources. There is no use of scarce national resources, and otherwise familiar problems of monopolies may dramatically decline.[21]

17. Sometimes, however, the State uses regulation to advance political and economic goals, such as universal service[22] or monitoring for national security purposes.[23] Alongside these types of rules especially designed for communication services, there are common law rules such as property laws, liability rules, and contract law, which have a general scope but are also applicable to information and communication services. The application of these rules in the information environment may define what would become an appropriate subject of property rights (and of course, what would not): the electromagnetic spectrum and databases are two familiar examples. Property

---

[17] *Id*. at 91 ("One reason … is the desire for state security, for protection against subversive or unpopular ideas …. It is far more important to control the distribution of information than the reproduction of information.").
[18] *Id.* at 92. *See also* DONALD E. LIVELY, MODERN COMMUNICATIONS LAW 515-529 (1991) (describing the nature of common carriers, such as the telephone industry, as a reason for content restriction).
[19] Willmore, *supra* note 12, at 92-93.
[20] de Sola Pool, *supra* note 14, at 2; Red Lion Broadcasting Co. v. FCC, 395 U.S. 367 (1969).
[21] The online information environment may facilitate, however, the creation of monopolies that gain their monopoly status by controlling technological standards. *See* Niva Elkin-Koren & Eli M. Salzberger, *Law and Economics in Cyberspace,* 19 INT'L REV. L. & ECON. 553, 557-559 (1999); Sun Microsystems, Inc. v. Microsoft Corp., 240 F. Supp. 2d 460 (2003).
[22] *See* Telecommunications Act of 1996, Pub. L. No. 104-104, § 254, 110 Stat. 56, 71 (1996).
[23] *See* National Security Decision Directive No. 145, *National Policy on Telecommunications and Automated Information Systems Security*, The White House (Sept. 17, 1984); Telecommunications Act of 1997, pt. 16 (Austl.), *available at* http://scaleplus.law.gov.au/html/pasteact/2/3021/top.htm.

law and tort law define how these rights are transferred[24] or who is liable for injurious content.[25] These rules may of course shape power relations and affect the behavior of the different players in the information and communication market.

18. In sum, the government can opt for an active role of an owner of the IT at stake or that of a regulator. We now turn to examine governmental policies toward the Internet.

B. The State and the Internet

19. One of the themes associated with the Information Age and with its prominent symbol — the Internet — was a general notion of the decline of the State. The 1990s were characterized by a predisposition to globalization, perceiving the Internet as an international endeavor lying beyond the reach of laws of any particular government.[26] It was conceived as a post-national situation where individual users acquired a new status of Netizens, undertaking novel commitments towards the global community of Internet users.[27]

20. The Information Age was thought of as marginalizing the State. For a while the global nature of the Internet appeared to be weakening the legitimacy of State regulation that would normally be justifiable within territorial borders. Because Internet activities were not restricted to any geographical area, regulating such activity by one state may affect citizens of another state.[28] The cross-border nature of the Internet was also thought of as damaging the enforceability of laws imposed by the State, thereby further weakening the effectiveness of State regulation.[29] The accelerating pace of technological change further impaired the effectiveness of State regulation, making it almost impossible for regulators to keep up with a technology that reinvents itself

---

[24] *See, e.g.,* UNIFORM COMPUTER INFORMATION TRANSACTIONS ACT (UCITA) § 501 et seq. (1999) (setting the rules of alienability of online information). The National Conference of Commissioners on Uniform State Laws decided in August 2003 not to "expend any additional Conference energy or resources in having UCITA adopted." *See* Letter from K. King Burnett, President, National Conference of Commissioners on Uniform State Laws, to Fellow Commissioners (Aug. 1, 2003), *at* http://www.nccusl.org/nccusl/ucita/KKB_UCITA_Letter_8103.pdf (last visited Aug. 25, 2003).

[25] *See* Iris Ferosie, *Don't Shoot the Messenger: Protecting Free Speech on Editorially Controlled Bulletin Board Services by Applying* Sullivan *Malice*, 14 J. MARSHALL J. COMPUTER & INFO. L. 347, 356-59 (1996) (stating that a newspaper may be liable after printing an editorial, because the newspaper editors read and edit stories before publication); *see also* Telecommunications Act of 1996, *supra* note 22, codified at 47 U.S.C § 223(c)(2) (2003) (discussing common carriers' exemption from liability for obscene or harassing telephone calls).

[26] *See* John Perry Barlow, *A Declaration of the Independence of Cyberspace* (Feb. 8, 1996), *at* http://www.eff.org/~barlow/Declaration-Final.html; David R. Johnson & David G. Post, *The New 'Civic Virtue' of the Internet* (Feb. 1998)*, at* http://www.cli.org/paper4.htm. For criticism, see Neil Weinstock Netanel, *Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory,* 88 CAL. L. REV. 395 (2000).

[27] *See* Johnson & Post, *supra* note 26.

[28] Joel R. Reidenberg, *Yahoo and Democracy on the Internet,* 42 JURIMETRICS J. 261 (2002); League Against Racism and Antisemitism (LICRA) v. Yahoo! Inc., Yahoo! France (County Court, Paris, Nov. 20, 2000); Yahoo! Inc., v. LICRA, 169 F. Supp. 2d 1181 (N.D. Cal. 2001); David R. Johnson & David G. Post, *Law and Borders: The Rise of Law in Cyberspace,* 48 STAN. L. REV. 1367 (1996).

[29] Johnson & Post, *supra* note 26.

every few months.[30]

21. At the same time, a few attributes of the Information Age strengthened the private sector. Corporations in the information economy, in which information is a central resource, turn out to be highly mobile and independent of any specific location. The ability to convey information and knowledge easily allowed multinational corporations to organize themselves across national borders, thereby decreasing the dominance of the State in organizing economic relations.[31] Furthermore, the design of the technology — or code — accorded private companies with regulatory power in shaping the information environment.[32] Code determines what actions are feasible and what options become available, and may prove more effective than legal rules in directing human behavior.[33] Overall, the private sector in the digital environment enjoyed more power in setting the agenda and shaping the priorities.

22. This picture of the decline of the State is, however, misleading. It underestimates the power of the State as a significant social and political institution and fails to acknowledge the force of law. Tracking the involvement of the State in the digital environment reveals that the State played a significant role in shaping the environment all along. As the following discussion demonstrates, the State undertook a dynamic role, but its actions, and inactions, were always substantial.

1. Ownership: In the Beginning There Was the State

23. In the beginning was the State, or to be precise, the United States. The first high-speed computer network, ARPANET, was initiated by the United States Defense Department's Advanced Research Projects Agency (DARPA).[34] The Internet was first conceived in the early 1960s. In 1969, the Defense Department commissioned ARPANET.[35] At the beginning of the 1970s ARPANET grew from four hosts at U.S. campuses (in 1969) to 23 hosts connecting universities and government research centers around the United States. It also launched its international connections.

24. Even though many celebrate the grassroots sources of the Internet and its anarchic, free, and voluntary communitarian nature, the Internet was conceived by military strategists and was only later privatized. The early ARPANET was commissioned by the government to serve a military purpose

---

[30] Elkin-Koren & Salzberger, *supra* note 21.
[31] MAY, *supra* note 4.
[32] LESSIG, *supra* note 2; Joel Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553 (1998).
[33] *See* filter software such as CyberPatrol, *available at* http://www.cyberpatrol.com/default.aspx; Net Nanny, *available at* http://www.netnanny.com/index.html.
[34] ARPA (Advanced Research Projects Agency), a Defense Department unit, was founded in 1958 to support research and development in technology, to confront the perceived threat of Soviet technological advantage. *See* Richard T. Griffiths, *History of the Internet, Internet for Historians, Chapter Two: From ARPANET to World Wide Web* (2002), *available at* http://www.let.leidenuniv.nl/history/ivh/chap2.htm.
[35] *See* Robert H'obbes' Zakon, *Hobbes' Internet Timeline v6.1 (2003)*, *available at* http://www.zakon.org/robert/internet/timeline/

and was consequently based on technologies designed for that purpose.[36] The decentralized nature of the Internet is often ascribed to the strategic problem it sought to address, namely to secure communication in the case of a nuclear attack on central facilities. The theory was that a distributed network would be more resilient to repeated attacks than a centralized network.[37]

25. At the same time, the government's exclusive policy, which restricted access to ARPANET until the early 1990s, facilitated the development of applications such as USENET.[38] Other networks, such as BITNET and CSNET, provided services to universities outside ARPANET. In other words, due to restrictions on access to the ARPANET, key Internet applications were designed by non-governmental agents and on non-governmental infrastructure. Thus, alongside the deliberate, centrally planned project designed by the government, non-governmental forces worked on independent technological projects,[39] developing the Internet as an anarchic sprawl and responding to grassroots pressure.[40] These conflicting forces[41] — control of the government on the one hand and private innovation on the other hand — shaped the unique character of the digital environment. The mixture of public, centrally designed technologies and private initiatives explains some of the controversies regarding the "true" nature of the Internet.[42]

---

[36] With a different view, Bob Taylor, one of the scientists and engineers who devised the APRA, claimed that ARPANET's intention was a very peaceful one — to link computers at scientific laboratories across the country, so that researchers might share computer resources. Saying that ARPANET was designed to protect national security in the face of a nuclear attack is just a myth. *See* KATIE HAFNER & MATTHEW LYON, WHERE WIZARDS STAY UP LATE 10 (1996).

[37] *See* Bruce Sterling, *History of the Internet*, F&SF SCIENCE COLUMN #5, *available at* http://w3.aces.uiuc.edu/AIM/scale/nethistory.html. For instance, packet switching technology was designed to serve a strategic goal of resiliency, by reducing dependency on central control systems, and securing continuous service even in case of major damage to control systems as result of a nuclear attack. Willmore, *supra* note 12, at 94 (arguing that the purpose of the ARPA project was to design a computer network that would be secure and resist attack in the event of war.) Willmore suggests that such technology was thought of as more secure, since "it is difficult for the enemy to make sense of intercepted, unassembled packets." *Id.*

[38] Willmore argues that the first step in opening the military network to the public was the creation of Telnet in 1974 — which was a public version of ARPANET. Telnet was used to establish USENET newsgroups. *See* Willmore, *supra* note 12, at 95.

[39] One example is Interface Message Processors (IMPs), which were arguably designed to facilitate the sharing of computer resources by scientific laboratories. *See* HAFNER & LYON, *supra* note 36, at 75-81.

[40] *See* MICHAEL HAUBEN & RONDA HAUBEN, NETIZENS 63-64, 319 (1997) ("These networks are also the result of hard work by many people aspiring for more democracy.")

[41] The Internet's special nature could be metaphorically described as, borrowing Eric S. Raymond's famous phrase, "The Cathedral and the Bazaar." The "Cathedral" stands for a centrally pre-designed project as against the decentralized mechanisms for producing content, such as the Linux project.

[42] Rather than emphasizing that a single dominant factor determined the nature of the Internet, it would be advisable, as suggested by Rosenzweig, to acknowledge its complicated nature.

> The rise of the Net needs to be rooted in the 1960s — in both the "closed world" of the Cold War and the open and decentralized world of the antiwar movement and the counterculture. Understanding this dual heritage enables us to better understand current controversies over whether the Internet will be "open" or "closed" — over whether the Net will foster democratic dialogue or centralized hierarchy, community or capitalism, or mixture of both.

Roy Rosenzweig, *Wizards, Bureaucrats, Warriors & Hackers: Writing the History of the Internet*, 103 AM. HIST. REV. 1530, 1531 (1998).

26. Towards the late 1970s and during the 1980s, ARPANET moved away from its military/research roots and became the Internet as we know it today. Restrictions on traffic on the backbone of the Internet (the NSFNET, the National Science Foundation's backbone) were lifted in 1991, when the NSF permitted commercial use. This decision cleared the way for the privatization of the Internet and opened the door to electronic commerce. Indeed, the State's withdrawal was never complete. Governmental sponsorship of research and development related to the Internet was a live and controversial issue during the second half of the 1990s, focusing on public investments in the Next Generation Internet.[44] Nevertheless, the process of privatization transformed the Internet from an enterprise designed and sponsored by the State into an anarchic global network-of-networks, sponsored by private firms and made of a mixture of applications designed by a variety of independent parties.[45]

2. The State's Regulatory Role

27. While during the 1990s the State withdrew from running the Internet, it undertook the role of a *regulator* and it proved to be rather active. The volume of regulation related to the Internet accelerated expeditiously, especially during the second half of the 1990s.[46] This legislation sought to achieve several purposes, such as employing the Internet to provide traditional public goods; developing the future infrastructure of the Internet; and attempting to adapt existing legal institutions, such as copyright law or contract law, to the changing information environment.[47]

28. The State's role as a regulator differs from its role as an actor — a provider of services, a producer, a sponsor, or otherwise a full player in the information environment. In its capacity as a regulator, the State is involved in directing private action (the behavior of individuals and firms) through the application

---

[44] This debate resulted in continued government funding of research and development through the National Science Foundation (NSF) and other government agencies. *See* Next Generation Internet Research Act of 1998, Pub. L. No. 105-305, 112 Stat. 2919 (1998).

[45] Few explanations are suggested in the literature for the State's decision to withdraw from its active role, and leave the scene to private parties. One is economic: the difficulty in financing the ever-growing Internet with public funds. Another explanation is growing resistance to public spending, which requires the government to cut support to publicly funded research and development, and rely more heavily on private financing. Privatization was also technologically driven, and was partly due to the introduction of new technologies, such as TCP/IP (in 1983), which allowed the interconnection of independent and incompatible computers and information systems, followed by the World Wide Web (in 1991), and Mosaic (in 1993), the first graphics-based Web browser. These technologies allowed open access in the sense that they were based on standards open and available to all. Connecting to the Internet required merely adopting such standards, which were not subject to military restrictions, nor to any proprietary rights.

[46] *See* Yochai Benkler, *How (if at all) to Regulate the Internet: Net Regulation: Taking Stock and Looking Forward*, 71 U. COLO. L. REV. 1203, 1207 (2000). Benkler's survey of Internet regulation shows that while regulation related to the Internet was at first rather modest (the 101st Congress enacted three laws related to the Internet, the 102nd enacted four, the 103rd enacted three, and the 104th enacted five), the 105th Congress enacted twenty-nine Internet related laws.

[47] *Id.* at 1204, 1259-60.

of rules.[48] The State as a regulator constitutes a system of rules. A regulator produces rules, designed to resolve conflicting interests and ideologies, aiming at protecting rights or advancing policy objects through the legal system. The State in this role functions as a referee.

29. Copyright law and its adjustment to the digital environment is one example of the State's role as a referee: it determined the rules (through legislation and adjudication) and facilitated their enforcement (through adjudication and execution procedures.) Other than that, it left the field to private players. Indeed, much of the criticism against the State, especially against Congress, in the context of copyright regulation, is that it was a biased referee; that the rules set were favorable to some actors, namely the incumbent industries,[49] and that after setting the rules it abandoned the field and allowed those players to assume unprecedented power at the expense of users.[50]

30. The State's role as a referee is also demonstrated in the context of digital data privacy. The public debate revolves around the justification of the State's intervention in the market, and the possible consequences of such a move. Is there a real market failure that justifies such intervention?[51] How would such intervention affect the (constitutional) rights of those whose activities will now be regulated?[52] One of the few situations in which the State did intervene by regulating data collection and distribution practices is the Children's Online Privacy Protection Act of 1998 (COPPA).[53] The decision to regulate digital data privacy reflects a choice between human rights — privacy in this case, and economic efficiency, as well as the financial interest of online providers. The statute declares its goal to "protect the privacy of personal information

---

[48] The phrase 'State as an Actor' refers to the State participating in the market as an economic player, burdened with the same restrictions imposed on private market participants. In doing so, the State exercises its right to favor its own citizens over others. State regulatory power refers to the State interfering with the natural functioning of the market, either through prohibition or through burdensome regulation, while enjoying special power not shared by any private entity. The line between market participation and market regulation is often blurred. *See* LAURENCE H. TRIBE, 1 AMERICAN CONSTITUTIONAL LAW 1088-1091 (3d ed. 2000); Hughes v. Alexandria Scrap Corp., 426 U.S. 794, 805-06 (1976); Reeves, Inc. v. Stake, 447 U.S. 429, 441 (1980).

[49] For accounts of the successful influence of the incumbent industries, see Pamela Samuelson, *The Digital Agenda of the World Intellectual Property Organization*, 37 VA. J. INT'L L. 369 (1997); Pamela Samuelson, *The Copyright Grab*, WIRED 4.01 (1996); Jessica Litman, DIGITAL COPYRIGHT (2001). In the international arena, see Susan K. Sell, PRIVATE POWER, PUBLIC LAW: THE GLOBALIZATION OF INTELLECTUAL PROPERTY RIGHTS (2003).

[50] For a critical discussion of the copyright regime as a facilitator of the concentration of power in information markets, see Niva Elkin-Koren, *It's All About Control*, *in* THE COMMODIFICATION OF INFORMATION (Niva Elkin-Koren & Neil W. Netanel eds., 2002).

[51] See the various views expressed by the commissioners of the FTC in FEDERAL TRADE COMMISSION, ONLINE PROFILING: REPORT TO CONGRESS, PART 2: RECOMMENDATIONS (July 2000), *available at* http://www.ftc.gov/os/2000/07/onlineprofiling.htm.

[52] For example, FTC Commissioner Orson Swindle, in dissenting from the FTC's recommendation to legislate minimum privacy standards, argued that when firms engage in data transfers, that is, information regarding users, it is commercial speech that is at stake. Hence, he argued, any privacy legislation should be subject to First Amendment scrutiny. *See* FEDERAL TRADE COMMISSION, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE – A REPORT TO CONGRESS (May 2000), *available at* http://www.ftc.gov/reports/privacy2000/privacy2000.pdf (dissenting statement of Commissioner Orson Swindle). We shall return to the constitutional implications of the State's new role; *see infra* Part V.A.

[53] Codified at 15 U.S.C. §§ 6501-6506 (2003).

collected from and about children on the Internet, to provide greater parental control over the collection and use of that information, and for other purposes."[54] In other words, the State undertook the steps it deemed necessary in order to protect the interests of children. The (constitutional) problem is that almost any intervention in the market affects the rights of others. In the case of COPPA, the requirements of businesses that collected personally identifiable information (PII) from children (defined as those under 13 years of age) imposed a heavy financial burden. A Web site operator who wishes to collect PII on children has to establish some sort of a customer relationship management (CRM) system to obtain parental consent.[55] The result is that many sites were forced to change their methods of doing business: either stop collecting PII on children, or prevent children from accessing the site. Of course, richer Web sites can afford to maintain the required CRM systems.[56] COPPA is an example of the State's rather rare direct intervention in setting the "rules of the game," but the State itself, after determining the rules, stays outside the field.

31. Regulation may shape the information environment directly, defining what is *right* or what is *wrong* in online behavior, or indirectly, by establishing the legal infrastructure of online markets, thereafter enabling the invisible hand to take control. Direct regulation is most evident in the attempt to limit the distribution of content that is perceived to be harmful. In the area of free speech the State has thus far taken the fiercest position, trying to intervene in the market by directly prohibiting certain kinds of behavior. The declared governmental interest in that case was the protection of children. Most of the blunt attempts by the federal government to do so have, to this day, failed: courts found the Communications Decency Act of 1996 (CDA), its improved version — the Child Online Protection Act of 1998 (COPA), as well as the Child Pornography Prevention Act of 1996 (CPPA) to be unconstitutional.[57] The exception is the Supreme Court's decision which found the Children's Internet Protection Act of 2000 (CIPA) to be constitutional.[58] However, this Act, conditioning some of the funding to public libraries on the installment of technological measures that filter content unsuitable for children, is better understood as a form of indirect regulation.[59] The role the State (both Congress and the Judiciary) undertook in these attempts was that of a protector of human rights. For example, when Congress outlawed the knowing

---

[54] S. 2326, 105th Cong. (1998) (enacted).

[55] *See* 15 U.S.C. § 6502(b)(1)(A)(ii). Parental consent can be obtained by e-mail, printed forms, toll-free telephone or via credit card verification. *See* § 6501(9) (defining "verifiable parental consent"). For the extent of compliance, *see* FEDERAL TRADE COMMISSION, PROTECTING CHILDREN'S PRIVACY UNDER COPPA: A SURVEY ON COMPLIANCE 6-7, 12 (2002) *available at* http://www.ftc.gov/os/2002/04/coppasurvey.pdf.

[56] The FTC COPPA REPORT, conducted one year after COPPA became effective, noted that "fewer sites were collecting personal information online." *See* PROTECTING CHILDREN'S PRIVACY UNDER COPPA: A SURVEY ON COMPLIANCE, *supra* note 55, at 13.

[57] *See* Reno v. ACLU, 521 U.S. 844 (1997) (CDA unconstitutional); Ashcroft v. ACLU, 535 U.S. 564 (2002) (COPA's "community standards" term is constitutional, but case remanded for further consideration); Ashcroft v. Free Speech Coalition, 535 U.S. 234 (2002) (CPPA unconstitutional).

[58] U.S. v. American Library Ass'n, Inc., 123 S. Ct. 2297 (2003).

[59] For a critical and comparative discussion of various forms of regulations aimed at protecting children in the online environment, see Michael D. Birnhack & Jacob H. Rowbottom, *Shielding Children: The European Way*, 79 CHI.-KENT L. REV. __ (forthcoming, 2003).

transmission of indecent material to minors by enacting the CDA, it did so in order to protect children from harmful material.[60] The Supreme Court recognized this to be a compelling state interest but concluded that "the interest in encouraging freedom of expression in a democratic society outweighs any theoretical but unproven benefit of censorship."[61]

32. Regulation may further take the form of indirect intervention by creating a series of background rules such as determining what can be owned, how rights would be transferred, who may be subject to liability, and under what circumstances. These rules may provide incentives for one type of behavior while discouraging another. For instance, liability imposed on intermediaries for injurious content distributed by their users could provide incentives for screening content, and thereby could reduce the number of decentralized interactive services that are offered online.[62] Such regulation may also affect the production of content. By making it more difficult and expensive for individuals to exchange files and distribute their self-made content, liability rules may encourage mass-production of content at the expense of alternative modes of producing and distributing informational goods.

33. Other rules affect the types of technologies that become available by raising the cost involved in developing or implementing specific technologies. For instance, legal exposure created by the Digital Millennium Copyright Act's (DMCA) anti-circumvention rules deters potential investments in circumvention technologies, namely technologies that allow the circumvention of self-help technological locks used by content providers.[63]

34. The entire regulatory regime that governs the Internet, both direct and indirect regulation, provides the background for the rise of a third type of State involvement in the digital environment: an alliance between the State's enforcement efforts and the private sector — the *Invisible Handshake*.

3. The Invisible Handshake

35. In recent years the State has become more active in the digital environment, acknowledging its growing significance for commerce and community, and identifying its potential importance as a new battle zone, where law offenders

---

[60] As the Court noted, there was no real debate in Congress as to the CDA, which was part of the Telecommunications Act of 1996. The CDA provisions were "added in executive committee after the hearings were concluded or as amendments offered during floor debate on the legislation." *Reno*, 521 U.S. at 858.

[61] *Id*. at 885.

[62] The amount of information communicated via interactive computer services is … staggering. The specter of tort liability in an area of such prolific speech would have an obvious chilling effect. It would be impossible for service providers to screen each of their millions of postings for possible problems. Faced with potential liability for each message republished by their services, interactive computer service providers might choose to severely restrict the number and type of messages posted. Zeran v. America On-Line, Inc., 129 F.3d 327, 331 (4th Cir. 1997). *See also* Niva Elkin-Koren, *Copyright Law and Social Dialogue on the Information Superhighway: The Case Against Copyright Liability of Bulletin Board Operators*, 13 CARDOZO ARTS & ENT. L.J. 345 (1995).

[63] *See* 17 U.S.C. §§ 1201-1205; Universal Studios Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001); U.S. v. Elcom Ltd., 203 F. Supp. 2d 1111 (N.D. Cal. 2002).

and terrorists act and could be targeted.[64] This trend was dramatically strengthened after the tragic events of September 11, and the declared international effort to fight terrorism. In the 9/11 aftermath massive legislation was introduced that significantly enhanced the authority of governments to operate in the online environment.

36. The emerging legal regime allows the government to intercept electronic communication and collect information on users and their computers. The digital environment has dramatically improved the potential for efficient collection of useful information on many aspects of an individual's life (such as bank transactions, personal e-mails, private chats, browsed Web sites, shopping habits and contacts.) Surveillance can now be executed on a single platform, using advanced technologies at a relatively low cost.[65] Precisely when the available interceptive and monitoring devices proved so powerful, the restraining rules that were supposed to secure civil liberties were relaxed. For instance, prior to the enactment of the USA PATRIOT Act ("the Act"), the law authorized the methods of "Pen Register" and of "Trap and Trace" of numbers dialed to or from a telephone line, although this authorization was extended to e-mail by some courts.[66] The USA PATRIOT Act explicitly authorizes the collection of addressing information (but not the content) of computer communications.[67] Furthermore, the Act establishes a de facto nationwide pen/trap order, thus making it easier for law enforcement agents to intercept e-mails that pass through many OSPs in different locations and that may be stored remotely outside the jurisdiction of where the search order was requested.[68] Law enforcement authorities that seek a pen/trap order need only specify the initial facility at which the order will be carried out and that same order will apply to any service provider nationwide.

---

[64] Several aspects of the information environment were identified as relevant for anti-terrorist efforts. First, the Internet as a major communication means, which allows exchange of information, was perceived as an arena that requires surveillance for preventing future hostile actions and collecting evidence for prosecuting terrorists. Second, the Internet as a relatively open distribution mechanism allows the distribution of propaganda by terrorist groups, recruitment of new supporters, collection of donations, and so forth. *See* Reuven Paz*, Qa'idat al-Jihad: A New Name on the Road to Palestine* (May 7, 2002), *at* http://www.ict.org.il/articles/articledet.cfm?articleid=436 (analyzing the use of the Internet for distributing terrorist ideology and establishing links among supporters).

[65] Such means include filters, recordings, and surveillance systems such as Carnivore and Magic-Lantern.

[66] The Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848, which governed the use of Pen Register, did not explicitly apply to e-mail. Kerr reports, however, that in practice courts routinely approved governmental requests — but for one case — and issued Pen Register orders in regard to e-mail communication. *See* Orin S. Kerr, *Internet Surveillance Law after the USA Patriot Act: The Big Brother that Isn't*, 97 NW. U. L. REV. 607, 639 (2003). *See also* Joginder S. Dhillon & Robert I. Smith, *Defensive Information Operations and Domestic Law: Limitation on Government Investigative Techniques* 50 A.F. L. REV. 135, 149-51 (2001).

[67] 18 U.S.C. § 3127 (as amended, 2003): "(3) the term 'pen register' means a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication." Similarly, subsection 4 defines the term "trap and trace device" as "a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communications."

[68] 18 U.S.C. § 2703(a).

37. The new type of State involvement in the information environment is different in various aspects from *ownership* or *regulation* previously undertaken by the State. One is the *kind of role* the State undertakes: in addition to the role of a regulator, the State recaptures its role as an active player, taking action in the online environment to secure national interests in a global network. The second aspect, a derivative of and intertwined with the previous one, is the *nature* of State intervention. The State no longer restricts itself to the role of a neutral regulator, a forum for resolving conflicting interests and ideologies of its citizenry through a system of rules; rather, it implements its ancient duty of securing individual safety and national security. In this context the digital environment is perceived as threatening national security and as an arena that must be governed.

38. The current intervention by the State in the digital environment differs in yet another way from previous forms of government intervention. The most intriguing aspect of the current type of State involvement is the mechanism by which the State seeks to seize control in the information environment. What characterizes the State's current pursuit is increasing reliance on private/commercial agents for executing governmental power, especially in the "war against terror." The working assumption is that terrorists hide behind the technological curtain of the (innocent) OSP,[69] and their operation takes advantage of online services provided by OSPs.

39. OSPs have inherent features that make them attractive to the State in its capacity as a provider of national security. For obvious reasons, it is difficult to detect suspected terrorists; they are scattered among numerous Internet users, their activities are usually conducted in private (physical) places, probably outside the territorial jurisdiction, and to act, they need the services of OSPs. The OSPs, in contrast, are fewer than the total number of users. Their activity is not disguised, they are not anonymous, and in most cases they have a permanent physical address, and hence are easier to detect. OSPs further hold robust databases of online activities, comprised of the digital tracks left by their subscribers. Such databases could considerably enhance law enforcement capabilities. Finally, the OSP is not only a curtain, but also a technical bottleneck. It is a place where users' activities (including terrorists') pass. It is easier to detect the terrorist activity at that point and block it there. The operation of government surveillance makes use of the facilities operated by OSPs and often requires their cooperation.

---

[69] We use the term OSP as the generic term for any online service provider, and reserve ISP (Internet Service Provider) for access providers. The Digital Millennium Copyright Act (codified at 17 U.S.C. § 512(k)(1)) defines service provider as either "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, without modification to the content of the material as sent or received," or "a provider of online services or network access, or the operator of facilities therefor." *But cf.* Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in particular Electronic Commerce, in the Internal Market (Directive on Electronic Commerce), art. 2(b), 2000 O.J. (L 178) [hereinafter E-Commerce Directive] (defining "Service Provider" as "any natural or legal person providing an information society service").

40. A well-publicized example is Carnivore,[70] a computer program that scans digital packets, transmitted through the service provider facilities, for specific information according to different parameters (such as targeted messages from a specific origin, or special strings of text). Carnivore can be programmed to capture only traffic information (such as e-mail addresses of sender and recipient), or to capture the entire content of a message. Carnivore is installed on the servers of Internet Service Providers (ISPs),[71] and requires the active cooperation of the ISP.[72]

41. Using OSPs for law enforcement purposes could further overcome some of the enforcement difficulties faced by the National State in the global networked digital environment. OSPs operated by multinational corporations may be more effective than law enforcement agencies in monitoring online behavior on a global network, since they are not tied, nor restricted, to any national border. OSPs may further prove more flexible in watching online activities since they are not subject to the same scrutiny which applies to the State and its agents.

42. The status of OSPs and their ability to serve as a node of control were shaped during the earlier phases of the Internet. The function of OSPs, their rights and duties to subscribers and third parties, their status, the market structure, and the level of competition in each particular market, were not developed in a vacuum. Under State regulation various players gained control over important junctions in the informational environment.

43. These players are now being recruited to serve governmental purposes. Now, as the State assumes its active role as a player, it is naturally drawn to these ready-made nodes of control and wishes to utilize them. Recruiting OSPs for executing security assignments is done either by compulsion (under a warrant, a subpoena or by a statutory imposition of this duty), or by offering them incentives to do so voluntarily, accompanied by immunity, if necessary.

44. Before turning to examine the legal regime that facilitates this change, we describe how the seemingly decentralized online environment has promoted new types of gatekeepers and control nodes. We then move on to describe how the new regime takes advantage of these gatekeepers.

---

[70] This name was given to the software by the FBI because it "chews" all the information, but "swallows" and "digests" only the specific information desired. Carnivore has been renamed DCS-1000. Reuters, *FBI Renames 'Carnivore' Internet Wiretap* (Feb. 14, 2001)*, at* http://archive.aclu.org/news/2001/w021401b.html.

[71] *See* FREEDOM HOUSE, THE ANNUAL SURVEY OF PRESS FREEDOM 2002, at 12 (Leonard R. Sussman & Karin Deutsch Karlekar eds., New York) (reporting that after Sept. 11 the FBI installed Carnivore on major U.S. ISPs' servers).

[72] *See* Statement of Donald M. Kerr, Assistant Director, Laboratory Division, FBI, on Internet and Data Interception Capabilities Developed by FBI, Before House Comm. on the Judiciary, Subcomm. on the Constitution (July 24, 2000), *available at* http://www.fbi.gov/congress/congress00/kerr072400.htm.

III. The Rise of Private Gatekeepers: Facilitating Nodes of Control in a Decentralized Environment

A. The Decentralized Network and the New Virtual Gatekeepers

45. For years the Internet enjoyed the image of an unmanageable anarchic network that frustrated any effort to regulate it and discipline the behavior of its users. The potential of the Internet as a technology of freedom[73] has to do with its unique and decentralized architecture, which allows every user of protocols that comply with the technical standards to connect to it. This architecture transformed the economics that governed the distribution of content in the print and broadcasting world. Production and distribution of content were liberated from the industrial paradigm, and for a while were opened to the public at large who engaged in the production of freely available materials and the exchange of data and informational works.

46. Compared with the pre-digital world, the Internet offered a relatively open environment for distributing content, exchanging ideas, and accessing information. On the distribution side, dissemination no longer involved high costs of production of copies and their traffic (as in print), or the use of scarce and expensive resources such as the electromagnetic spectrum (as in broadcasting). Neither did it require the large financial investments involved in managing the distribution of content, nor the business models that would secure a financial return. On the Internet, everyone could become a speaker, and was free to distribute information to the general public simply by posting it online at minimal cost. No editorial scrutiny, no censorship, and no selection — the Internet was thought of, and often was, a fully accessible public forum.[74]

47. On the production side, the Internet allowed potential creators to join efforts in an unmanaged way, assigning themselves to tasks as they saw fit, and coordinating their efforts through online communication.[75] Indeed, the Internet opened up opportunities for creation, free from corporate censorship that obeys ratings and potential profits,[76] and opened up opportunities for individual and communal creation of content outside the industrial commercial model. The information environment was supposedly open and accessible to all.[77]

48. Nevertheless, in the seemingly decentralized open-access environment, new types of gateways developed — portals, junctures of operation, and facilitators of access. OSPs such as providers of e-commerce services, toolmakers, search

---

[73] The term is borrowed from de Sola Pool, *supra* note 14.
[74] *See* Eugene Volokh, *Cheap Speech and What It Will Do,* 104 YALE L.J. 1805 (1995).
[75] *See* Yochai Benkler, *Coase's Penguin, or, Linux and the Nature of the Firm,* 112 YALE L.J. 369 (2002).
[76] *See* Neil W. Netanel, *Market Hierarchy and Copyright in Our System of Free Expression,* 53 VAND. L. REV. 1879 (2000); NAOMI KLEIN, NO LOGO (2000); C. EDWIN BAKER, ADVERTISING AND A DEMOCRATIC PRESS 62-66 (Malcolm DeBevoise ed., 1994) (noting that the need to keep the audience in a "buying mood" affects the content of television programs and newspapers).
[77] See NIVA ELKIN-KOREN & ELI M. SALZBERGER, LAW, ECONOMICS AND CYBERSPACE 168-69 (forthcoming 2004).

engines, and content providers, function as gateways to online traffic. A typical gateway is an ISP. ISPs design the gateways through which users must pass to use the Internet, and affect many aspects of their online experience. They can make access to some sites easier than to others by providing wide exposure and links, and by using data accelerators, and they can block some materials altogether using filtering software. ISPs may also block users off and track their online activities. These capabilities made ISPs the object of legislation aimed at blocking access to obscene or child pornography materials.[78]

49. Another, more virtual, gatekeeper is a search engine. In the information glut that developed on the Internet, users are dependent upon search engines for locating useful information. Content that is undetectable or otherwise remains unlisted on the search results is almost nonexistent on the Web since the chances that users will be able to locate it without prior information are slim.[79] OSPs such as search engines could therefore make it difficult to track certain sites and retrieve some information. They may further provide a robust database, recording online activities.

50. Online gateways could be attractive nodes for facilitating governmental efforts to re-enter the information arena. The current architecture of the Internet makes the OSPs a mirror of much of the activity that passes through it. Surfing leaves digital traces both on the client computer and on the OSP's server. The OSP's server documents users' activities as an integral part of its operation. A user can connect via a dynamic IP system,[80] surf through an anonymizer service,[81] choose a fictitious nickname in a chat room, or use other digital self-help mechanisms, but the OSP can still identify the user.[82] OSPs keep records of much of this activity, their motivation being simple: billing and system maintenance. The direct (technical) connection between the user and the OSP, combined with the direct legal (contractual) relationship between them, allow OSPs to identify users who, for any other purpose, disguise their identity.

---

[78] *See supra* note 57 and accompanying text.

[79] That is why providers rely on search engines' capability to control access to information. Information providers who seek control over users' attention increasingly focus on search engines to maximize exposure to their own materials, and minimize exposure to information and informational works provided by their competitors. For a discussion of the role of search engines and the legal attempts to regulate them, see Niva Elkin-Koren, *Let The Crawlers Crawl: On Virtual Gatekeepers and The Right to Exclude Indexing,* 26 U. DAYTON L. REV. 179 (2001).

[80] A dynamic IP address is analogous to a "temporary phone number[,] for the duration of that Internet session or for some other specified amount of time. Once the user disconnects from the Internet, their [*sic*] dynamic IP address goes back into the IP address pool so it can be assigned to another user. … [U]sing a dynamic IP address is similar to using a pay phone." Interactive Advertising Bureau UK, Interactive Jargon Buster (Sept. 7, 2002), *at* http://www.interactivejargonguide.org/Glossary/Term /Dynamic+IP+Address. However, unlike a payphone, the ISP can identify the user.

[81] An "anonymizer service" is a "privacy service that allows a user to visit Web sites without allowing anyone to gather information about which sites they [*sic*] visit and without allowing a visited Web site to gather information about them, such as their IP address." SearchSecurity.com, Definitions: Anonymizer, *at* http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci775657,00.html (last updated Jan. 16, 2002). For an example of such a service, see http://www.anonymizer.com/.

[82] A user can, however, go to an Internet café or a public library to gain anonymity. This option has not escaped the eyes of the legislators. See *infra* Part IV.B.5.

B. Virtual Gatekeepers and the Legal Regime

51. The characteristics of OSPs that were recognized by governments as useful for implementing governmental policies also attracted civil suits against OSPs. Suits by third parties, such as copyright owners, sought to exploit the OSPs' monitoring capability to enforce copyright compliance. While the first generation of copyright suits sought to hold ISPs liable to copyright infringements committed by their users, the second generation of suits targeted peer-to-peer facilitators such as Napster.[83] The much-publicized campaign of the Recording Industry Association of America against individual users of peer-to-peer systems, identified through their service providers, is another example.[84] And suits among competing OSPs were brought to limit alternative gateways in the market and preserve dominant positions over access to services or information.[85]

52. The legal regime that emerged during the 1990s increasingly turned these online gateways into virtual *gatekeepers*. To be precise, the advantage in controlling online traffic or affecting access to information is the outcome of a technological necessity, a particular architecture, or a business model. Indeed, OSPs or search engines have a technical advantage over other nodes in the form of enhanced monitoring capabilities. Yet the legal regime that emerged from court decisions and legislation during the 1990s strengthened the power enjoyed by existing gateways, facilitating their development as virtual gatekeepers. The legal regime facilitated this process in two ways: first, by weakening competition, thereby increasing the power of each OSP to exclude information, services, and/or their providers. The legal regime weakened competition and facilitated the dominance of fewer players by creating barriers

---

[83] *See, e.g.,* Religious Technology Center v. Netcom On-Line Communications Services, 907 F. Supp. 1361 (N.D. Cal. 1995). The court exempted Netcom, the ISP, from direct liability and vicarious liability for copyright infringement committed by a subscriber, who posted portions of the Religious Technology Center's copyrighted works. The court held, however, that Netcom might be liable for contributory infringement. Under the *Netcom* rule, in order to establish contributory liability, the plaintiff must show that the defendant (1) had knowledge of the infringing activity and (2) induced, caused or materially contributed to the infringing conduct of another. Vicarious liability will be imposed when the defendant (1) had the right and ability to control the infringer's acts, and (2) received a direct financial benefit from the infringement. In Ellison v. Robertson, 189 F. Supp. 2d 1051 (C.D. Cal. 2002) the court rejected plaintiff's demand to impose direct liability on AOL, the ISP, for copyright infringement by a fan, who uploaded his favorite author's novel to a newsgroup on the Internet. The plaintiff asserted that AOL was liable for allowing the books to reside for two weeks on its USERNET server. The second generation of copyright lawsuits sought to hold peer-to-peer facilitators liable for copyright infringements committed by their subscribers. *See, e.g.,* A&M Records, Inc. v. Napster*,* Inc*.,* 239 F.3d 1004 (9th Cir. 2001) (holding Napster liable for its users' copyright infringements).

[84] *See* In re Verizon Internet Services, Inc., 240 F. Supp. 2d 24 (D.D.C. 2003) and the RIAA's own press release, *Recording Industry to Begin Collecting Evidence and Preparing Lawsuits Against File "Sharers" Who Illegally Offer Music Online* (June 25, 2003), *at* http://www.riaa.com/news/newsletter/062503.asp (last visited Aug. 25, 2003).

[85] *See* Ticketmaster Corp. v. Tickets.com, Inc*.,* No. 99-7654, 2000 U.S. Dist. LEXIS 4553 (C.D. Cal. Mar. 27, 2000). In *Ticketmaster*, the plaintiffs sued a Web site operator who offered tickets and information for various events, claiming that the defendant's deep linking to their site violated the federal copyright act, among other laws. *See also* eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058 (N.D. Cal. 2000). Bidder's Edge was an auction aggregator site that allowed users to search for items across numerous online auctions; eBay claimed the defendant's automated agents burdened eBay's computer system and harmed its reputation.

to entry, failing to prevent anticompetitive behavior, and endorsing strong property rights. Second, legal rules affected the rise of gatekeepers by assigning OSPs with certain duties regarding the behavior of their users, or by providing them with certain immunities, thereby shaping the relationships between OSPs and Internet users.

1. Facilitating Concentration

53. A gateway functions as a gatekeeper when users are forced to use it and practically have no reasonable alternatives for accessing information on the Web. Even though none of the gateways currently operating on the web enjoys hegemony, it is arguable that the effect of OSPs on designing access, denying access, or blocking it altogether would be stronger in a market that is less competitive and where users have fewer options. A more concentrated information market, handled by only a few gatekeepers, is of course more easily governed. The legal regime that developed during the 1990s posed impediments to competition and barriers to entry in several ways. These, in turn, facilitated the concentration of power in the hands of a few private entities.

a. Broad Interpretation of Rights

54. One example is the broad rights accorded to some players against their competitors in the online environment. This resulted in market domination, forcing the creation of business alliances that were otherwise unnecessary. The *eBay* case is illustrative. eBay, the largest online auction site, brought a suit against Bidder's Edge, a metacrawler of auction sites, which allowed its users to search for items simultaneously across various online auctions sites.[86] eBay objected to the indexing of transactions facilitated on its Web site and was granted a preliminary injunction enjoining Bidder's Edge from accessing eBay's system by the use of any automated querying program. Bidder's Edge no longer exists, and the court's ruling certainly strengthened eBay's dominant position in the online auction market.[87] In fact, the *eBay* rule allows strategic behavior against competitors and therefore impedes competition among search engines and facilitates the concentration of power by very few search engines. Data regarding the search engine market suggests that it is a market governed by only a small number of companies, and that most of the search traffic is managed by a few search engines, some of which are affiliated.[88] The search

---

[86] *eBay*, 100 F. Supp. 2d. at 1060-63.

[87] Findings from the Nielsen/NetRatings and Harris Interactive eCommercePulse, collected from an online survey of 35,000 web users in May 2001, show that eBay's share in the online auction category was 64.3% of total auction revenues. The rest was divided among uBid (with 14.7%), Egghead.com (4%), Yahoo! Auctions (2.4%), and Amazon.com (2%.) *See* Troy Wolverton, *eBay Riding Net Auction Industry's Wave*, CNET.COM, June 28, 2001, *at* http://news.com.com/2100-1017-269211.html?legacy=cnet.

[88] There are several examples of this affiliation. Google "provide[s] editorial search results and paid listings to AOL's various search properties in the United States, including AOL Search, Netscape Search and CompuServe Search." Danny Sullivan, *Overture & Inktomi Out, Google in at AOL*, THE SEARCH ENGINE REPORT (May 1, 2002), *at* http://www.searchenginewatch.com/sereport/02/05-aol.html. In addition, Ask Jeeves "carr[ies] paid listings from Google on its search properties," including Ask Jeeves-owned Teoma.com. Danny Sullivan, *Ask Jeeves To Carry Google's Ads,* THE

engines market is arguably governed by only five major companies: MSN, Yahoo!, Google, AOL, and Ask Jeeves.[89]

55. Reduced competition in the online environment and increased concentration were further facilitated by implementation of the DMCA anti-circumvention legislation.[90] That legislation created situations where encryption was used to prevent the development of complementary products that required interoperability. The cases of RealNetworks[91] and Sony PlayStation[92] are illustrative.

SEARCH ENGINE REPORT (Aug. 5, 2002), *at* http://www.searchenginewatch.com/sereport/02/08-ask.html.

[89] Reported market share for each search engine differs among the various surveys. A survey by Nielsen/NetRatings measuring audience reach in June 2002 (the percentage of U.S. Internet users estimated to have searched on each site at least once during the relevant period) shows MSN having reached 28.6% of U.S. Internet users, Yahoo! 27.7%, Google 26.4%, AOL 18.7%, and Ask Jeeves 11.2%. Kathy Varjabedian, *Search Engines: What are People Using?*, RESEARCH LIBRARY NEWSLETTER (Sept. 2002), *at* http://lib-www.lanl.gov/libinfo/news/2002/200209.htm. A similar survey, conducted by another Internet analysis service in March 2002, shows MSN having reached 37% of the market, Yahoo! 34%, Google 28.9%, AOL 22.4%, and Ask Jeeves 15.7%. (Because an Internet user may visit more than one service, the combined total exceeds 100%.) Danny Sullivan, *Jupiter Media Metrix, Search Engine Ratings*, THE SEARCH ENGINE REPORT (April 29, 2002), *at* http://www.infinityinformations.com/search_engine_optimization/search_engine_optimization_popularity_us.html. *But see* Danny Sullivan, *Google Tops in Search Hours Rating*, THE SEARCH ENGINE REPORT (May 6, 2002), *at* http://www.searchenginewatch.com/sereport/article.php/2164801 (claiming that according to the search hours measurement, Google is the most popular; search hours were calculated by multiplying "unique visitors by average time spent per visitor").

[90] *See* Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to Be Revised*, 14 BERKELEY TECH. L.J. 519 (1999).

[91] RealNetworks Inc. v. Streambox Inc., 2000 U.S Dist. Lexis 1889 (W.D. Wash. Jan. 18, 2000). RealNetworks developed software products that "enable consumers to access audio and video content over the Internet, without downloading it to their personal computer, in a process known as 'streaming.' " *Id.* at *3. RealNetworks' products enable owners of audio and video content to make their content available for consumers to hear or to view, while at the same time securing the content against unauthorized access or copying. *Id.* at *4. The defendant provided software products, among them the Streambox VCR, which enabled end-users to download copies of audio and video files that were streamed over the Internet using RealNetworks' application. *Id.* at *10. The court accepted RealNetworks' claim that the defendant violated the DMCA, 17 U.S.C § 1201, and issued a preliminary injunction against the defendant. *Id* at *20.

[92] Sony Computer Entm't Am. Inc. v. GameMasters, 87 F. Supp. 2d 976 (N.D. Cal. 1999). The defendants sold in their store a device known as "Game Enhancer." *Id.* at 986. When the "Game Enhancer" is plugged into the Sony PlayStation game console, it "permits users to modify the rules of a specific game," *id.* at 981, and permits players to play imported games, which Sony intended "for use exclusively on Japanese or European PlayStation consoles," *id.* The court ruled that "[t]he Game Enhancer circumvents the mechanism on the PlayStation console that ensures the console operates only when encrypted data is read from an authorized CD-ROM," *id.* at 987, and thus the defendant likely violated the Digital Millennium Copyright Act (17 U.S.C. § 1201), *id.* at 988. In *Sony Computer Entm't, Inc. v. Connectix Corp.*, 48 F. Supp. 2d 1212, 1215 (N.D. Cal. 1999), the defendant made and sold a software program called "Virtual Game Station," which allowed playing Sony PlayStation games on a regular computer and not only on Sony PlayStation console. Sony also asserted, among its other claims, that the defendant violated § 1201 of the DMCA. The District Court accepted Sony's claims about copyright infringement. The Court of Appeals for the Ninth Circuit reversed this decision. Sony Computer Entm't, Inc. v. Connectix Corp., 203 F.3d 596 (9th Cir. 2000). *See also* Sony Computer Entm't Am. Inc. v. Bleem LLC., 214 F.3d 1022 (2000). However, both Connectix and Bleem were unable to bear the high costs of litigation against Sony and ultimately were forced to pull their products off the market. *See generally* Electronic Frontier Foundation, *Unintended Consequences: Three Years under the DMCA*, *at* http://www.eff.org/IP/DMCA/20020503_dmca_consequences.html (exploring the effects of the anti-circumvention provisions of the DMCA).

56. These examples demonstrate how the State's position facilitated concentration: imposing liability or broadly interpreting rights (and in some cases recognizing new rights) without paying attention to concerns such as competition and open access. Yet sometimes the State's inaction regarding the development of powerful monopolies in the information environment facilitated concentration. Examples include government inaction on Microsoft before the Microsoft case[93] and the approval of the AOL Time Warner merger.[94]

b. Higher Barriers to Entry

57. Another type of barrier to entry is cost. The legal regime developed in recent years significantly increased the costs, including the legal costs, involved in operating an online service. One reason for the increased legal costs involved in providing online interactive services is the potential liability for injurious content posted by users.[95]

58. A second reason for increased legal costs is the recognition of new property interests that require the purchase of licenses for routine Internet functions. For instance, new European legislation[96] and several court decisions prohibited unauthorized data mining[97] and deep linking,[98] thereby entitling

---

[93] *See* Bruce A. Epstein, *Does the DoJ prefer a Microsoft Monopoly?* THE O'REILLY NETWORK, para. 1 (Nov. 16, 2001), *at* http://www.oreillynet.com/lpt/wlg/872 (suggesting the U.S. government negotiated with Microsoft after the court ruling that Microsoft "abused its monopoly power" because the government "seek[s] Microsoft's cooperation in electronic surveillance").

[94] Scholars express their concerns that without suitable remedies, the merger will create strong incentives for AOL Time Warner to discriminate against unaffiliated conduits and content providers. *See* Daniel L. Rubinfeld & Hal J. Singer, *Open Access to Broadband Networks: A Case Study of the AOL/Time Warner Merger*, 16 BERKELEY TECH. L.J. 631 (2001). Some scholars even criticized the review and approval of the merger by the European Union's Directorate-General for Competition of the Commission of the European Communities ("Competition Commission"), given the potential dominance by AOL Time Warner of Internet access and the entity's ability to become a gatekeeper in the digital environment. *See* James M. Turner, Note and Comment, *Mega Merger, Mega Problems: A Critique of the European Community's Commission on Competition's Review of the AOL-/Time Warner Merger*, 17 AM. U. INT'L L. REV. 131 (2001).

[95] An ISP must adopt a notice and take-down policy in order to escape liability. *See* 17 U.S.C. §512(c)(2), (3); 3 MELVILLE NIMMER & DAVID NIMMER, ON COPYRIGHT § 12B.04 (2002).

[96] *See* Council Directive 96/9/EC of 11 March 1996 on the Legal Protection of Databases, 1996 O.J. (L 77) 20, *available at* http://europa.eu.int/ISPO/infosoc/legreg/docs/969ec.html [hereinafter Database Directive].

[97] See, for example, *eBay, Inc. v. Bidder's Edge, Inc*., 100 F. Supp. 2d 1058, 1069-70 (N.D. Cal. 2000), where the court held that unauthorized automated search on eBay's site was trespass to chattels. The eBay rule allows the owners of search engines and searchable sites to prevent any undesirable (potentially competitive) use of data. A search engine could seek an injunction against a metacrawler or any automated use of the site. This new property right in cyberspace was criticized, *see, e.g.,* Dan L. Burk, *The Trouble with Trespass*, 4 J. SMALL & EMERGING BUS. L. 27, 27-28 (2000), and was not followed by the California Supreme Court. *See* Intel Corp. v. Hamidi, 1 Cal. Rptr. 3d 32 (2003).

[98] A Danish court prohibited Newsbooster.com, a site that provided links to news sites all over the world, from deep linking to Web sites of Danish newspapers. *See* The Associated Press, *Danish Court Rules against News Links at Web Site*, THE IHT ONLINE (July 6, 2002), para. 1, *available at* http://www.iht.com/ihtsearch.php?id=63676&owner=The%20Associated%20Press)&date=20020708170446. *See also* Michelle Delio, *Deep Link Foes Get Another Win*, WIRED NEWS, July 8, 2002, *at* http://www.wired.com/news/politics/0,1283,53697,00.html. The court held that Newsbooster.com was in direct competition with the plaintiffs' newspapers, and thus the deep linking to specific news articles damaged the value of the newspapers' advertisements. The Associated Press, *supra,* at para. 2. A

every Web site and content provider to determine how and to what extent their site could be indexed. A right to exclude data mining and indexing reduces competition in the search engines market. When search engines must acquire a license to locate and refer to information that has already been posted online, the costs of operating a search engine increase. This increase is due to higher transaction costs involved in negotiating and acquiring the necessary licenses and paying the license fees. The commercialization of the reference process increases barriers to entry and allows a considerable advantage to commercial engines. Commercialization also creates a bias toward large commercial sites that could use this advantage to control the indexing process, condition licensing in exchange for a higher ranking, or condition licensing on the exclusion of competitors from the search results. Low barriers to entry guarantee the decentralized nature of the Internet. When the costs of online operation are high fewer players are able to engage in online activities.

2. Encouraging OSPs to Exercise Policing Power

59. Another way legal rules affected the rise of gatekeepers was by shaping the relationships between OSPs and their users. Liability rules impose on OSPs certain duties to inspect and monitor the behavior of their users. The potential liability encourages, and often forces, OSPs to perform policing functions, and to some extent turns them into the long arm of right holders and private enforcement agents. In other cases rules provide for certain exemptions and immunities,[99] thus strengthening the power of some players in the online environment.[100]

60. While, by the mid-1990s, U.S. courts ruled that OSPs should not be held directly liable for copyright infringements committed by their users,[101] liability of OSPs was invoked under two other copyright doctrines: contributory infringement and vicarious liability.[102] Under the doctrine of contributory infringement the plaintiff must establish that an end-user committed direct infringement (namely that it used one of the copyright owner's exclusive

---

German court handed down a similar ruling, holding that deep linking by the search service NewsClub directly to the German newspaper Mainpost's content violated the European Database Directive, *supra* note 96, which "protects against the 'unfair extraction' of materials contained in a database, specifically mentioning downloading or hyperlinking as examples of prohibited extraction methods." Michelle Delio, *Deep Linking Takes Another Blow*, WIRED NEWS, July 25, 2002, para. 1, 2, 4, *at* http://www.wired.com/news/print/0,1294,54083,00.html. In *Kelly v. Arriba Soft Corp*., 280 F.3d 934 (9th Cir. 2002), the court prohibited Arriba, a search engine, from deep linking to Kelly's full-size images because it violated Kelly's exclusive right to publicly display his copyrighted works. This decision was later withdrawn, due to procedural considerations. *See* Kelly v. Arriba Soft Corp., 336 F.3d 811 (9th Cir. 2003).

[99] *See, e.g.,* 17 U.S.C. § 512(i). *See also* Peer to Peer Piracy Prevention Act, H.R. 5211, 107th Cong. (2002), *available at* http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_bills &docid=f:h5211ih.txt.pdf. This bill, introduced by Representative Howard Berman, would grant copyright holders near immunity against legal action stemming from the copyright holder's involvement in network vandalism against users suspect of copyright infringement in peer-to-peer (P2P) networks. This bill has generated much concern. *See* The Digital Speech Project, The Berman Bill, *at* http://www.digitalspeech.org/berman.shtml.

[100] See the immunity clauses of the DMCA (safe harbor provisions) at 17 U.S.C. § 512(a)-(d).

[101] *See, e.g.*, Religious Tech. Ctr., 907 F. Supp. at 1372; *see also supra* note 83 (discussing *Religious Technology Center*).

[102] *See, e.g.*, Religious Tech. Ctr., 907 F. Supp. at 1373, 1375.

rights without authorization), that the OSP *knew or should have known* of the user's direct infringement, and that it *materially contributed* to the direct infringement.[103] Liability will not be imposed if there are substantial non-infringing uses.[104] An OSP could be further held liable for vicarious infringement when an end-user commits direct infringement,[105] provided that the OSP has the right and ability to control the direct infringer and derives direct financial benefit from such activities.[106] In the *Napster* case, the Ninth Circuit provided an expansive interpretation to both contributory and vicarious infringement.[107] The court found that upon receiving a notice from a right-holder regarding allegedly infringing materials using its system, Napster should have taken reasonable steps, including implementing technical changes in its system, to stop the infringing behavior, or else face liability.[108]

61. Similarly, the standard for vicarious liability set by the court was very low, holding that the mere ability to terminate user accounts or block user access to the system was enough to constitute "control."[109] Financial benefit from the infringing activity was interpreted by the court to include evidence that the availability of infringing material acts as a draw for customers.[110] The potential of liability, even in the absence of actual knowledge of the infringing actions, encourages OSPs to monitor the behavior of their users and control their conduct to reduce potential legal risk.

62. These legal doctrines, as interpreted and implemented by courts, establish the legal framework for OSPs exercising policing power over their users. The court in *Napster* explicitly held that "the reserved right to police must be exercised to its fullest extent. Turning a blind eye to detectable acts of infringement for the sake of profit gives rise to liability."[111]

63. To avoid liability, either by preventing the distribution of potentially injurious materials in the first place, or by satisfying the requirements of the DMCA safe harbor provisions, an OSP must establish a system that either pre-screens content, or scrutinizes material that has already been posted, or implements a "notice and take down" policy (in which an OSP collects complaints of copyright owners, passes those complaints to the alleged infringers, and removes the infringing materials).[112] The high cost involved in escaping

---

[103] *See id.* at 1373.
[104] *See, e.g.*, Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417 (1984).
[105] *See* Religious Tech. Ctr., 907 F. Supp. at 1375.
[106] *See id.*; A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1023-24 (9th Cir. 2001).
[107] *See* Napster, 239 F.3d at 1019-24; In re Aimster Copyright Litigation, 334 F.3d 643 (2003).
[108] *See* Napster, 239 F.3d at 1021 ("if a computer system operator learns of specific infringing material available on his system and fails to purge such material from the system, the operator knows of and contributes to direct infringement.")
[109] *See id.* at 1023 ("The ability to block infringers' access to a particular environment for any reason whatsoever is evidence of the right and ability to supervise.").
[110] *See id.* ("Financial benefit exists where the availability of infringing material 'acts as a "draw" for customers.' . . . Napster's future revenue is directly dependent upon 'increases in user base.' More users register with the Napster system as the 'quality and quantity of available music increases.'" (citations omitted)).
[111] *Id.*
[112] The ISP must assign a special agent (designated agent) for receiving the notifications regarding copyright infringements. 17 U.S.C. §512(c)(2). The notifications function as a "red flag" before the

liability, through legal counseling or insurance, increases the cost of providing interactive online services and reduces competition in that market. Therefore, applying such a standard of liability for injurious content distributed by users could impede competition in the intermediary markets.

64. The safe harbor provisions under the DMCA, which arguably intended to reduce potential legal exposure for OSPs, further encourage monitoring and supervision of online distribution. The provisions require an OSP to undertake technical and legal procedures in order to escape liability for copyright infringement when subscribers are using its service for copyright infringement.[113] Even though the DMCA imposes no duty to monitor the service for copyright infringements,[114] OSPs are exempted from liability, provided that they undertake some enforcement responsibilities. To be eligible for the exemptions, an online service provider must accommodate the technical measures adopted by copyright owners, allow termination of service to repeated infringers, and handle infringements complains by an appointed copyright agent implementing a "Notice and Take-Down Policy." By implementing copyright enforcement policies, online service providers are enrolled in protecting the online interests of right holders, performing some roles that are normally reserved to the courts and the police.

65. Similar provisions were adopted by the European Community in the Directive on E-Commerce.[115] Indeed, the Directive does not impose a general obligation to monitor information provided on its services, nor does it require providers to actively "seek facts or circumstances indicating illegal activity."[116] Still, it permits member States to establish obligations of providers to inform the authorities of alleged illegal activities discovered or reported by subscribers.[117]

66. Google's March 2001 decision to remove links to files that allegedly infringed the rights of the Church of Scientology reflects the censorial power that OSPs such as Google enjoy.[118] The Church of Scientology demanded that Google remove Operation Clambake Web pages from its search engine, complaining that the materials on that site infringed the Church's copyrights. Google explained that it was forced to remove the links rather than risk litigation.[119]

---

service provider. *See* 3 MELVILLE NIMMER & DAVID NIMMER, ON COPYRIGHT § 12B.04[1] (2002). In addition, the notification from the copyright owners must comply with the requirements detailed in 17 U.S.C. §512(c)(3). *See* 17 U.S.C. §512(c)(3); NIMMER, *supra*, § 12B.04.

[113] *See* 17 U.S.C. § 512(a)-(d).

[114] 17 U.S.C.A. § 512(m) ("Nothing in this section shall be construed to condition the applicability of subsections (a) through (d) on - (1) a service provider monitoring its service or affirmatively seeking facts indicating infringing activity, except to the extent consistent with a standard technical measure complying with the provisions of subsection (i) … .") .

[115] *See* E-Commerce Directive, *supra* note 69, at art. 12-14.

[116] *Id.* at art. 15(1).

[117] *Id.* at art. 15(2).

[118] *See* Declan McCullagh, *Google Yanks Anti-Church Sites*, WIRED NEWS, Mar. 21, 2002, *at* http://www.wired.com/news/politics/0,1283,51233,00.html. Under pressure from the Church of Scientology, Google removed Operation Clambake's Web pages, a scientology-protest Web site based in Norway, from its search engine database. *Id.* at para.6, 11.

[119] E-mail from Google.com to Operation Clambake (Mar. 20, 2002), *available at* http://xenu.net/news/20020320-google.txt ("We removed certain specific URLs in response to a notification submitted by the Religious Technology Center and Bridge Publications under section

The implementation of such censorial authority is encouraged by the current regime. Thus, liability rules have established a framework for using online service providers for policing purposes.

C. Convergence of Interests: How Unholy Alliances Form

67. It is interesting to note the current convergence of interests of some (but not all) of the private commercial players and the government's interests. Each side's interests predate September 11 and the legal reform that followed, but the convergence of these interests has never been as apparent and strong as it is now.[120]

68. Copyright owners, for example, have great interest in imposing liability on certain OSPs. It is easier and far more effective for right holders to sue the OSP. Due to the inherent enforcement failure, most copyright owners — the RIAA being a notable exception — prefer not to go after end-users who infringe the copyright.[121] In addition to the difficulties and costs of locating the infringer, the cost of suing him or her and the legal risk it involves far exceed the actual damage and hence do not justify bringing suit. The public relations implications that naturally arise when a provider sues its clients add to this. The OSP, in contrast, usually has a "deeper pocket" and is also capable of monitoring and blocking infringing activity.

69. Several legal doctrines, such as the doctrine of contributory infringement, serve to make the technical bottleneck a legal one.[122] Naturally, OSPs object to this attempt and do not wish to serve as the policing long-arm of the copyright owner, as the *Napster* case taught us.[123]

70. The State has an interest, under the model we described, that private nodes of power — gatekeepers — maintain their power, so that the State can later recruit it to its own needs. As long as this does not conflict with the industry's goals, the State has an ally. But interests are bound to conflict, and then we are likely to face new "power & control" battles, until a new equilibrium is reached. Furthermore, one might speculate that conflicting agendas will emerge *within* the private sector. Some industries — ISPs for example — might find themselves under pressure from the State, and simultaneously under pressure from copyright owners who seek a more convenient bottleneck to block unauthorized uses of their works.

512(c)(3) of the Digital Millennium Copyright Act (DMCA). Had we not removed these URLs, we would be subject to a claim for copyright infringement, regardless of its merits.").

[120] *See* Julie E. Cohen, *Information Rights and Intellectual Freedom*, *in* ETHICS AND THE INTERNET 11-32 (Anton Vedder, ed., 2001) (noting the convergence of commercial and law enforcement interest before September 11).

[121] However, it has recently been reported that the music industry is doing just that. *See* John Borland, *The Record Labels' New Target: Users*, ZDNET UK NEWS, July 4, 2002, *available at* http://news.zdnet.co.uk/story/0,,t269-s2118507,00.html.

[122] *See* Napster, 239 F.3d 1004.

[123] The district court in *Napster* and the court of appeals differed on this point. Whereas the district court's injunction turned Napster, de facto, into a policing long-arm of the copyright owners, the court of appeals required the copyright owners to do the policing themselves, and provide Napster with lists of infringed files on the Napster system. *Id.* at 1027.

71. At present, the copyright owners' interests and the governmental interests in utilizing the monitoring advantage of OSPs converge. Of course, the convergence is incomplete, for copyright owners would prefer to see some OSPs disappear (*e.g.*, Napster), whereas the government has an interest in maintaining these centralized nodes of private power, so it can have a "free ride" from them. Such was the case when the bills that resulted in the enactment of the USA PATRIOT Act were pending in the Senate and in the House of Representatives. The RIAA lobbied for inserting a section that would immunize copyright owners from legal actions if they caused damage while taking technical measures to prevent infringements. This attempt was received with harsh criticism and was characterized in the press as a plan to hack users' computers.[124] The RIAA was quick to explain this move as a response to an "inadvertent mistake" in the bill, which would have outlawed the use of technical measures to enforce copyright.[125] While this episode might have been an unfortunate misunderstanding, it exemplifies the close ties of the RIAA with Congress, and the convergence of interests. Another incident once again had to do with the RIAA's attempts to utilize the power of intermediaries to further its (legitimate in themselves) needs of enforcing its copyrights. The RIAA proposed to the Copyright Office, during a rule-making process, to require Web-casters to collect information on users' listening habits. The listener's log, the Copyright Office explained on behalf of the RIAA, is needed "to monitor compliance." Once again, the public outcry resulted in the RIAA's withdrawing its proposal.[126]

72. We now turn to illustrate our argument that the State is recruiting private powers to serve its interests as a provider of national security.

IV. The Nature of the Emerging Legal Regime

A. Legal Framework for Seizing Control Online

73. So far we have seen that State intervention in the digital environment may take various forms. The urgent need to exercise State power in a decentralized global network, especially in light of global threats to individual safety and national security, gave rise to the co-optation of online players in law enforcement missions. Law enforcement agencies in the United States and around the world enjoy a wide range of powers to fulfill their mission as providers of national security with regard to prior prevention, investigation, and prosecution. In this section we focus on a segment of these, namely situations in which the State through the police and intelligence agencies, has the legal authority to draft private nodes of power to its service. The authorities are scattered in various statutes, and are subject to constitutional imperatives, such as the First and Fourth Amendments of the Constitution of

---

[124] *See, e.g.,* Declan McCullagh, *RIAA Wants to Hack Your PC,* WIRED NEWS, Oct. 15, 2001, *available at* http://www.wired.com/news/politics/0,1283,47552,00.html.

[125] See the RIAA's report of the events: Letter to Editor from RIAA to Billboard Magazine, Response to Billboard Article on Anti-Terrorism Bill (Oct. 24, 2001), *at* http://www.riaa.com/news/newsletter/press2001/102401.asp.

[126] *See* Brenda Sandburg, *Groups Fear Webcast Listeners Will Lose Privacy*, THE RECORDER, Apr. 12, 2002, *available at* http://www.law.com/jsp/newswire_article.jsp?id=1022183115313.

the United States or the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR).

74. The legal battle against terror began long before September 11, but the legislation that followed those tragic events reflects a change of attitude, especially in regard to the digital environment. To some extent the information environment was perceived as an arena for fighting terror before September 11. Bills identifying online threats to national security were already introduced in the late 1990s. These bills reflect various concerns regarding terrorist-related activities on the Internet, including online sales of weapons and ammunition,[127] and the availability of technologies or information that could become useful for mass destruction.[128] Many bills addressed the regulation of encryption, seeking to secure freedom to use encryption products, but also providing authority to prohibit the export of products, for national security reasons.[129] Some concerns also focused on "cyberterrorism," designated as "an emerging threat to the national security of the United States," and called for "a partnership between the Federal Government and private industry in combating the 'cyber menace' [and] a revised legal framework for the prosecution of 'hackers' and 'cyberterrorists'… ."[130] Nevertheless, only a few of these bills were eventually enacted.[131] Prior to September 11 one could find only scattered references to the digital environment in the context of anti-terrorist legislation. The Wiretap Act, for example, included a reference to

---

[127] *See* H.R. 4114, 105th Cong. (1998); Internet Gun Trafficking Act of 1999, H.R. 1245, 106th Cong. (1999); Internet Gun Trafficking Act of 1999, S. 637, 106th Cong. (1999) (prohibiting the online sale or exchange of firearms); H.R. 87, 106th Cong. (1999) (prohibiting Internet and mail-order sales of ammunition). *See also* Electronic Commerce Crime Prevention and Protection Act, H.R. 3020, 106th Cong. (1999); H.R 1702, 106th Cong. (1999); H.R. 726, 107th Cong. (2001) (a proposal to amend Title 18, United States Code, to ban using the Internet to obtain or dispose of a firearm).

[128] *See* Defense Against Weapons of Mass Destruction Act of 1996, H.R. 3730, 104th Cong. (1996) (referring to the Internet in the Finding section: "(1) Weapons of mass destruction and related materials and technologies are increasingly available from worldwide sources. *Technical information relating to such weapons is readily available on the Internet* …" (emphasis added)); Chemical Safety Information, Site Security and Fuels Regulatory Relief Act, S. 880, 106th Cong. (1999) (authorizing the President to assess the risk of terrorist and other criminal activity associated with the posting of off-site consequence analysis information on the Internet.) This bill became Public Law No. 106-40.

[129] *See, e.g.,* Promotion of Commerce On-Line in the Digital Era (Pro-CODE) Act of 1996, S. 1726, 104th Cong. (1996) (authorizing regulation by Secretary of Commerce); Promotion of Commerce On-Line in the Digital Era (Pro-CODE) Act of 1997, S. 377, 105th Cong. §5 (3)(b) (1997) (authorizing limits on export of computer software and hardware if suspected that they will be modified for military or terrorist end-use); Encryption Protects the Rights of Individuals from Violation and Abuse in Cyberspace (E-PRIVACY) Act, S. 2067, 105th Cong. (1998); Encrypted Communications Privacy Act of 1997, S. 376, 105th Cong. (1997); Security and Freedom Through Encryption (SAFE) Act, H.R. 695, 105th Cong. (1997); Electronic Rights for the 21st Century Act, S. 854, 106th Cong. (1999); Promote Reliable On-Line Transactions to Encourage Commerce and Trade (PROTECT) Act of 1999, S. 798, 106th Cong. (1999); Security and Freedom through Encryption (SAFE) Act, H.R. 850, 106th Cong. (1999); Encryption for the National Interest Act, H.R. 2616, 106th Cong. (1999).

[130] H.R. Con. Res. 285, 106th Cong. (2000), *available at* http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_cong_bills&docid=f:hc285ih.txt.pdf (expressing the sense of Congress regarding Internet security and "cyberterrorism"); *see also* H.R. Con. Res. 22, 107th Cong. (2001) (expressing the same).

[131] Chemical Safety Information, Site Security and Fuels Regulatory Relief Act, which became Pub. L. No. 106-40, 113 Stat. 207 (1999); Protection of Children from Sexual Predators Act of 1998, Pub. L. No. 105-314, § 801, 112 Stat. 2974, 2990 (codified as amended at 18 U.S.C. § 4042 note (1999)) (restricting unsupervised access to the Internet by State prisoners).

electronic communication.[132] In the United Kingdom, a 2000 Act addressed interception in the digital environment as well as data retention by service providers. These examples reflect the pre-9/11 attitude to the Internet. The Internet was conceived as one of a few means of communications that might be (ab)used by terrorists, as well as other cyber-criminals. The new communication devices (such as e-mails sent from cellular phones or an Internet café) and the new systems of inspection and interception called for adaptations of laws governing surveillance and seizure.[133] While some amendments aiming at updating the law were adopted prior to September 11, most of the relevant changes in the law were passed after the tragic events.

75. In the September 11 aftermath, terrorism is perceived as a major threat to civilization, and the Internet is conceived of as a whole new territory where terrorist activities might take place; hence it is a territory of interest to the State's various security agencies. The definitions of cyberterror are quite broad and rather vague.[134] Cyberterror is often confused, perhaps deliberately, with cybercrime.[135] The Internet, which turned out to be so central to individuals' everyday lives, was discovered as a significant arena for data-mining, a resource neglected by public authorities. It was now realized that data mining could be used in the "war against terror" for investigation, inspection, interception, and governing.

76. This change in the State's attitudes to the Internet was reflected in the post-9/11 legislative efforts. The most typical example of these efforts is the **U**niting and **S**trengthening **A**merica by **P**roviding **A**ppropriate **T**ools **R**equired

---

[132] *See* 18 U.S.C. § 2511(1)(a) and definition in § 2510(12).

[133] There were a few proposals over the years of anti-terrorism legislation that had some reference to the Internet. For example, the bill which resulted in the Antiterrorism and Effective Death Penalty Act of 1996, Pub. L. No. 104-132, 110 Stat. 1248, initially included a prohibition on distributing information relating to the manufacture of explosives. This proposal was eventually dropped, but § 709 of the Act instructs the Attorney General to conduct a study concerning this issue. The 1997 report submitted to Congress recommended that such legislation be adopted if it can be achieved "in a manner that does not impermissibly restrict the wholly legitimate publication and teaching of such information, or otherwise violate the First Amendment." Dept. of Justice, Report on Availability of Bombmaking Information (1997), *available at* http://www.usdoj.gov/criminal/cybercrime/bombmakinginfo.html. For discussion, *see* David B. Kopel & Joseph Olson, *Preventing a Reign of Terror: Civil Liberties Implications of Terrorism Legislation*, 21 OKLA. CITY U. L. REV. 247, 277-278 (1996); *see also* Amitai Etzioni, *Implications of Select New Technologies for Individual Rights and Public Safety*, 15 HARV. J.L. & TECH. 257 (2002).

[134] The USA PATRIOT Act defines "international terrorism" as "activities that (A) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or of any State; (B) appear to be intended (i) to intimidate or coerce a civilian population; (ii) to influence the policy of a government by intimidation or coercion; or (iii) to affect the conduct of a government by mass destruction, assassination or kidnapping; and (C) occur primarily outside the territorial jurisdiction of the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to intimidate or coerce, or the locale in which their perpetrators operate or seek asylum." 18 U.S.C § 2331.

[135] *See* Ariel T. Sobelman, *Is Everyone an Enemy in Cyberspace?*, 2(4) STRATEGIC ASSESSMENT, Feb. 2000, *available at* http://www.tau.ac.il/jcss/sa/v2n4p4.html; Richard Forno, *You Say Hacker, The Feds Say Terrorist*, SECURITY FOCUS ONLINE, Nov. 21, 2001, *available at* http://online.securityfocus.com/columnists/38.

to **I**ntercept and **O**bstruct **T**errorism (USA PATRIOT) Act of 2001,[136] which was passed by both Houses and signed into law by President Bush on October 26, 2001.[137] Human rights organizations, joined by a number of columnists[138] and other non-profit organizations, warned of the danger the Act posed to human rights,[139] but the public debate was muted. The Act amended no less than 15 other Acts and addressed a wide range of issues.[140] Of interest here are those sections that enhance the intelligence services' powers to gather information, process and share it, while lessening judicial oversight.[141] Similar bills were introduced in the United States during 2002.[142] Congress approved the Homeland Security Act, which includes several amendments to the USA PATRIOT Act, which are of concern here, especially the Cyber Security Enhancement Act (CSEA).[143]

77. Across the Atlantic, the British effort to address the digital environment's

---

[136] H.R. 3162, 107th Cong. (2001). This version incorporated another bill, the Financial Anti-Terrorism Act, H.R. 3004, 107th Cong. (2001).
[137] Pub. L. No. 107-56, 115 Stat. 272 (2001).
[138] *See, e.g.,* Lisa Guernsey, *Living Under an Electronic Eye*, THE NEW YORK TIMES, Sept. 27, 2001, at G1; Robin Toner & Neil A. Lewis, *A Nation Challenged: Congress, House Passes Terrorism Bill Much Like Senate's, but with 5 Year Limit*, THE NEW YORK TIMES, Oct. 12, 2001; Editorial, *Stampeded in the House*, THE WASHINGTON POST, Oct. 16, 2001, at A22; Editorial, *A Panicky Bill*, THE WASHINGTON POST, Oct. 26, 2001, at A34; and critical discussion in Kerr*, supra* note 66.
[139] *See, e.g.,* American Civil Liberties Union, *ACLU Says Congress Should Treat Administration Proposal Carefully; Says Many Provisions Go Far Beyond Anti-Terrorism Needs* (Sept. 20, 2001), *available at* http://archive.aclu.org/news/2001/n092001e.html; ACLU, *ACLU Tells House Judiciary Panel That Administration Seeks Reasonable Anti-Terrorism Tools and Troubling Provisions* (Sept. 24, 2001), *available at* http://archive.aclu.org/news/2001/n092401a.html; ACLU, *As Senate Begins Consideration of Anti-Terrorism Legislation, House Panel Says Concern Over Civil Liberties Requires Slowdown* (Sept. 25, 2001), *available at* http://archive.aclu.org/news/2001/n092501a.html; Electronic Frontier Foundation, *EFF Condemns "Anti-Terrorism" Bill: Legislation Dramatically Curtails Online Civil Liberties* (Oct. 10, 2001), *available at* http://www.eff.org/Privacy/Surveillance/Terrorism_ militias/20011025_ff_usa_patriot_statement.html; EFF, *ALERT: Congressional Response to Terrorism Threatens Privacy – Urge Congress to Legislate to Improve Security Not Eliminate Freedoms* (Sept. 19, 2001) *available at* http://www.eff.org/effector/HTML/effect14.25.html; Electronic Privacy Information Center, *EPIC Letter to Congress on Proposed Anti-Terrorism Legislation* (Oct. 2, 2001), *available at* http://www.epic.org/privacy/terrorism/cong_ltr_10_02_01.html. *See also* IN DEFENSE OF FREEDOM, signed by more than 150 organizations and 300 law professors, *available at* http://www.indefenseoffreedom.org/.
[140] Among these are international money laundering (Title III); border security, immigration (Title IV); benefits for victims of terrorism (Titles IV, VI); and criminal laws against terrorism (Title VIII). A few cases thus far have addressed various sections of the Act. *See U.S. v. Graham*, 275 F.3d 490, 529, 542 (6th Cir. 2001) (discussing the definition of "Federal Crimes of Terrorism"); *Global Relief Foundation, Inc. v. O'Neill*, 207 F. Supp. 2d 779 (N.D. Ill. 2002) (discussing power to freeze assets); *U.S. v. Reid*, 206 F. Supp. 2d 132 (D. Mass. 2002) (finding that an aircraft is not a "vehicle" under the Act). Other cases mentioned the Act, but did not apply it.
[141] *See* USA PATRIOT Act, Title II, Pub. L. No. 107-56, § 201 et seq., 115 Stat. 272 (2001).
[142] *E.g.,* the National Cyber Security Defense Team Authorization Act, S. 1989, 107th Cong. (2002) (proposing "the establishment of a National Cyber Security Defense Team for purposes of protecting the infrastructure of the Internet from terrorist attack"); The Financial Anti-Terrorism Act of 2002, H.R. 3004, 107th Cong. (2002) (prohibiting acceptance of any bank instrument for unlawful Internet gambling to prevent the financing of terrorism and other financial crimes); and The Security and Liberty Preservation Act, S. 2846, 107th Cong. (2002) (stating in the preamble its purpose to "establish a commission to evaluate investigative and surveillance technologies to meet law enforcement and national security needs in the manner that best preserves the personal dignity, liberty, and privacy of individuals within the United States").
[143] Pub. L. No. 107-296, 116 Stat. 2135 (2002).

unique features in regard to the battle against terror predates September 11. These efforts had a wider goal in mind and were not specifically aimed at terror. In 2000 the British Parliament approved the Regulation of Investigatory Powers Act 2000 (RIPA).[144] The Act prohibits, *inter alia*,[145] interception which is "without lawful authority,"[146] authorizes interception without a warrant in certain situations,[147] lists the circumstances in which a warrant can be issued,[148] and regulates in great detail the relevant procedures.[149] The Act also imposes some duties on "telecommunications services," a term which includes Internet service providers (ISPs).[150] The Act was an attempt to achieve several goals: expand law enforcement's ability to gather information in the digital environment; comply with the provisions of the Human Rights Act of 1998 under which interference with the right to privacy is allowed only if it is "in accordance with the law, and is necessary in a democratic society in the interests of national security …";[151] and responds to European law (both legislation and litigation).[152] It also reflects a "fundamental switch away from the reactive policing of incidents to the proactive policing and managing of risks."[153] In this sense, RIPA veined an early appreciation of the digital environment's potential for terrorist activity.

78. Soon after September 11 the United Kingdom enacted an omnibus legislation, responding to the new realization of the changing methods used by terrorists. Like the USA PATRIOT Act, the Anti-Terrorism, Crime and Security Act 2001, which received royal assent on December 14, 2001,[154] amends several other statutes,[155] only some of which relate to the digital environment.[156] In fact, a law review editorial noted that the Act "brings a host of disparate

---

[144] Regulation of Investigatory Powers Act, 2000, c. 23 (Eng.). For review and analysis of the Act, see Yaman Akdeniz, Nick Taylor & Clive Walker, *Regulation of Investigatory Powers Act 2000: Part I: Bigbrother.gov.uk: State Surveillance in the Age of Information and Rights*, CRIM. L. REV., Feb. 2001, at 73.

[145] Other issues addressed are surveillance and covert human intelligence sources (Part II), investigation of electronic data protected by encryption (Part III), and scrutiny of investigatory powers (Part IV).

[146] Regulation of Investigatory Powers Act § 1.

[147] *Id.* § 3.

[148] *Id.* § 5. The Act lists four grounds which render a warrant necessary: national security, preventing and detecting serious crime, safeguarding the economic well-being of the United Kingdom, and prevention of serious crime in other nations. *See id.* § 5(3).

[149] *See id.* Part I.

[150] *Id.* §§ 12, 21-25.

[151] *See* Human Rights Act, 1998, c. 42, § 1 (Eng.), which incorporates part of the European Convention on Human Rights, including Art. 8 thereof, entitled "Right to Respect for Private and Family Life."

[152] *See* Akdeniz et al., *supra* note 144, at 73-75; Jeffrey Yeates, *CALEA and the RIPA: The U.S. and the U.K. Responses to Wiretapping in an Increasingly Wireless World*, 12 ALB. L.J. SCI. & TECH. 125, 131-34 (2001) (discussing the background of the Regulation of Investigatory Powers Act in the European Court of Human Rights' decisions). *See also* Regulation of Investigatory Powers Act § 65 (establishing a tribunal for adjudicating claims against public authorities that are accused of violating the Human Rights Act).

[153] Akdeniz et al., *supra* note 144, at 74.

[154] Anti-Terrorism, Crime and Security Act, 2001, c. 24 (Eng.).

[155] The Act addresses issues such as forfeiture of terrorists' money (Part I), freezing terrorists' bank accounts and other assets (Part II), sharing of information among governmental agencies (Part III), immigration and asylum (Part IV), control of weapons of mass destruction (Part VI), nuclear security (Part VIII), aviation security (Part IX), and police powers (Part X).

[156] One example is Part XI, regarding communications data retention.

measures, some of which are only distantly related, or unrelated, to the security concerns which prompted it."[157] It is fair to say that the 2001 Act strengthens the focus on the digital environment as a potential arena for terrorist activity and makes explicit the earlier, rather implicit, realization of this threat, as embodied in RIPA.[158]

79. The explosive growth of the digital environment during the 1990s enhanced the misuse of the Internet as an instrument of crime – either as a means in the performance of "traditional" crimes, such as using a telephone to coordinate a crime, or to conduct new varieties of crimes, now commonly referred to as "cybercrime." The new technology's unique characteristics, such as its non-territorial and decentralized architecture, have raised new challenges to law enforcement around the world. The Council of Europe, a body in which over 40 European countries are represented, initiated a legal inquiry into this matter as early as 1989,[159] which resulted in the 2001 Convention on Cybercrime.[160] The Convention was adopted by the Committee of Ministers of the Council and opened for signature in November 2001. Thus far, 33 members of the Council have signed it, as have four more non-members, including the United States, which participated in the negotiations that led to the Convention.[161] The Convention has so far been ratified by three countries.[162] It will enter into force once ratified by five countries, at least three of which are member states of the Council.[163]

80. The Convention does not directly address issues of cyberterror, at least not as distinct from cybercrime.[164] Although it was drafted before September 11 (but adopted shortly thereafter), the concepts it reflects are in line with post-September 11 legislation in both the United States and the United Kingdom. The Convention's goals are to harmonize domestic criminal substantive law, to revise domestic criminal procedural law to allow investigations and

---

[157] Editorial, *Anti-Terrorism, Crime and Security Act 2001*, CRIM. L. REV., Mar. 2002, at 159, 159.
[158] The explanatory notes to the Act state its purpose: "to build on legislation in a number of areas to ensure that the Government, in the light of the new situation arising from the September 11 terrorist attacks on New York and Washington, have the necessary powers to counter the threat to the UK." Anti-Terrorism, Crime and Security Act, Explanatory Notes (2001), *available at* http://www.hmso.gov.uk/acts/en/2001en24.htm [hereinafter ATCSA Explanatory Notes].
[159] *See* Recommendation No. R. (89) 9 of the Committee of Ministers to Member States on Computer-Related Crime, Council of Europe (1989), *available at* http://cm.coe.int/ta/rec/1989/89r9.htm.
[160] Convention on Cybercrime, Nov. 23, 2001, Europ. T.S. No. 185, *available at* http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm. For the legislative history of the Convention, see the Explanatory Report (adopted Nov. 8, 2001 by the Committee of Ministers of the Council of Europe) [hereinafter EXPLANATORY REPORT], ¶¶ 12-15, *available at* http://conventions.coe.int/Treaty/en/Reports/Html/185.htm. In November 2002, a protocol addressing hate crimes was added to the Convention. *See* Additional Protocol to the Convention on Cybercrime Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems (Nov. 7, 2002), *available at* http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Combating_economic_crime/Cybercrime/Racism_on_internet/PC-RX(2002)24E.pdf.
[161] *See* U.S. Dept. of Justice, Frequently Asked Questions and Answers: Council of Europe Convention on Cybercrime, *at* http://www.usdoj.gov/criminal/cybercrime/COEFAQs.htm#QA3.
[162] The countries are Albania, Croatia and Estonia. For the current status of the Convention, see http://conventions.coe.int/Treaty/EN/searchsig.asp?NT=185&CM=8.
[163] Convention on Cybercrime, *supra* note 160, art. 36.
[164] For the blurring of the distinction between cybercrime and cyberterror, *see* Sobelman, *supra* note 135.

prosecutions of cybercrimes, and to establish an effective international cooperation network.[165] It requires members to adopt legislation to outlaw various computer-related activities,[166] including offenses related to child pornography[167] and infringement of copyrights;[168] imposes liability on aiding and abetting,[169] mandates certain procedural rules,[170] and establishes a framework for international cooperation.[171] It also addresses the issues that we have mentioned in regard to the U.S. and U.K. legislation, and another that will be discussed shortly: subordinating service providers to law enforcement needs.[172]

81. Other legislatures around the world are considering anti-terror legislation.[173] The legislative instruments just noted are the first and are likely to be the most influential.

B. Recruiting Private Nodes of Control

82. How can a decentralized environment that connects individuals outside the jurisdiction be governed? How do you control and monitor hazardous activities of individuals, often disguised, in a virtual environment? One way of addressing these difficulties is by identifying existing nodes of control, such as infrastructure designers, access providers, and facilitators of online services, and utilizing their prerogative. In this section we examine the legal framework which assigns to private nodes of power in the digital environment a law enforcement role. The discussion that follows is organized according to the kind of intervention or requirement imposed on the ISPs, rather than according to the individual legislative instruments.

1. Technological Capability

83. One sort of State interference in the market is imposing technological capability requirements on various technological junctions and technical bottlenecks in the Internet, especially on connectivity service providers. The intention is clear: to enable law enforcement authorities to intercept communications. The technological capability requirements do not in themselves authorize interception, which requires following separate detailed procedures, usually involving a warrant issued by a judge.[174] The technological capability requirements affect the ISPs' ability to design and

---

[165] EXPLANATORY REPORT, *supra* note 160, ¶ 16.
[166] These activities include illegal access to a computer system (Convention on Cybercrime, art. 2); illegal interception (art. 3); data interference (art. 4); system interference (art. 5); misuse of devices (art. 6); computer-related forgery (art. 7); and computer-related fraud (art. 8).
[167] Convention on Cybercrime, *supra* note 160*,* art. 9.
[168] *Id.* art. 10.
[169] *Id.* arts. 11-13.
[170] *Id.* arts. 14-15. *See also* art. 22 (discussing jurisdiction).
[171] *Id.* ch. III.
[172] *See id*. arts. 16-21 and discussion *infra* Part VI.B.4
[173] *See e.g.*, Canada Dept. of Justice, Lawful Access: Consultation Document (Aug. 25, 2002), *available at* http://www.canada.justice.gc.ca/en/cons/la_al/.
[174] *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, § 201, 100 Stat. 1848, 1860, codified at 18 U.S.C. § 2701 *et seq*.

employ their systems as they wish; hence they implicate their property rights. Some of the legislation of this kind predates September 11, and addresses other forms of communications, namely telephony. The post-September 11 legislation expanded this sort of interference in the digital environment and extended it to ISPs, with the explicit and deliberate goal of combating terrorism.

84. The most detailed example of a technological capability requirement is the Communications Assistance for Law Enforcement Act of 1994 (CALEA).[175] The Act in itself does not address the Internet and does not apply to ISPs.[176] However, it represents an early example of the "comeback of the State," and raises some of the problems that now become acute.[177] CALEA mandates that telecommunications services design their technology so it can be wiretapped by the government pursuant to a lawful authorization or a court order,[178] in a manner that can enable the government to access call-identifying information,[179] and so that it allows the transmission of the intercepted information to the government.[180] The technological requirements are not to interfere with subscriber services.[181] These requirements should be enabled simultaneously, up to a pre-announced capacity. The "capacity requirement" sets the limit on how many interceptions can be performed at any minute.[182] These technological capability requirements are backed by the authority of a court to issue an order of compliance or the Attorney General's authority to bring a civil action.[183] CALEA does not require a specific design of

---

[175] Communications Assistance for Law Enforcement Act of 1994, Pub. L. 103-414, 108 Stat. 4279, codified at 47 U.S.C. §§ 1001-1010. Prior to the enactment of CALEA, telecommunications carriers were required to provide "any assistance necessary" for lawful interceptions; CALEA clarifies and spells out the required assistance. For a public choice theory perspective of the Act, *see* Lillian R. BeVier, *The Communications Assistance for Law Enforcement Act of 1994: A Surprising Sequel to the Break Up of AT&T*, 51 STAN. L. REV. 1049 (1999); Yeates, *supra* note 152, at 128-131 (summarizing the legislative background). The Act was discussed in *United States Telecom Ass'n v. FCC*, 227 F.3d 450 (D.C. Cir. 2000) (finding that portions of an FCC implementing order, regarding custom calling features and dialed digits, violated CALEA).

[176] Definitions should be taken seriously in this respect. The Act applies to "telecommunications carrier" (47 U.S.C. § 1002(a)), a term which is defined to exclude "information services" (§ 1001(8)(C)(i)), a term which is defined in § 1001(6)(A). In addition, § 1002(b)(2)(A) excludes the information services. The inapplicability to "information services" causes the FBI some headaches, such as in the case of the FCC's deregulation of broadband. The FCC's intention to deregulate broadband Internet access services would result in its reclassification as "information services," instead of "telecommunications services," with the unintended result of placing it beyond CALEA's reach. *See* Paul Davidson, *FBI Uneasy About Plan to Deregulate Fast Net*, USA TODAY, July 8, 2002, *available at* http://www.usatoday.com/life/cyber/tech/2002/07/09/wiretap-net.htm.

[177] Professor BeVier observed in 1999 that "CALEA represents a subtle but genuine paradigm shift in both privacy and technology policy." BeVier, *supra* note 175, at 1052.

[178] 47 U.S.C. § 1002(a)(1).

[179] 47 U.S.C. § 1002(a)(2); 47 U.S.C. § 1001(2).

[180] 47 U.S.C. § 1002(a)(3). *See* 47 U.S.C. §1002(a)(1) (not allowing the wiretapping itself; authority for which has to be obtained under other substantive laws); 47 U.S.C. § 1004 (obligating the telecommunications carrier to ensure the security and integrity of the communication if such a warrant is issued). *See also* 47 U.S.C. § 1002(d) (placing mandates on commercial mobile service providers); 47 U.S.C. § 1005 (placing mandates on equipment manufacturers).

[181] 47 U.S.C. § 1002(a)(4).

[182] 47 U.S.C. § 1003. *See* BeVier, *supra* note 175, at 1082-83; Yeates, *supra* note 152, at 140.

[183] 18 U.S.C. § 2522.

technology or prohibit any particular technology.[184] CALEA has not yet been fully implemented.[185] The USA PATRIOT Act explicitly excludes the application of CALEA to Internet surveillance, and therefore there is no mandate on equipment that would facilitate surveillance.[186]

85. Britain's Regulation of Investigatory Powers Act (RIPA) has a similar goal, but unlike CALEA, it does apply to the Internet and to ISPs[187] and has a different administrative mechanism to achieve its goals.[188] RIPA authorizes the Secretary of State to impose, by order, technological capabilities to make possible wiretapping.[189] The statute details the procedures to be taken before such an order is issued, including a preliminary parliamentary approval,[190] and compensation for the service providers,[191] and it is backed by (civil) sanctions for non-compliance.[192] As in the case of CALEA, the technological capability requirements in RIPA are distinct from the procedures and safeguards of conducting specific interceptions.[193]

86. CALEA and RIPA are not anti-terrorism legislation and cannot be defined as "Internet legislation" (especially not CALEA). Their interference with the market and their effect on the commercial activities of service providers is considerable, but their effect on other citizens, those to whom interception will eventually be applied, is only indirect. Unlike other legislative incidents, which will be examined shortly, CALEA and RIPA create the facility onto which other law enforcement activities take place.[194]

---

[184] 47 U.S.C. § 1002(b)(1). *But see* Yeates, *supra* note 152, at 143-145 (applying the Act imposes costs on the telecommunications carriers); 47 U.S.C. § 1008 (stating which carriers are compensated).
[185] *See* U.S. Dept. of Justice, Office of the Inspector General, Implementation of the Communications Assistance for Law Enforcement Act by the Federal Bureau of Investigation, Report No. 02-14 (Mar. 2002), *available at* http://www.usdoj.gov/oig/audit/FBI/0214/index.htm; BeVier, *supra* note 175, at 1114-16 (assessing CALEA in 1999); Yeates, *supra* note 152, at 145 (assessing CALEA in 2002). *But see* Michael P. Clifford, Communications Assistance for Law Enforcement Act (CALEA) 36 PROSECUTOR 22, 25 (Mar.-Apr. 2002) (noting that CALEA is "one of the most valuable tools in law enforcement's crime fighting arsenal" by the FBI's supervisor of the CALEA Implementation Section).
[186] USA PATRIOT Act, Pub. L. No. 107-56, § 222, 115 Stat. 272, 292 (2001).
[187] Regulation of Investigatory Powers Act § 12 (applying the technological capability requirement to "public telecommunications services"). *Id.* § 2 (defining the term "telecommunication service" in reference to "telecommunications system" which includes "communications by any means involving the use of electrical or electromagnetic energy").
[188] *See* Yeates, *supra* note 152 (comparing in detail CALEA and RIPA).
[189] Regulation of Investigatory Powers Act § 12. *See* The Regulation of Investigatory Powers (Maintenance of Interception Capability) Order, (2002) SI 2002/1931, *available at* http://www.hmso.gov.uk/si/si2002/20021931.htm (imposing such an order in July 2002 and coming into force in August 2002).
[190] *See* Regulation of Investigatory Powers Act § 12(10); *id.* § 12(9) (requiring that the Secretary also consult a Technical Advisory Board); *id.* § 13 (establishing a Technical Advisory Board).
[191] *Id.* § 14 (imposing costs of the statute on private entities). *See* Akdeniz et al., *supra* note 144, at 78 (discussing the legislature's attention to costs similar to the debate in the United States).
[192] Regulation of Investigatory Powers Act § 12(7).
[193] *Id*. §§ 13-25.
[194] The case of CALEA and RIPA is somewhat different from other cases discussed below. In these cases the State targeted privately held nodes of power, which are the result of the architecture of the telecommunications system. The State uses the technological advantage of the carriers: they are technological bottlenecks, through whose systems the communication is carried. Yet, it is interesting to examine the contribution of the State to the development of such an infrastructure.

87. Another example of an attempt to affect technologies in a way that would serve government security needs is the regulation of encryption. Strong encryption could certainly be an obstacle to public authorities' efforts to track online hostile activities. Even if security agencies are legally authorized to track the traffic information and the content of messages, they cannot make use of encrypted information unless they are able to decipher the encrypted transmissions. Therefore, for many years enforcement agencies sought to regulate the use of strong encryption. Several legal initiatives attempted to require that a back door be built into encryption software to enable law enforcement authorities to decrypt messages when necessary.[195] These attempts failed due to the pressure of civil liberties groups and the computer industry lobby. These groups argued that liberalization of the encryption market was required to support electronic commerce, to protect global information infrastructures, to protect privacy, intellectual property rights, and important information, and to allow American companies to compete equally with their overseas counterparts. In fact, in recent years there has been a trend to reduce restrictions and prior control on the domestic use and export of encryption. Within the United States there are currently no restrictions on production or commerce in the means of encryption of any strength. There is regulation that governs the export of encryption items outside the United States, and it is implemented by the Bureau of Export Administration (BXA).[196] The only blanket prohibition remaining in force is that which relates to the export of the means of encryption to states that support terrorism, or their citizens.[197] The legal situation is different in other countries.[198]

2. Data Retention

88. A clear example of the *Invisible Handshake* is the requirement that ISPs retain users' communication and/or data about that communication. The data

---

[195] In 1993 the U.S. Administration proposed the idea of the Clipper Chip, which would be a means of encryption licensed by the Administration, with the Administration retaining the means to decipher the Clipper Chip. In this way, the Administration would retain the ability to access any content encrypted by means of this chip. The idea was not successful. Opposition came from software companies, which were restricted in terms of software exports and competitively disadvantaged in world markets, and from human rights organizations and privacy advocates. *See* STEVEN LEVY, CRYPTO: HOW THE CODE REBELS BEAT THE GOVERNMENT — SAVING PRIVACY IN THE DIGITAL AGE 226-268 (2002).

[196] *See* Export Administration Regulations, 15 C.F.R. §§ 740.13, 740.17 (2003), *available at* http://w3.access.gpo.gov/bis/ear/pdf/740.pdf; *see also* Export Administration Regulations, 15 C.F.R. 742.15 (2003), *available at* http://w3.access.gpo.gov/bis/ear/pdf/742.pdf. Authority for the control of encryption was transferred in 1996 to the Bureau of Export Control (BXA), in the Department of Commerce. Encryption items were reclassified: they were transferred from the Munitions Control list to the Commerce Control list. The new regulations created a process by which the owner of means of encryption with a key length of up to 40 bits could have the product removed from the Commerce Control list after a single examination by the BXA, and then would be exempt, in practice, from any export restrictions. 61 Fed. Reg. 68,572 (Dec. 30, 1996), *available at* http://w3.access.gpo.gov/bis/fedreg/ear_fedreg96.html#encryption1.

[197] *See* Congressional Research Service, Terrorism, the Future, and U.S. Foreign Policy (Apr. 11, 2003), *available at* http://www.fas.org/irp/crs/IB95112.pdf. The U.S. government lists the states supporting terror as: Syria, Iran, Iraq, Libya, Sudan, North Korea, and Cub). *Id.; see also* U.S. State Dept., Patterns of Global Terrorism: 1999, *available at* http://www.state.gov/www/global/terrorism/1999report/sponsor.html.

[198] Regulation of Investigatory Powers Act §§ 49-56 (providing authority to require disclosure of key to protected information, *i.e.,* a decryption tool).

retention requirements are far more intrusive than the technological capability requirements, as they impose a costly burden on the ISPs, they have a direct effect on the privacy of users, and they turn the ISPs, in practice, into a long arm of law enforcement authorities.

89. One kind of data retention requirement refers only to the *traffic data*. This is the case of RIPA in the United Kingdom,[199] which refers to "communications data," a term which covers *traffic data*, but explicitly excludes the contents of the communication.[200] *Traffic data* refers to the identity of the sender and the addressee of the communications, to the means of communications, and to communication that is logically associated with it.[201] In other words, *traffic data* might include information such as who sent an e-mail to whom, from which IP address and which geographical location, via which ISP, when the e-mail was sent, what was the duration of the communication, whether there was an attachment, and of what format, and the like information.[202]

90. RIPA authorizes enumerated public authorities to require a telecommunications operator (including ISPs) to obtain communications data and disclose it.[203] It has several built-in checks and balances over the execution of the authority, though these appear to leave ample leeway to the executive. Firstly, the order to the operator should be issued only if the person designated with the authority "believes that it is necessary."[204] The latter term is then spelled out to include interests of national security, prevention and detection of crime and disorder, the economic well-being of the United Kingdom, public safety, public health, and prevention of death.[205] But this list also allows the Secretary of State to specify further purposes, with the approval of Parliament.[206] Secondly, the notice to the operator should be "proportionate to what is sought to be achieved."[207] Thirdly, there are several procedural safeguards,[208] and fourthly, the retention order is limited to a one-month period, though it is renewable.[209] Lastly, the authority is limited to enumerated agencies, such as the police and the National Criminal Intelligence Service, but the Secretary may add more bodies, with the approval of Parliament.[210] This authority is backed by civil proceedings, including the issuance of an injunction.[211] It also offers reimbursement of costs.[212] This scheme allows, by default, the option of ex-post judicial review, but does not

---

[199] *See* Regulation of Investigatory Powers Act, ch. II ("Acquisition and Disclosure of Communications Data").
[200] *See* Regulation of Investigatory Powers Act § 21(4)(b).
[201] *See id.* § 21(6) (defining "traffic data" complexly).
[202] *See also* Convention on Cybercrime, *supra* note 160, art. 1(d) (defining "traffic data").
[203] Regulation of Investigatory Powers Act § 22(4).
[204] *Id.* § 22(1).
[205] *Id.* § 22(2).
[206] *Id.* §§ 22(2)(h), 22(9).
[207] *Id.* § 22(5). *See also id.* § 23(8) (requiring the authority to cancel a notice once the order is no longer proportionate).
[208] *See id.* § 23(2) (requiring the notice to the operator be in writing).
[209] *Id.* §§ 23(4), 23(5).
[210] *Id.* §§ 25(1), 25(5).
[211] *Id*. § 22(8).
[212] *Id*. § 24.

provide for ex-ante judicial review of the order to retain the data.[213]

91. RIPA has been criticized on several grounds: for its lax standards and procedures, for the wide range of public agencies allowed to issue the retention orders, and for the absence of prior judicial review.[214] The fear is of a slippery slope. Indeed, in June 2002, Home Secretary David Blunkett intended to issue an order that would have extended the surveillance powers to additional bodies, including local councils. After a critical public response, the Secretary withdrew the proposed order.[215]

92. Another source of difficulty might be the compatibility of RIPA's data retention requirements with European law.[216] Other than the general protection of privacy in the ECHR, which allows limiting it under certain conditions,[217] European law takes a strong position against data retention in the private, commercial context. A 2002 Directive restricts the processing of traffic data by service providers:[218] once the data is no longer required for the transmission of the communication or for the purpose of billing, it should be erased or made anonymous,[219] unless the user has consented to the use of the data.[220] The adaptation of the Directive followed a political debate between the European Parliament and the Council of Ministers regarding the data retention sections. The former opposed it, but after September 11 the latter succeeded.[221] The final version of the Directive explicitly allows data retention when "necessary, appropriate and proportionate … within a democratic society to safeguard national security …,"[222] and hence RIPA and similar European measures do not facially conflict with the new Directive. Nevertheless, the Directive does set limits of a constitutional magnitude.

---

[213] There is some administrative review under RIPA §§ 57(2)(b) and 62, by the Interception of Communications Commissioner and the Chief Surveillance Commissioner, respectively.

[214] The Information Commissioner warned that RIPA and the Anti-Terrorism, Crime and Security Act 2001 could violate human rights, as in the case where an order would be issued on the basis of national security, but applied to gain access for other purposes. *See* Matthew Broersma, *RIPA Surveillance May Break Human Rights Laws*, ZDNET UK NEWS, July 31, 2002, *at* http://news.zdnet.co.uk/story/0,,t295-s2120139,00.html. *See also* Akdeniz et al., *supra* note 144, at 81, and the criticism of the Data Protection Commissioner quoted there.

[215] *See Blunkett: We Blundered over Data Access Plan*, THE GUARDIAN, June 18, 2002, *available at* http://www.guardian.co.uk/Archive/Article/0,4273,4435947,00.html.

[216] European law is an over-inclusive term, but will suffice for the current purpose. In fact, there are three layers of law: that of the European Union, binding its member states, that of the Council of Europe, such as the ECHR, and each state's legal system.

[217] *See* European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), *as amended* Nov. 1, 1998, Council of Europe, art. 8(2), which allows a public authority to interfere with the exercise of the right if "in accordance with the law and is necessary in a democratic society in the interests of national security…." The requirements in RIPA seem to have been tailored to fit this section.

[218] Directive 2002/58/EC of the European Parliament and of the Council Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, 2002 O.J. (L 201) 37 [hereinafter Directive on Privacy and Electronic Communications].

[219] *See id.* art. 6; *see id.* art. 2 (defining "traffic data").

[220] *See id.* art. 6(3). The consent should be informed (*see* art. 6(4)), and users should be given the opportunity to withdraw their consent (*see* art. 6(3)).

[221] For an account of this debate, see ELECTRONIC PRIVACY INFORMATION CENTER, PRIVACY AND HUMAN RIGHTS 2002: AN INTERNATIONAL SURVEY OF PRIVACY LAWS AND DEVELOPMENTS 11-12, 43-44 (2002), *at* http://www.privacyinternational.org/survey/phr2002/phr2002-part1.pdf.

[222] *See* Directive on Privacy and Electronic Communications, *supra* note 218, art. 15(1).

93. Following September 11, RIPA was supplemented with the Anti-Terrorism, Crime and Security Act of 2001. The explanatory notes that accompany the Act declare that it does not purport to "affect the access framework and safeguards set out in RIPA," but to "clarify[] the lawful basis for the retention of data by communications service providers."[223] The Act creates a new legal basis for data retention by ISPs — a code of practice that is to be drawn up in consultation with the industry and approved by Parliament.[224] The code of practice is meant to provide more detailed instructions as to when the data should be retained.[225] The code is voluntary and there is no penalty for non-compliance.[226] The Act also allows for other, specific, agreements between the Secretary of State and the ISPs. Alongside the voluntary code, the Secretary is authorized to issue compulsory directions and order either all ISPs or a particular ISP to retain communications data.[227] The latter power lapses two years after the enactment of the Act, but it might be extended.[228] Despite the Explanatory Notes' declaration that the Act clarifies RIPA, it has been observed by the Information Commissioner that the post-September 11 legislation has potentially far-reaching consequences. These initiatives have led to a noticeable shift in the balance between respect for an individual's private life and the needs of society to protect itself against criminal actions. The Information Commissioner has noted that, "although this shift has occurred in the name of counter-terrorism, the measures deployed often go much further into addressing areas of more general criminality."[229]

94. To date, and to the extent reported, the Act has not yet reached litigation. However, it is now clear that the financial burden is enormous.[230] Other countries have already adopted data retention rules[231] or are in the process of consideration or adoption of similar rules.[232] The United States does not have similar rules, though one might argue that retention orders could be issued as part of interception orders, which are far more burdensome from the ISPs'

---

[223] *See* ATCSA Explanatory Notes, *supra* note 158, at para. 30.
[224] *See* ATCSA § 102(1) and procedures at § 103. Failure to comply with the code does not in itself subject provider to civil liability or criminal sanction. ATCSA § 102(4).
[225] *See* ATCSA Explanatory Notes, *supra* note 158, at para. 258.
[226] *See* ATCSA § 102(4), and ATCSA Explanatory Notes, *supra* note 158, at para. 263. Some ISPs in the United Kingdom refused to sign such codes, stating concerns that the code violates EU law. *See Internet Intelligence Plans Hit Hurdle*, BBC NEWS, Oct. 22, 2002, *at* http://news.bbc.co.uk/1/hi/uk_politics/2350059.stm.
[227] *See* ATCSA § 104(2).
[228] *See* ATCSA § 105.
[229] INFORMATION COMMISSIONER, ANNUAL REPORT AND ACCOUNTS 17 (June 2002), *at* http://www.dataprotection.gov.uk/dpr/dpdoc.nsf/ed1e7ff5aa6def30802566360045bf4d/1c8db1dc3355f62b80256bf1004eabc2/$FILE/AR2002.pdf.
[230] AOL estimated that the cost of adopting its systems and running them are around £60 million. *See* Matt Loney, *ISPs Spell Out True Cost of Data Retention*, ZDNET UK NEWS, Dec. 12, 2002, *at* http://news.zdnet.co.uk/business/legal/0,39020651,2127408,00.htm.
[231] *E.g.,* Belgium, France, Spain. *See* PRIVACY AND HUMAN RIGHTS 2002, *supra* note 221, at 44. For example, Spain's Law on Services for the Information Society, passed on June 27, 2002, requires ISPs to keep a one-year record of IP addresses. *See* Jerome Socolovsky, *Foes Vow to Challenge New Spanish Law Regulating Internet Commerce,* THE ASSOCIATED PRESS, June 28, 2002, *available at* http://www.govtech.net/news/news.phtml?docid=2002.06.28-3030000000015251.
[232] *See*, *e.g.,* Canada Dept. of Justice, Lawful Access: Consultation Document, *supra* note 173.

point of view and more intrusive from the users' viewpoint.[233] But this absence of an explicit authority to order ISPs to retain data should not mislead us: it is not an indication of stronger protection for privacy. To the contrary, data retention orders are absent from the American legal scene because there is no need to compel ISPs to retain information: they do so for their own commercial purposes. Privacy laws in the United States are aimed mostly at the government, but leave the private sphere relatively unregulated, with only few, sector-based legislation. Unlike European law, there is no general prohibition to the collection of data by private entities in the United States. This is indeed a thriving business. Hence, the government does not need to order data retention. If interested in the data, it can turn to other law enforcement instruments: data preservation orders and production orders, to which we now turn.

3. Data Preservation and Production Orders

95. The Council of Europe's Convention on Cybercrime includes another law-enforcement toll: data preservation requirements. The Convention separates the "expedited preservation of stored data" from the "production" of computer data (and of subscriber information) and from the seizure of data or the real-time collection thereof or interception of content.[234]

96. The data preservation orders are presented by the drafters of the Convention as "an entirely new legal power … [and] an important new investigative tool."[235] The official rationale is to maintain the integrity of data, a crucial factor for investigation as well as for evidentiary reasons, and to do so expeditiously and in a less intrusive manner than the alternative of governmental access and seizure.[236] Accordingly, the Convention requires that member states adopt legislation that authorizes the order of "the expeditious preservation" of specified computer data.[237] The ISP is then obliged to maintain the integrity of the data for a limited time, no more than 90 days, and to keep the procedures confidential.[238] This is where preservation differs from retention, in the words of the Convention's Explanatory Report:

> To preserve data means to keep data, which already exists in a stored form, protected from anything that would cause its current quality or condition to change or deteriorate. To retain data means to keep data, which is currently being generated, in one's possession into the future. … Data retention is the process of storing data. Data preservation, on the other hand, is the activity that keeps that stored data secure and safe.[239]

---

[233] One news report announced that the idea is being considered by the White House. *See* Kevin Poulsen, *U.S. Cyber Security May Draft ISPs in Spy Game*, THE REGISTER, June 19, 2002, *available at* http://www.theregister.co.uk/content/55/25781.html. We did not find confirmation on any official site.
[234] *See* Convention on Cybercrime, *supra* note 160, arts. 16-21.
[235] *See* EXPLANATORY REPORT, *supra* note 160, ¶ 155.
[236] *See id.*
[237] *See* Convention on Cybercrime, *supra* note 160, art. 16(1); *id.* art. 1 (definition of "computer data" and "traffic data").
[238] *See id.* arts. 16(2) and 16(3), respectively.
[239] *See* EXPLANATORY REPORT, *supra* note 160, ¶ 151.

97. In other words, *preservation* refers to data that has already been retained. To be more accurate in the legal sense, it refers to data that was retained by the ISP for its own reasons, such as processing the service or billing.

98. Preservation orders are not new in the United States. The Electronic Communications Privacy Act of 1986 (ECPA) authorizes providers of electronic communication services to "preserve records and other evidence in its possession pending the issuance of a court order or other process."[240] The preservation period is for 90 days, with an option to extend it.[241] The intent is clear: to prevent the loss of valuable evidence until a warrant is issued. Accordingly, a warrant need not be issued *before* the ISP is requested to preserve the data,[242] though it seems that at some point such a warrant should be issued.[243] Finally, the USA PATRIOT Act immunizes ISPs against civil action for damages caused by violations of the ECPA. Under prior law, a defense to such a cause of action was limited to good faith reliance on a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization. Section 815 of the USA PATRIOT Act explicitly provides that good faith reliance on a government request to preserve evidence under ECPA § 2703(f) will be a defense in civil action.[244]

99. In the United Kingdom, preservation orders of electronic transmissions such as e-mails are regulated within a general law enforcement act.[245]

100. We return our attention to the Convention. The *production order* provides another "flexible measure" for law enforcement agencies to obtain data.[246] Once again, as in regard to the preservation orders, the production order refers to data that is already in the possession of the operator — in our context the ISP. Interestingly, the official rationale for the production order is that it offers an alternative investigative power, "instead of requiring States to apply systematically coercive measures in relation to third parties, such as search and seizure of data …."[247] While this is indeed true from the ISPs' point of view, it has legal implications for users' rights in regard to their ability to raise constitutional arguments. This issue will be dealt with in the next part of this

---

[240] 18 U.S.C. § 2703(f)(1). For an example of a request letter for preservation of data, *see* Department of Justice, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, Appendix C (July 2002), *available at* http://www.cybercrime.gov/s&smanual2002.htm.

[241] 18 U.S.C. § 2703(f)(2).

[242] *See* United States v. Bach, 2001 WL 1690055 at *1, 2001 U.S. Dist. LEXIS 21853 at *3 (D. Minn. Dec. 14, 2001) ("An officer need not issue a warrant before requesting that a service provider retain evidence."). The district court, however, found the unsupervised seizure of e-mails by the ISP, without a law enforcement officer present, violated defendant's Fourth Amendment privacy. The Court of Appeals reversed this latter legal decision, ruling that the execution of a warrant without the presence of an official investigator does not violate privacy. *See* United States v. Bach, 310 F.3d 1063 (8th Cir. 2002).

[243] Although a warrant is not needed to request the preservation of data, if a government agency requires disclosure of the data by an ISP, that agency must secure a warrant. 18 U.S.C. § 2703(a).

[244] *See* 18 U.S.C. § 2707(e) (2002).

[245] *See* Police and Criminal Evidence Act (PACE), 1984, c. 60 (Eng.), especially sections 9, 14 and Schedule I to the Act. It has been ruled that a preservation order of e-mails, whose observance required the ISP to redirect the e-mails, did not violate RIPA's prohibition of unlawful interception. *See* NTL Group Ltd. v. Ipswich Crown Court, 2003 Q.B. 131 (2002).

[246] *See* EXPLANATORY REPORT, *supra* note 160, ¶ 171.

[247] *Id.* at § 170.

article.

101. Another noteworthy point is the following, offered in the explanatory report:

> The implementation of such a procedural mechanism will also be beneficial to third party custodians of data, such as ISPs, who are often prepared to assist law enforcement authorities on a voluntary basis by providing data under their control, but who prefer an appropriate legal basis for such assistance, relieving them of any contractual or non-contractual liability.[248]

Once again, we observe the convergence of interests of the State and of the ISPs, at the price of neglecting users' rights.[249]

4. Obligations and Immunities of OSPs

102. The ISPs and other Online Service Providers, such as providers of hosting services or webmail services, become crucial junctions of control in the digital environment. Users log on to their servers, communication passes through their system, and content (such as programs, text, e-mail) is stored on their facilities. Because ISPs bill users per use, they can (and do) match the IP number assigned to each user per each surfing session (whether dynamic or static) to the specific user. Thus, information collected and processed as part of the routine operation of ISPs is invaluable for law enforcement agencies. Such information could be used to match virtual online identities and real persons, to trace suspects, to identify and establish conspiratorial associations among users, or to accomplish any other intelligence tasks.

103. Several provisions in the USA PATRIOT Act that were further amended by the Cyber Security Enhancement Act of 2002 (CSEA)[250] authorize the disclosure of information to law enforcement authorities. The post-September 11 legislation amends the ECPA, which sets limits on disclosure of content and non-content records by public providers, *i.e.,* any provider that provides "service to the public."[251] The ECPA provides several exceptions that permit disclosure under strictly defined circumstances.[252]

104. The new legislation (as amended first by the USA PATRIOT Act and later by

---

[248] *Id*. at § 171.
[249] On the convergence of interests, *see supra* text accompanying notes 120-126.
[250] *See* Homeland Security Act of 2002 § 225, entitled Cyber Security Enhancement Act.
[251] 18 U.S.C. § 2702(a).
[252] 18 U.S.C. § 2702(b). These exceptions permit disclosure of the contents of a communication: "1) to an addressee or intended recipient of such communication or [their] agent …; 2) as otherwise authorized in §§ 2517, 2511(2)(a) or 2703 …; 3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computer service; 4) to a person employed or authorized or whose facilities are used to forward such communication to its destination; 5) as may be necessarily incident to the rendition of the service or the protection of the rights or property of the provider of that service; … or 7) to law enforcement agency if the contents: A) were inadvertently obtained by the provider and appear to pertain to the commission of a crime."

the CSEA) permits the voluntary disclosures of content[253] and information on customer records[254] to a law enforcement agency "if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency."[255] Under this exception a provider may disclose the content of e-mail stored on its system if it believes emergency conditions have occurred. Non-content information that could be disclosed voluntarily under this section without a court order may include: name, address, billing records, telephone number, records of session times and duration, temporarily assigned network addresses, type of service provided, and means and sources of payment. The authority to make voluntary disclosure does not mandate a duty to review subscribers' communication in search of such information. The new legislation further stipulates that providers are authorized to disclose non-content records to protect their rights and their property.[256] When ISPs make such authorized disclosure they are immune against civil action based on the ECPA.[257]

105. The law further allows providers to authorize monitoring of computer communications on their system, when such interception is perceived relevant to computer trespasser investigation.[258] While under prior law such real-time interception of electronic communications required a court order,[259] the new legislation allows any government employee to conduct surveillance at the invitation of the ISP (the "computer owner or operation"). Under this rule, monitoring without a court order will be legal if the following four conditions are satisfied: 1) the ISP authorized the interception of the trespasser's communications, 2) the intercepting person is lawfully engaged in an ongoing investigation, 3) the person acting under color of law has "reasonable grounds to believe that the contents of the computer trespasser's communications will be relevant to the investigation," and 4) investigators intercept only the

---

[253] 18 U.S.C. § 2702(b).
[254] 18 U.S.C. § 2702(c).
[255] 18 U.S.C. § 2702(b)(8). Before the 2002 amendment, § 2702(b)(6)(C) allowed voluntary disclosure "if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person requires disclosure of the information without delays." *See* § 212 of the USA PATRIOT Act, amending § 2702(b)(6)(C) (permitting voluntary disclosure in case of an emergency in regard to content), and § 2702(c)(4) (same, in regard to non-content information). The CSEA replaced the condition of reasonableness with that of good faith, and omitted the condition that the emergency be immediate. Another change is that the information can be divulged not only to a law enforcement agency, but to "Federal, state or local governmental entities." § 2702(b)(8).
[256] *See* § 212 of the USA PATRIOT Act, adding § 2702(c)(3) to the ECPA, which authorizes an ISP to disclose a record or other information pertaining to a subscriber as may be necessary to protect the rights or property of the provider.
[257] 18 U.S.C. § 2703(e), as amended by the CSEA, § 225(h)(1) ("No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena, statutory authorization or certification under this chapter.").
[258] A "computer trespasser" is broadly defined by § 217 of the USA PATRIOT Act, which amends 18 U.S.C. § 2510(21), to include any person who accesses a protected computer without authorization.
[259] Such a court order could be either a wiretap order under 18 U.S.C. § 2516(1) issued by a court upon application supported by affidavit showing probable cause that the target committed one of a list of serious crimes, or a Foreign Intelligence Surveillance Act (FISA) order issued under 50 U.S.C. § 1805 by a secret FISA court upon application by the Attorney General.

communications sent or received by trespassers.[260]

106. This legal framework, which allows an ISP to authorize interception by government officials simply by an invitation to investigate, could be dangerous. Arguably, an ISP, like any other computer owner, should be capable of protecting its property against trespass and invite law enforcement agents to assist it. Such a right would accord ISPs a powerful status equating their rights to those of real-estate owners who defend their property against burglars.[261] Yet ISPs run a facility that serves many communities of users. Some are subscribers of the ISP while others may have no contractual relationship with it. Inviting law enforcement agents without a warrant may compromise the civil liberties of a large body of users. Furthermore, allowing ISPs to authorize interception on their systems opens up a "back door" for government interception beyond the reach of judicial review.

107. In fact, this type of regulation demonstrates the potential risk in authorizing ISPs to disclose users' information and employing ISPs in monitoring tasks. This regulation creates a convergence of ISPs' property and commercial interests and government national security tasks. Notwithstanding their potential value as powerful information junctions, ISPs have their own legitimate commercial interests. Subscribers' information is a valuable commercial asset and providers could benefit from data mining and data retention. The broad authority to intercept communications and disclose information when necessary to protect their property rights entrusts the protection of precious values such as privacy to the hands of self-interested parties. One must keep in mind the fact that ISPs' special function as facilitators of decentralized online communication renders them an important potential *shield* for users' activities.

108. This mixture of conflicting interests of ISPs, users, and the public at large has already been the center of one policy debate regarding the scope of ISPs' immunities and responsibilities.[262] An attempt to use ISPs as enforcement agents was made in the campaign against the distribution of injurious content online. The declared purpose of the broad exemption of ISPs under Section 230 of the Communications Decency Act (CDA) was to provide incentives to ISPs to restrict access to objectionable materials.[263] The law defines ISPs' immunity in § 230(c), titled "Protection for 'Good Samaritan' blocking and screening of offensive material." Under this section, interactive service providers are exempted from liability towards third parties who were injured by content posted on the ISP system by its subscribers. They are also exempted from civil liability for any action voluntarily taken in good faith to restrict access to or availability of materials the provider considers objectionable, or any action taken to enable or make available the technical

---

[260] 18 U.S.C. § 2511(2)(i).

[261] For a discussion of such conflicting rights, see Orin S. Kerr, *Are We Overprotecting Code? Thoughts on First-Generation Internet Law*, 57 WASH. & LEE L. REV. 1287 (2000).

[262] *See, e.g.*, 47 U.S.C. § 230; Zeran v. America Online, Inc. 129 F.3d 327 (4th Cir. 1997). Compare to the far more limited immunity in the context of copyright law at 17 U.S.C. § 512. For analysis of the interplay of the incentives in these situations, see Elkin-Koren, *supra* note 62.

[263] *See* Benkler, *supra* note 46, at 1209 ("[Congress] began to regulate Internet service providers … by exempting them from liability on the condition that the ISPs would help enforce federal regulations.")

means to restrict access to objectionable materials.

109. Yet the exemption of liability, as broadly interpreted by the courts, reflects another rationale. Several courts have held that the reason for not imposing liability on the ISPs was First Amendment considerations.[264] The fear was that liability would create a chilling effect. In the absence of immunity, ISPs, wishing to avoid liability, would have adopted a simple guideline: if there is doubt, there is no doubt. In any situation in which they might be (indirectly) liable for various (direct) violations of users — they would have interfered in the service, chat room, forum, or taken down the "suspect" link, Web sites, and the like. Indeed, the negative effect of liability on users' freedoms is immediate. To avoid these effects and to ensure a robust and free expressive environment, legislatures chose to provide ISPs with immunity.[265]

110. The immunity accorded to the ISPs serves users' freedom. This sort of consideration is, for the time being, absent from the logic of the data retention, preservation, and production orders. The duties imposed on the ISPs limit users' privacy and create a chilling effect on speech.

5. Libraries and Bookstores

111. Production orders are not limited to the digital environment, and the same trend of using private nodes as information centers is also reflected in the context of libraries. One of the amendments brought about by the USA PATRIOT Act is an extension of "production orders" aimed at what was previously referred to in the statute as a "physical storage facility,"[266] a term that includes libraries and bookstores. The amendment omits the enumerated lists of businesses subject to the production orders,[267] and now permits the FBI to apply to the "spy" court[268] for an order requiring the production of any tangibles, including books, records and the like, if it is relevant to an investigation against international terrorism. The relevancy requirement (not explicit in the statute) is a far cry from the much stricter standard of probable cause, which is the constitutional Fourth Amendment standard.[269] The Act distinguishes between American citizens and foreigners: if the investigation against an American citizen is based solely upon First Amendment activities

---

[264] *See* Zeran, 129 F.3d at 333.

[265] Congress noted in the CDA: "The Internet and other interactive computer services have flourished, to the benefit of all Americans, *with a minimum of government regulation*," § 230(a)(4) (emphasis added), and that "[i]t is the policy of the United States … (2) to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, *unfettered by State or Federal regulation*," § 230(b)(2) (emphasis added).

[266] *See* 50 U.S.C. §§ 1861-1862 (1999).

[267] *See* USA PATRIOT Act, § 215, amending 50 U.S.C. §§ 1861-1862.

[268] The Foreign Intelligence Surveillance Act of 1978 established a special court to grant orders approving electronic surveillance. *See* 50 U.S.C. § 1803.

[269] For criticism on First and Fourth Amendments grounds, see Electronic Privacy Information Center, The Attorney General's Guidelines, *available at* http://www.epic.org/privacy/fbi/ (last updated Mar. 17, 2003). In one drug investigation case, the Supreme Court of Colorado found that under Colorado's Constitution, law enforcement officials need to make a heightened showing of their need of a bookstore's customer purchase records. *See* Tattered Cover, Inc. v. City of Thornton, 44 P.3d 1044 (Colo. 2002).

the production order is unavailable.[270] The Act is supplemented by the Attorney General's guidelines to the FBI.[271]

112. These amendments have attracted criticism by privacy organizations as well as bookstores and libraries.[272] The American Library Association has even published guidelines for librarians.[273] Several municipalities have passed resolutions barring employees — including librarians — from collaborating with Federal officials.[274] No official statistics are available on the use of the production order, and there is a statutory prohibition against disclosure of a production order,[275] but unofficial surveys indicate a dramatic increase in the FBI's use of this extended power.[276]

113. Though these production orders aimed at libraries and bookstores (or any other private database) are not limited to the digital environment, they clearly fit into the general features of the *Invisible Handshake*. The State utilizes information that is lawfully gathered and held by private entities. Had the State initiated a direct attempt at gathering such information, the Fourth and First Amendment implications would have been clear. But here the State attempts a sophisticated way to sidestep the constitutional hurdles.

V. A New Landscape? Possible Ramifications

114. What does all this mean? The *Invisible Handshake* marks a new phase in the digital environment. We wish to emphasize that the new role does not replace the previous role of the State as a regulator; rather they function alongside one another. But we observed a new phase of the State's complex relationship with

---

[270] 50 U.S.C. § 1861(a)(1).

[271] U.S. DEPT. OF JUSTICE, THE ATTORNEY GENERAL'S GUIDELINES ON GENERAL CRIMES, RACKETEERING ENTERPRISE AND TERRORISM ENTERPRISE INVESTIGATIONS (May 30, 2002), *available at* http://www.usdoj.gov/olp/generalcrimes2.pdf.

[272] *See* EPIC, *supra* note 269; Press Release, American Booksellers Foundation for Free Expression (ABFFE), ABFFE Protests Free Speech Threats Posed by War on Terrorism (Apr. 25, 2002) (on file with authors); American Library Association (ALA), *FBI In Your Library, at* http://www.ala.org/alaorg/oif/fbiinyourlibrary.html. *But cf*. Robert A. Pikowsky, *An Overview of the Law of Electronic Surveillance Post September 11*, 94 LAW LIBR. J. 601, 620 (2002) (arguing that the USA PATRIOT Act did not have an unreasonable impact on privacy of library patrons: "it merely awakened the library community to the issues of electronic surveillance that had already existed.")

[273] *See* ALA, GUIDELINES FOR LIBRARIANS ON THE USA PATRIOT ACT (Jan. 19, 2002), *available at* http://www.ala.org/Content/NavigationMenu/Our_Association/Offices/ALA_Washington/Issues2/Civil_Liberties,_Intellectual_Freedom,_Privacy/The_USA_Patriot_Act_and_Libraries/patstep.pdf.

[274] *See* Julia Scheeres, *Cities Say No to Federal Snooping*, WIRED NEWS, Dec. 19, 2002, *available at* http://www.wired.com/news/politics/0,1283,56922,00.html.

[275] 50 U.S.C. § 1862(d).

[276] A survey of 1020 public libraries, conducted by the University of Illinois in January and February 2002, found that 85 had been approached by the FBI. *See* Marlene Naanes, *Patriot Act Touches Nerve at BR Libraries*, BATON ROUGE ADVOC., June 27, 2002, at 1B, *available at* http://staging.theadvocate.com/stories/062702/new_act001.shtml; *see also* Leigh S. Estabrook, *The Response of Public Libraries to the Events of September 11, 2001*, 84 ILL. LIBR. 1 (2002), *at* http://www.cyberdriveillinois.com/publications/pdf_publications/illibrary_v84_n1.pdf. A subsequent survey of 1503 public libraries, which serve a population of over 5000 patrons, found that 4.1% of all libraries surveyed were approached by authorities requesting information about patrons pursuant to the events of September 11. *See* LIBRARY RESEARCH CENTER, PUBLIC LIBRARIES' RESPONSE TO THE EVENTS OF SEPTEMBER 11TH, at 6 (2002), *available at* http://alexia.lis.uiuc.edu/gslis/research/national.pdf.

the digital informational environment, and we are probably only at the beginning of this new phase.

115. The State, now re-entering the digital field, is different from what it was in the 1970s and 1980s, and the field itself has changed dramatically.[277] The *Comeback of the State* is not a replay of its first role as an owner of the IT infrastructure. It is a new game. Accordingly, it would be a mistake to evaluate the current role by applying the familiar tools with which we assessed the previous roles. In this concluding part of the article we explain why it is important to observe the *Invisible Handshake* and point to possible ramifications thereof.

116. *Firstly*, we examine the *Invisible Handshake* through constitutional lenses. At first sight, the new situation might appear to be a familiar constitutional issue: the public (or governmental) interest conflicts with individual interests and rights. However, we argue that the ready-made constitutional law toolkit does not fully address the new issues. We address the complexity of the current situation and point to some questions that should be addressed in the future.

117. *Secondly*, we conceptualize the *Invisible Handshake* within recent Information Law discourse: this is the discussion of the benefits of decentralization and the potential danger posed by concentrated control in the digital environment.

118. *Thirdly*, we point to the implications on the design of the digital environment. Here the underlying assumption is that the technology is not void of values: it both reflects and constitutes values; hence the realization of the *Invisible Handshake* is likely also to affect the technological infrastructure.

A. The Limits of Current Constitutional Law

119. Constitutional law is structured around the image of the State as one of limited powers.[278] The image of the State as an inevitable social institution and the main threat to human rights lies at the heart of American political thought. In the words of Thomas Paine:

> Society is produced by our wants, and government by our wickedness; the former promotes our happiness *positively* by uniting our affections, the latter *negatively* by restraining our vices. The one encourages intercourse, the other creates distinctions. The first is a patron, the last a punisher. Society in every state is a blessing, but government even in its best state is but a necessary evil.[279]

120. Accordingly, it is constitutional law that addresses the relationship between

---

[277] Once again, unless otherwise noted, we use the term "State" to denote all branches of government, in the broadest political sense, and not in the American federalist context of the federal government vis-à-vis the several states.

[278] Not only of the federal government vis-à-vis the several states, but also vis-à-vis citizens.

[279] THOMAS PAINE, COMMON SENSE 65 (Penguin Classics ed., Penguin Books 1986) (1776).

the State and the individual, keeping this image of the State as a necessary evil in mind. The paradigmatic juxtaposition is that of State vs. the Citizen. Call this the *Governmental Paradigm*. Many constitutional doctrines have been developed with this paradigm in view. Jurists are well trained in recognizing it and in applying the ready-made constitutional rules and doctrines. This leaves relationships between individuals to private law, outside the scope of constitutional law and beyond its reach.[280]

121. The new situation of the *Invisible Handshake* might seem to be a constitutional no-brainer: the State acts, and its activities impact human rights, directly or indirectly, intended or unintended. When the State spies on users' cyber-whereabouts, privacy is violated, and this violation requires justification. The first place to assess the legality and constitutionality of this act would be the Fourth Amendment and subsequent federal law.[281] To the extent that free speech is affected — and the chilling effect created when the State spies on its citizens is a case in point[282] — the First Amendment should be consulted. To the trained constitutional lawyer, so it might seem, all that remains is to apply the relevant doctrines to the newly acquired powers of the government. Within this application, however, things might not be that easy: after September 11, there is little doubt about the paramount importance of law enforcement efforts to prevent further terror attacks. A balanced approach is required here.[283] This decision might be extremely difficult, but at least the legal framework is known.

122. But the constitutional picture is more complex than the one just described. In the next few paragraphs we wish to point to some of these difficulties, which we do not purport to solve here. Our intention is more limited: to draw attention to the insufficiency of current constitutional law in addressing some aspects of the *Invisible Handshake*. The difficulty derives from the unique pattern of the State's new role, namely its use of the private powers that developed while the State acted as a regulator in the digital environment. This form of State power adds a third party to the usually bilateral constitutional setting, and turns it into a triangle. It is not the familiar *Governmental*

---

[280] The European terminology is helpful here: the State-Citizen level is referred to as the vertical dimension, whereas the Citizen-Citizen level is referred to as the horizontal dimension. Constitutional law deals with the vertical dimension.

[281] *See, e.g.*, U.S. v. Scarfo, 180 F. Supp. 2d 572, 578 (D.N.J. 2001) (finding that the FBI's use of a Key Logger System (KLS) did not violate the Fourth Amendment); *see also* Berger v. New York, 388 U.S. 41, 53 (1967); Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (a Fourth Amendment search occurs when government violates the subjective expectation of privacy that society recognizes as reasonable). The last two cases brought Congress to enact Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 82 Stat. 211, codified at 18 U.S.C. §§ 2510-2520, as amended. The Act is commonly known as the Wiretap Act.

[282] "In a democratic society privacy of communication is essential if citizens are to think and act creatively and constructively. Fear or suspicion that one's speech is being monitored by a stranger, even without the reality of such activity, can have a seriously inhibiting effect upon the willingness to voice critical and constructive ideas." PRESIDENT'S COMMISSION ON LAW ENFORCEMENT AND ADMINISTRATION OF JUSTICE, THE CHALLENGE OF CRIME IN A FREE SOCIETY 202 (1967), *quoted in* Bartnicki v. Vopper, 532 U.S. 514, 533 (2001).

[283] For an interesting attempt to curve the principles of such a balance, see Etzioni, *supra* note 133, at 280-81 (arguing that the starting point of the discussion should be that there are two valid claims which should be balanced — advancing the public interest in security and the protection of human rights, and searching for a balance by focusing on accountability).

Paradigm of State vs. Citizen, but State-[OSP]-Citizen. Let us break this triangle into its components: State-Citizen, State-OSP, OSP-Citizen.

123. The first of these relationships is the familiar *Governmental Paradigm*. A Citizen whose rights have been violated will naturally name the State as responsible for this violation, blame it, and eventually claim her rights.[284] The legal framework of such a claim is obvious: current constitutional law. A Citizen will only be able to seek an injunction or a declaratory relief. Under the (federal) sovereign immunity doctrine, a Citizen is barred from suing the government for damages.[285]

124. The second of these relationships, that of State-OSP, also falls within the *Governmental Paradigm*. An OSP that does not wish to cooperate with a governmental order (interception, data retention, data preservation, and the like) might argue, for example, that it is the owner of the data,[286] as well as of the computer system, and that requiring it to retain data imposes costs on it, and hence raises an issue of takings.[287] Or an OSP that offers content services might argue that it practices editorial discretion, and that governmental

---

[284] For this process see William L.F. Felstiner, Richard L. Abel & Austin Sarat, *The Emergence and Transformation of Disputes: Naming, Blaming, Claiming…*, 15 L. & SOC'Y REV. 631 (1980-1981).

[285] For a statement of the doctrine, see United States v. Nordic Vill., Inc., 503 U.S. 30, 33 (1992) (government's immunity from actions for monetary relief can be waived only if unequivocally expressed). 42 U.S.C. § 1983 (1979) enables a plaintiff to sue for damages when public (state) officials deprive the citizen of constitutional rights. Bivens v. Six Unknown Named Agents of Fed. Bureau of Narcotics, 403 U.S. 388, 397 (1971), created a parallel cause of action on the federal level. In the text we aim at the federal immunity, rather than state immunity from federal intervention, a matter which is addressed in the 11th Amendment.

[286] For a critical discussion of such arguments, see Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1377-91 (2000). Such a claim is not surprising in light of the increasingly proprietary view of information; *see also* THE COMMODIFICATION OF INFORMATION, *supra* note 50. A counter-argument is that the data subjects own the information about themselves, and not the collectors of the information. Reducing the discussion to property rights in information might serve as a basis for addressing the OSP-Citizen relationship, but suffers from major deficiencies. *See* Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1295-1301 (2000) (arguing that a property rights model of data, owned by the data subject, would be ineffective in protecting data privacy, and would result in encouraging transactions in data and vesting control in the hands of data collectors).

[287] Such a claim raises a host of "taking" questions, such as whether a data retention requirement is a regulation or a taking, a question that would require discussion of the governmental interest and the means-end fit, as well as the effect on the owner: does the requirement deny economically viable use? For a statement of the taking doctrine in regard to land use, see Agins v. City of Tiburon, 447 U.S. 255, 260-61 (1980). Another set of questions will address the application of the taking clause of the Fifth Amendment and the taking doctrine to data and to computer systems. The Supreme Court found intangible property rights are within the scope of the takings clause. *See* Ruckelshaus v. Monsanto Co., 467 U.S. 986, 1003 (1984) (trade secrets considered a protected property right for the purpose of the Fifth Amendment). For a discussion of the application of the doctrine to intangibles, see Thomas F. Cotter, *Do Federal Uses of Intellectual Property Implicate the Fifth Amendment?* 50 FLA. L. REV. 529 (1998). Other courts found, in other contexts, that computer systems are sufficiently tangible. *See* Thrifty-Tel, Inc. v. Bezenek, 46 Cal. App. 4th 1559, 1567 n.6 (1996) (electronic signals in telephone lines sufficiently tangible); eBay, Inc., 100 F. Supp. 2d at 1069 (electronic signals in computer system sufficiently tangible). In any case, the post-September 11 legislation that we examined, *supra* Part IV.B, includes compensation clauses to the OSP, so the remaining question will be whether the compensation is just.

interference violates its First Amendment rights.[288] The OSP might also argue that its data practices should be treated as commercial speech.[289] These arguments also fit within current constitutional law.[290]

125. The difficulty lies with the third of these relationships, that of OSP-Citizen. Consider the case of privacy, when Citizen's privacy is violated by the activity of an OSP that cooperates with the government. Citizen has a number of possible legal avenues. She might sue the government, under the legal model of the first relationship. However, this avenue is unavailable in those cases where the OSP voluntarily cooperated with the government, without being compelled or even approached by the government. There is no statute to argue against its constitutionality, and the possibility of invoking the state action doctrine seems unclear.[291]

126. A second legal avenue might be to sue the OSP. However, according to current constitutional law, the OSP-Citizen relationship lies within the realm of private law, void of a constitutional dimension. Within the contours of private law, it is not unlikely that the legal/digital environment would not provide any cause of action. A contractual claim might be absent for a number of reasons: in some cases there simply is no valid or enforceable contract between the OSP and Citizen,[292] or the contract is silent on this issue, or the State provides for immunity to the OSP.[293] Furthermore, monitoring the OSP system may violate the (privacy) rights of third parties (i.e., e-mail correspondence) that are subject to no contract with the OSP whatsoever. Is there a cause of action against the OSP for violation of privacy? Citizen will soon find out that American privacy law focuses on the *Governmental Paradigm*,[294] and its view of what is considered breach of privacy by private

---

[288] Courts found editorial discretion protected under the First Amendment in regard to various media. *See* Columbia Broad. Sys. v. Democratic Nat'l Comm., 412 U.S. 94, 120-21 (1973) (broadcast); Miami Herald Publ'g Co. v. Tornillo, 418 U.S. 241, 258 (1974) (print); Turner Broad. Sys. v. FCC, 512 U.S. 622, 636 (1994) (cable). In light of Reno v. ACLU, *supra* note 57, applying this doctrine to the digital environment should not run into particular difficulties.

[289] Eugene Volokh views privacy protection laws as a restriction on the speech rights of the collectors of the information, and warns against expanding such restrictions. *See* Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking about You*, 52 STAN. L. REV. 1049 (2000). For a critical discussion of the claim that data collectors have free speech rights in their data practices, see Cohen, *Examined Lives, supra* note 286, at 1408-23 (suggesting that "at most, data privacy regulation should be subject to the intermediate scrutiny applied to indirect speech regulation." *Id.* at 1418).

[290] *See, e.g.*, U.S. Telecom Ass'n v. F.C.C., 227 F.3d 450 (D.C. Cir. 2000).

[291] *See infra* note 297 and accompanying text.

[292] *See, e.g.,* Specht v. Netscape Communications Corp.*,* 150 F. Supp. 2d 585 (S.D.N.Y. 2001), *aff'd* 306 F.3d 17 (2d Cir. 2002) ("plug-in" software license not an enforceable contract); ProCD, Inc. v. Zeidenberg, 908 F. Supp. 640 (W.D. Wis. 1996), *rev'd* 86 F.3d 1447 (7th Cir. 1996) (shrink-wrap licenses enforceable, but subject to general contract law doctrines, such as unconscionability).

[293] For the immunity of OSPs, see *supra* text accompanying note 257.

[294] *See* Silverman v. United States, 365 U.S. 505, 511 (1961) (describing the Fourth Amendment to be "the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.") For recent judicial articulations of the Fourth Amendment, see Kyllo v. United States, 533 U.S. 27 (2001) (governmental use of a previously unknown device, that is not in general public use, to explore the internal space of a home without entering is a Fourth Amendment "search"). *See also* the Privacy Act of 1974, 5 U.S.C. § 552a (2003) (describing generally rules concerning disclosure of personal information by a government agency). There are other statutes that address the behavior of individual citizens, and define these particular activities as a violation of privacy. *See, e.g.,* Electronic

entities is rather limited. The American concept of privacy does not extend to personal data (also referred to as informational privacy).[295] The American approach is narrower than the European view, a gap that has raised many fears on both sides of the Atlantic, and resulted in complex legal mechanisms.[296] If the right violated is freedom of speech, Citizen might find it even more difficult to find the legal anchor on which she can hang her argument.

127. In these cases, Citizen is left with no real avenue to recover damages or seek protection of her rights. This situation requires a sound response. However, the public/private lines do blur occasionally. Such is the case of the state-action doctrine,[297] which might provide an answer to some of these cases. When a private entity's behavior renders it the status of a "state actor,"[298] constitutional law governs the legal landscape. If the doctrine were successfully invoked, the OSP's action (or inaction) would be evaluated under the Constitution. And if this is found to be unconstitutional, the result might be that the governmentally-sponsored, seemingly private activity of the OSP can be enjoined.[299] It is not unlikely that under this doctrine, in light of the post-September 11 legislation, an OSP that will be compelled to assist the

---

Communications Privacy Act of 1986, 18 U.S.C. § 2701 (2003) (prohibiting unlawful access to stored communication); Protection of Subscriber Privacy, 47 U.S.C. § 551 (2003) (prohibiting disclosure of personally identifiable information of subscribers by cable operators); Wiretap Act, 18 U.S.C. §§ 2510-2522 (2003) (prohibiting the interception of communication); Video Privacy Protection Act, 18 U.S.C. § 2710 (2003) (limiting disclosure of personally identifiable information by video service providers). *See also* RESTATEMENT (SECOND) OF TORTS § 652A (listing four situations as violation of privacy).

[295] See critical discussion in Cohen, *supra* note 286; Helen Nissenbaum, *Protecting Privacy in an Information Age: The Problem of Privacy in Public*, 17 L. & PHILO. 559 (1998).

[296] The European view is manifested in Council Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31. The 2000 Agreement between the Department of Commerce and the European Commission resulted in the "Safe Harbor Privacy Principles." *See* Commission Decision 2000/520/EC, 2000 O.J. (L 215) 7. For general discussion on the European Privacy Directive, see PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE (1998).

[297] For discussion of the state-action doctrine, see, *e.g.*, Lugar v. Edmondson Oil Co., Inc., 457 U.S. 922, 936 (1982) (The first question is whether the claimed deprivation has resulted from the exercise of a right or privilege having its source in state authority. The second question is whether, under the facts of this case, respondents, who are private parties, may be appropriately characterized as state actors.); Edmondson v. Leesville Concrete Co., Inc., 500 U.S. 614, 620 (1991) (applying *Lugar*); Am. Mfrs. Mut. Ins. Co. v. Sullivan, 526 U.S. 40, 50 (1999) (emphasizing that both prongs of *Lugar* are required to establish state action). For the history and various formulations of the doctrine, see G. Sidney Buchanan, *A Conceptual History of the State Action Doctrine: The Search for Governmental Responsibility,* 34 HOUS. L. REV. 333 (1997).

[298] Courts applied various tests in determining when a party is to be considered a "state actor." For example, when the examined activity is the result of the state's "coercive power," when there is a close nexus between the state and the challenged action, and when the state provided significant encouragement, it will be considered state action. *See* Blum v. Yaretsky, 457 U.S. 991, 1004 (1982). For a recent discussion of these various tests, see Brentwood Academy v. Tennessee Secondary School Athletic Association, 531 U.S. 288, 295-96 (2001).

[299] For the possible consequences of the application of the state action doctrine, see Buchanan, *supra* note 297, at 337-38.

government will be considered a state actor. Such a finding will, on the one hand, implicate constitutional limitations, require judicial review, and might subject the OSP or its officials to a "*Bivens* action."[300] On the other hand, such a finding might provide the OSP with immunity.[301]

128. In other cases, if the (private) litigation is based on a statute, the statute might be subject to constitutional scrutiny.[302] The property talk might be another legal space to explore the OSP-Citizen relationship: the OSP might claim a property right in the data collected,[303] either as a trade secret or as a copyrighted compilation of facts, if the selection and arrangement are original.[304] But the data-subject too might claim ownership in the information about herself.[305] Hence, the property talk is flawed and problematic.[306]

129. The difficulty, then, is that the OSP-Citizen relationship is limited, by definition, to the realm of private law, void of constitutional aspects. This difficulty has yet another prong, which is the separation of the State-Citizen relationship from the State-OSP relationship. Citizen has no say in the latter relationship, and has no bargaining power or an opportunity to negotiate the terms in which her privacy (or other rights) will be violated. Because these two relationships are distinct, the OSP is not accountable to Citizen, and Citizen lacks any effective means of learning how her privacy (or other rights) has been compromised.

130. The *Invisible Handshake* requires that we adjust our constitutional thinking. We should be aware of the entrance of a third player into the legal setting, namely the OSP, and the unusual structure of its relationship with the State.[307] It is not surprising that in analyzing situations in the third phase of the digital environment, commentators focus on the prong they are familiar with — the State-Citizen one, and ignore the vital role of the OSP in between.[308] While

---

[300] See *Bivens*, 403 U.S. 388.

[301] See Boyle v. United Technologies Corp., 487 U.S. 500 (1988) (federal law can shield government contractors from liability even in the absence of federal legislation).

[302] This, for example, is the case in defamation law, where both parties are individual citizens, but nevertheless, the constitutionality of the statute according to which the suit was brought is examined. *See* New York Times v. Sullivan, 376 U.S. 254, 269 (1964) ("libel can claim no talismanic immunity from constitutional limitations. It must be measured by standards that satisfy the First Amendment"); *id.* at 277 ("What a state may not constitutionally bring about by means of a criminal statute is likewise beyond the reach of its civil law of libel.") *See also Bartnicki*, 532 U.S. at 525, in which the majority defined the question at stake as "whether the application of [the Wiretap Act] in such circumstances violates the First Amendment." The Court concluded that the First Amendment protects the public disclosure of an illegally intercepted conversation when it is a "matter of public concern," and the person disclosing the conversation obtained it lawfully and was not involved in the interception.

[303] See the critical analysis of Cohen, *supra* note 286.

[304] *See* Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., Inc., 499 U.S. 340 (1991).

[305] *See* Litman, *supra* note 286.

[306] *See id.;* Cohen, *supra* note 286.

[307] Professor Daniel Solove suggests that an "architecture of power" be adopted, meaning a legal scheme which should address minimization (of governmental information gathering), particularization (*i.e.*, careful selection of targets) and control (*i.e.*, meaningful oversight). *See* Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1151-1167 (2002).

[308] *See, e.g.,* Etzioni, *supra* note 133, at 270-72 (discussing the constitutionality of roving intercepts); Catherine M. Barrett, Note, *FBI Internet Surveillance: The Need for a Natural Rights Application of the Fourth Amendment to Insure Internet Privacy,* 8 RICH. J.L. & TECH. 16 (2002) (advocating the

this is a crucial relationship to be explored, it should not leave the other prongs of this complex situation unexamined.

B. Information Policy

131. Our foregoing discussion focused on the way the State's re-entry into the digital environment may affect power relations among the different players.

132. The *Invisible Handshake* could further reframe several theoretical debates regarding the scope and nature of legal intervention in the digital environment. One issue that is vigorously debated in legal commentary about information policy focuses on Internet governance and the appropriate scope of State intervention in the online environment. Some argue that the State should shy away from regulating the Internet, leaving the arena to online self-governance and private ordering. Others believe that the online environment is not distinct from the physical environment. In fact, it is not an environment (cyberspace) at all, but simply a communication means which citizens of national States use to communicate. This activity requires State intervention just as any other human activity that could affect public welfare. The *Invisible Handshake* between the State and the private sector challenges the distinction between private ordering and public laws. This distinction served to restrain State intervention in the private realm. The convergence of interests and the collaboration between multinational, online-conglomerates and State enforcement agencies introduce a strong case for massive intervention for the sake of protecting civil rights.

133. Another debate relates to the liberating potential of IT. In its early days, the Internet raised high hopes for new opportunities to advance democracy and individual autonomy. Marshall McLuhan's famous slogan "the medium is the message" was adopted by those who believed that the Internet represented the ultimate technology of freedom.[309] Low production costs and negligible distribution costs promised to make any user a potential producer of content and the Internet an open forum of ideas. The new decentralized infrastructure that located information at the heart of the new economy destabilized existing structures of control over the production and dissemination of information. The information economy, it was argued, would facilitate decentralized structures for production and distribution of information. The potential for such a shift was already observed in the software industry, where production by well-established software companies was challenged by the decentralized development of Linux. It was also sensed in the music industry, where the status of record companies as the sole producers and distributors of music was shaken by the introduction of peer-to-peer (P2P) systems.

134. In reviewing the law-related literature concerning the regulation of information and the Internet, two competing approaches emerged. One

---

adoption of a natural-rights based theory to privacy, and subjecting Carnivore to a higher standard of review than the FBI submits); Jennifer C. Evans, Comment, *Hijacking Civil Liberties: The USA PATRIOT Act of 2001*, 33 LOY. U. CHI. L.J. 933, 974-81 (arguing that the USA PATRIOT Act violates the Fourth Amendment).

[309] *See* MARSHALL MCLUHAN, UNDERSTANDING MEDIA: THE EXTENSIONS OF MAN 7 (1964).

perceived this potential as encompassing a promise for greater freedom. The other was more skeptical of the feasibility of such decentralization, emphasizing its drawbacks for democracy.

135. Advocates of decentralization believe that opening up opportunities for creating and distributing information of all sorts on a non-commercial basis would decrease manipulation by economic superpowers, increase diversity, and ultimately lead to greater individual autonomy.[310] Others hold to the traditional liberal model of governance, arguing that liberal democracy requires at least some concentration of private expressive power capable of standing up to the government as well as the economic superpower.[311] The re-entry of the State raises some doubts as to the usefulness of relying on private powers for guaranteeing freedom. Not only has the private sector failed in mitigating the power of the State, it now joins forces with it.

136. The mixture of public, centrally-designed technologies and private initiatives created the dual nature of the Internet as an arena where two conflicting forces are operating. One is decentralized development, based on individual efforts and reflecting the spirit of civil society and individual freedom, and the other is a publicly designed environment which could be centrally controlled and monitored. The current *Invisible Handshake* reminds us that power nodes of any sort could be abused.

C. Design

137. Another important ramification of the current comeback of the State in the digital environment and the *Invisible Handshake* is the way it may affect ideas, ideologies and values which will subsequently shape the design of the digital environment.

138. It is by now widely accepted that technology is not void of values. The design of software, the architecture of the digital environment, or simply, code, both reflect and shape values simultaneously. Hence, in light of the *Invisible Handshake*, which signals a change of priorities of values, we foresee a change in the design: a design that will further the State's purposes and at the same time try to counter them.

139. There is a complex relationship between the history of ideas and technological change. A rather deterministic view perceives technological changes as provoking economic changes, thereby transforming social institutions. But the relationship between technology and ideas also acts in reverse. For instance, mass production could be viewed as an inevitable outcome of economic expansion, but it could also be attributed to major demographic changes during the twentieth century that led to a population explosion and created the "masses." The notion of the "masses" affected both political theory and the concept of the self, which in turn created a need for mass-produced goods.

---

[310] Yochai Benkler, *Siren Songs and Amish Children: Autonomy, Information, and Law*, 76 N.Y.U. L. Rev. 23 (2001).

[311] Neil W. Netanel, *The Commercial Mass Media's Continuing Fourth Estate Role*, *in* THE COMMODIFICATION OF INFORMATION, *supra* note 50, at 317.

Technology addressed that need. In other words, technology not only affects new paradigms but also assumes, reflects, and serves these paradigms.

140. The assertion that design embodies values requires a brief elaboration. Sometimes it is the case that the design reflects values without the programmers intending it. Lou Montulli invented cookies simply because he could not remember all his passwords, but these cookies have had a tremendous impact on privacy.[312] Tim Berners-Lee invented the World Wide Web because he could not find his way in his documents and wanted a convenient and intuitive method to connect them.[313] However, sometimes there is a deliberate intention on the part of the designer that the technology will reflect a certain value. This, for example, is the case with filtering software,[314] or with the W3C's initiative of Platform for Privacy Preferences (P3P).[315]

141. Jurists have noticed for some time that technology is not value-neutral and have drawn our attention to it. Professor Joel Reidenberg first called this "Lex Informatica,"[316] and Professor Lawrence Lessig then expressed a similar idea, encapsulated in the now famous statement that "Code is Law."[317] This insight is that code can shape the ways in which we go about in cyberspace no less than traditional direct public ordering, namely the law.

142. The state of war, the shaky post-national era, the reemergence of national identity and national boundaries, and the belief in or distrust of global harmony, in collective action, or communal actions — all create a new social and political environment. The fact that the State becomes more apparent on the Internet in the aftermath of September 11 is likely to change our expectations from digital networks. These expectations will surely shape the design of the digital environment in the near future.

VI. Conclusion

143. Imagine that a government agency suspects that someone in Virginia is involved in a conspiracy to plant a bomb in a café in Atlanta. Law enforcement agents, seeking to gather information about the suspect as quickly as possible, rush to AOL, and ask its local data security manager voluntarily to disclose all information related to that suspect. AOL cooperates and reveals all information related to the suspect, which it has on its servers.

144. In the old days law enforcement agents needed a judicial order authorizing search and seizure of the information. They would have to convince a court that their suspicions were reasonable and based upon a probable cause. Under

---

[312] *See* John Schwartz, *Giving the Web a Memory Cost Its Users Privacy*, N.Y. TIMES, Sept. 4, 2001.
[313] TIM BERNERS-LEE, WEAVING THE WEB: THE ORIGINAL DESIGN AND ULTIMATE DESTINY OF THE WORLD WIDE WEB (2000).
[314] *See, e.g.,* CyberPatrol, *available at* http://www.cyberpatrol.com/default.aspx; Net Nanny, *available at* http://www.netnanny.com/index.html.
[315] *See* World Wide Web Consortium, W3C Platform for Privacy Preferences (P3P) Project, *available at* http://www.w3.org/P3P/; LORRIE FAITH CARNOR, WEB PRIVACY WITH P3P (2002).
[316] Reidenberg, *supra* note 32.
[317] LESSIG, *supra* note 2.

the new regime, neither warrant nor subpoena is required. No court will ever consider the necessity of the State's actions; no judicial review will scrutinize whether this invasion of privacy was justified. In addition, there is no reason for the ISP to refuse such a request. In fact, ISPs may benefit from collaborating with the government in various ways. Furthermore, in some cases, as the one sketched above, the ISPs may very well sincerely believe that they are doing the right thing.

145. The USA PATRIOT Act imposes a citizen-soldier burden on the still rather young virtual gatekeepers of the information environment. They are perceived as best positioned to police terrorist-related activities. These gatekeepers, in the post-September 11 era, are more willing voluntarily to comply with laws like the USA PATRIOT Act. This is the *Invisible Handshake*.

146. This article sought to make the *Invisible Handshake* visible. We analyzed several major pieces of legislation from the post-September 11 era, which facilitate collaboration between law enforcement agencies and the private sector, beyond the reach of judicial review and away from the critical eye of public opinion. We then offered some thoughts on the new alliance of government and private industries: on constitutional law, information law and policy, and design of code. These aspects require close attention.

147. The *Invisible Handshake* might turn out to be successful in fighting terror online — but it might backfire by creating a monstrous concentration of power that is bound to threaten human rights. To make sure this new public-private cooperation is channeled toward the former scenario, and in order to avoid the latter, we ought to further study this handshake.

8 Va. J.L. & Tech. 6 (2003), *at* http://www.vjolt.net