THE THIRD INDUSTRIAL REVOLUTION: POLICYMAKING FOR THE INTERNET

BRADFORD L. SMITH*

Abstract: *The Internet heralds the onset of a third industrial revolution, one based in technological advances in software, hardware and telecommunications. These technological advances are transforming commercial practices, generating substantial gains in productivity and opening new avenues for political and social expression. But like the industrial revolutions that preceded it, the Internet revolution raises difficult legal and social issues, which in turn have generated a growing body of laws and regulatory proposals. This article seeks to provide an analytic structure for addressing and resolving the legal and policy challenges raised by the Internet. It endorses the use of self-regulatory and other extra-legal solutions to these challenges, but argues that governments should establish a supportive regulatory framework and should ensure that proposed solutions ultimately represent the public interest. This approach also seeks to look beyond traditional notions of the public and private sectors' respective roles and to articulate a model that harnesses each sector's unique strengths and abilities in reaching viable, practical solutions to online problems. Four themes form the cornerstones of this approach: (1) liberal use of market-based solutions; (2) reliance on technology solutions for problems rooted in technology; (3) recognition of government's multi-faceted role in responding to online challenges; and (4) support for broader international harmonization of applicable rules. This article also examines two prominent schools of legal scholarship in this area and argues that, while each provides valuable insights into law's relationship to the Internet, neither position offers a compelling response to key online legal and policy issues.*

I. Introduction

Three times in the past 250 years the world has witnessed a major transformation affecting virtually every aspect of society. Founded on advances in science and fueled by innovations in technology, these industrial revolutions produced major leaps forward in human productivity and changed the way people work and interact with each other. By the time such a

---

* Senior Vice President and incoming General Counsel, Microsoft Corporation. Columbia University School of Law, J.D. (1985); Institut Universitaire De Hautes Etudes Internationales, University of Geneva, Switzerland, Diplôme program (1983-84); Princeton University, A.B. (1981). This article was prepared based on ideas initially explored in Bradford L. Smith, *The Third Industrial Revolution: Law and Policy for the Internet*, 282 RECUEIL DES COURS 229 (Martinus Nijhoff 2000). The views expressed herein are solely those of the author and do not necessarily represent the position of Microsoft Corporation.

revolution runs its course, virtually every aspect of society has been affected in some significant way.

The first industrial revolution originated in Britain and lasted from roughly 1760 to 1830. It was founded on new methods of manufacturing based on iron and steam, and at its core were the first major advances since antiquity to use scientific reasoning to develop new products – in short, modern applied research.[1] These innovations ultimately spurred new forms of transportation such as the steamship and the railroad, as well as the invention of mechanical looms and other machinery, which together prompted socio-economic changes such as the introduction of specialized labor and the factory system.[2] Specialization and factories, in turn, led to widespread population shifts from rural to urban areas and to fundamental changes in the way people worked and interacted.[3]

The second industrial revolution lasted from about 1875 to 1930. It was powered by inventions such as electricity, the telephone and the internal combustion engine and automobile, as well as new synthetics and alloys and new applications of steel and oil. These advances were made possible by the unprecedented availability of capital and the creation of the modern business organization. Among the revolution's many socio-economic effects were greater mobility, a growing middle class and the beginnings of more widespread leisure time.[4]

Although different in many ways, these industrial revolutions shared certain characteristics. First, each was founded upon one or more new technologies that fundamentally changed manufacturing processes in a number of industries. Second, the adoption of these new technologies made it possible for manufacturers to improve productivity, which ultimately resulted in greater purchasing power and higher standards of living for broad segments of the population. Finally, these new technologies exerted profound and lasting effects on how people worked, socialized and used their leisure time.

Today the Internet is at the heart of a third industrial revolution. Made possible by technological advances in computer hardware, software, and telecommunications, the Internet has forced companies everywhere to reinvent themselves and the way they do business. This transformation in business practices has fueled unprecedented gains in productivity, generated

---

[1] For an analysis of the use of scientific reasoning in the process of invention during the first industrial revolution, see JAMES THOMAS FLEXNER, STEAMBOATS COME TRUE: AMERICAN INVENTORS IN ACTION (2d ed. 1992).

[2] *See* T.S. ASHTON, THE INDUSTRIAL REVOLUTION, 1760-1830 (2d ed. 1999). For an analysis of the importance of steam to this era, see FLEXNER, *supra* note 1, at 7-8.

[3] *See* ASHTON, *supra* note 2, at Introduction, 88-101.

[4] For a thorough review of the role of electricity in the second industrial revolution and the inventions that made use of it, see PAUL ISRAEL, EDISON: A LIFE OF INVENTION (1998). The importance of steel to this era is described in JOSEPH FRAZIER WALL, ANDREW CARNEGIE (1989); the development of the oil industry and the creation of the modern business organization are discussed in RON CHERNOW, TITAN: THE LIFE OF JOHN D. ROCKEFELLER, SR. (1998).

both by improvements in efficiency and the creation of new markets. At the same time, the Internet is profoundly changing the way people communicate with one another and express and enjoy themselves.

But as in any period of dramatic change, the Internet revolution raises several challenges and questions for legal systems around the world. To what extent do we need to adapt existing legal structures to facilitate efficient commercial practices while promoting innovation? How do we ensure that the law advances important social values that transcend these commercial interests? More fundamentally, what are the appropriate responsibilities of the public and private sectors in addressing these issues? Although several legal scholars – including David Post, James Boyle, Lawrence Lessig and others – have offered insightful critiques of law's relationship to the Internet, these authors have been less successful in articulating a coherent model for resolving the many social and legal issues that arise online.

This article seeks to provide such a model. Its thesis is that the Internet highlights the need for a new approach to solving legal problems rooted in technology. This approach focuses less on articulating specific solutions to such problems and more on providing a framework within which these problems can be identified and resolved. This approach endorses the use of extra-legal solutions to online problems, but tempers it with the recognition that public officials have an essential role to play in establishing an appropriate regulatory framework for such solutions and ensuring that these solutions ultimately represent the public interest. This approach seeks to look beyond traditional notions of sometimes starkly opposing roles for governments and private parties in addressing online social and legal problems and instead suggests a more balanced approach, one that harnesses the unique strengths and abilities of the public and private sectors in reaching viable, practical solutions to these problems.

Four themes animate this approach:

1. *Use of market-based solutions.* First, self-regulatory measures and related market-based solutions can often respond more quickly and effectively to the rapidly changing technologies and business models that characterize modern economic life than traditional government regulation. Society should normally begin by seeking to address Internet-related problems through market-based solutions and should then rely on direct legal intervention when these solutions prove to be inadequate.

2. *Technology solutions to problems rooted in technology.* Just as technology is at the root of many of the legal issues confronted in the online environment, so too can technology often provide a solution to these issues. Those who care about such problems should actively solicit technologists to help develop solutions to online challenges.

3. *A multifaceted role for governments.* First and foremost, pubic actors should work collaboratively with private-sector constituencies to identify online problems, unite diverse interests and encourage viable self-regulatory solutions. But governments also have a vital role to play in

crafting a supportive regulatory framework and "filling the gaps" in private-sector action through focused, technology-neutral laws.

4. *International harmonization.* The Internet minimizes the significance of geographic borders, and in doing so accelerates globalization – with its attendant advantages and disadvantages. To promote these advantages, and ameliorate the disadvantages, both the public and the private sectors should pursue internationally harmonized solutions to online problems.

Part II of this article begins with a brief history of the technological innovations that underlie the Internet and examines the economic significance of these innovations. Part II then examines two analyses of law's relationship to the Internet from respected legal scholars in this area. Against this background, Part III develops the proposed approach to Internet policymaking outlined above and examines how this approach might help policymakers evaluate among competing options to address technology-related problems. Part IV offers some final thoughts on the future of the Internet and how this future will continue to present challenges for policymakers, both public and private.

II. The Third Industrial Revolution

A. Technological Origins

Like the industrial revolutions that preceded it, the Internet revolution has its genesis in innovations in technology. Although a vast number of discrete innovative steps helped contribute to emergence of the Internet – and continue to fuel its growth – the Internet, as we know it, was made possible in large part by four advances in technology: (1) low-cost computing power based on the integrated circuit; (2) advanced software that has made computers more versatile and easier to use; (3) a high bandwidth telecommunications network; and (4) the development of the World Wide Web.[5]

There is room for debate about when this third industrial revolution started, especially in terms of when its broader economic impacts first took hold. As with all such prior historical epochs, this question may not be settled until long after it comes to an end and the dust has settled. It is perhaps easier to point to the dates and places when the technologies at its heart first began to take shape.

---

[5] The introduction of the Web, together with innovative browsers and search engines, expanded the Internet beyond the academic and research sectors and made the power of online computing much more accessible to the general public. *Cf.* THE EMERGING DIGITAL ECONOMY, U.S. DEPARTMENT OF COMMERCE, Ch. 1, at n. 12 (1998) (noting importance of introduction of web browser and opening of Internet to commercial activity as key factors in broadening public use of Internet), *available at* http://www.ecommerce.gov/viewhtml.htm (last visited October 8, 2001).

In that sense, the story begins in the summer of 1958 with the invention of the integrated circuit. Jack Kilby and Robert Noyce share the distinction of inventing the "integrated circuit" or microprocessor, now often referred to simply as "the chip."[6] The integrated circuit is credited as one of the most important inventions of the twentieth century,[7] yet it is impressive more for its impact on technology than for its sheer inventiveness. Kilby and Noyce, working separately and for competing companies, each integrated a number of individual pre-existing components – transistors, resistors, capacitors and connecting wiring – to make the integrated circuit a reality.

The invention of the microprocessor had a tremendous impact on the affordability of computing power.[8] By reducing the cost of computers while massively increasing their power, the microprocessor made computers accessible to many who could never have afforded or operated their predecessors.[9] Noyce later went on to start Intel Corporation with a friend named Gordon Moore, who led the project team at Intel that would eventually develop the first microprocessor chip, the Intel 4004. The 4004 was the first "computer on a chip." It integrated on a single chip all the parts that made a computer "think." As Moore continued his work on the microprocessor, he noticed that the computing power of the microprocessor doubled every 18 to 24 months, an observation known today as Moore's Law.[10]

Moore's Law had a tremendous impact on the computing industry, one that prompted a second important technological innovation. As computer processing power began to drop in price, it became increasingly apparent to some that the computer might one day become affordable to consumers and small- and medium-sized businesses. This could only occur, however, if the software used on these machines made them easier to use and if the computer industry's business model evolved towards a mass-market economics that would reduce prices.

---

[6] Charles C. Mann, *The End of Moore's Law?*, TECHNOLOGY REVIEW, May/June 2000, available at http://www.technologyreview.com/magazine/may00/mann.asp (last visited March 9, 2001).

[7] In October 2000, Kilby was awarded the Nobel Prize in physics for his part in the invention and development of the integrated circuit. *See Three Technologists Split Physics Nobel*, MSNBC NEWS (Oct. 10, 2000), at http://www.msnbc.com/news/474611.asp (last visited March 9, 2001).

[8] Kilby has said in hindsight, "What we didn't realize then was that the integrated circuit would reduce the cost of electronic functions by a factor of a million to one. . . . Nothing had ever done that for anything before." *See* Charles Zewe, *"Humble giant" Hailed for Inventing Integrated Circuit*, CNN INTERACTIVE (Sept. 9, 1997), at http://www.cnn.com/TECH/9709/09/chip.inventor/index.html (last visited March 9, 2001).

[9] In 1940, the Chairman of IBM, Thomas Watson, predicted that computers would never have widespread uses and that the entire world market for computers would add up to precisely five. Today, sixty years later, the number of computers in use around the world is estimated to exceed 300 million. *See Elementary, My Dear Watson: How Information Technology Can Boost Economic Growth*, THE ECONOMIST, Sept. 23, 2000, at 7 [*hereinafter Elementary, My Dear Watson*].

[10] *See* Mann, *supra* note 6.

As late as the early 1980s, the majority of computers used in commerce were built by companies such as IBM and DEC and ran proprietary operating systems and software applications developed specifically for each computer. This business model produced powerful machines that could do specific things well, but it also kept prices high and versatility low. Beginning in the mid-1970s, however, companies like Apple, Microsoft and others began to develop operating systems and applications designed for the small but growing market of individual computer users and enthusiasts. This software was more appropriate for a mass-market business model because a single version of the software could accomplish a variety of tasks and support a broad array of applications, and could be used by non-experts without difficulty.[11] These innovations laid the groundwork for companies such as Dell, Compaq and others to develop a similar mass-market business model for the computers on which this software could run. As economies of scale in both the software and hardware industries began to take hold, prices dropped dramatically.[12]

At the same time that personal computers were beginning to spread, a third important development was emerging, this one in the area of telecommunications. As late as the mid-1980s, phone service in nearly every country in the world was provided by telecommunications monopolies that were either state-owned or state-sanctioned. In 1984, for example, AT&T Corporation controlled 95 percent of the U.S. long distance market and provided most local services through its wholly owned subsidiaries.[13] Beginning in the 1980s, however, governments around the world began liberalizing, to varying degrees, the market for basic telephone services. Liberalization of the U.S. telecommunications market began with the 1984 divestiture by AT&T, which ended AT&T's monopoly over long distance service and divided local telephone service among the newly independent Baby Bells.[14] Europe followed suit in 1990 with the European Commission's Services Directive, which imposed deadlines for telecommunications liberalization in its Member States.[15] This liberalization, together with important innovations in the areas of cable-based and wireless telecommunications services, greatly expanded the availability of moderately priced telecommunications bandwidth to large segments of the population.

---

[11] *See* WILLIAM H. GATES, THE ROAD AHEAD (1995) at 20-51.

[12] For example, the cost of one megahertz of computing power has dropped from $7600 in 1970 to $.17 today. The cost of storing one megabit of information has likewise fallen, from $5257 in 1975 to $.17 in 1999. *See* U.S. FEDERAL RESERVE BANK OF DALLAS, THE NEW PARADIGM : 1999 ANNUAL REPORT 9 (1999) [*hereinafter* THE NEW PARADIGM].

[13] See James A. White, *Local Bell Companies Begin Push to Re-enter Long-Distance Market*, WALL STREET JOURNAL, February 2, 1984.

[14] See AT&T, THE BACKGROUND TO DIVESTITURE, at http://www.att.com/corporate/restructure/hist2.html (last visited March 9, 2001).

[15] *Commission Directive 90/388/EEC of 28 June 1990 on Competition in the Markets for Telecommunications Services*, 1990 O.J. (L 192), p. 1.

The realities of Moore's Law, higher telecommunications bandwidth and the new mass-market business model in the information technology (IT) industry gave birth to a colossal increase in the availability and use of computers throughout the world. Standard software applications such as word processors and spreadsheets made computers both more useful and easier to use, while computer games introduced a whole new type of recreation. But as late as 1990, only 22 percent of U.S. households had a computer, and in other countries the figure was far lower.[16] And despite growing investment by businesses, information technologies were not causing noticeable increases in productivity or living standards.[17]

It took the advent of a fourth innovation to unleash more broadly the potential of microprocessors, software and high bandwidth telecommunications. This new technology came from the work of Tim Berners-Lee, a British computer scientist. In 1989, while working at CERN, the European Laboratory for Particle Physics in Switzerland, Berners-Lee proposed a new global hypertext project for the Internet that was designed to allow people to collaborate and share information through inter-connected hypertext documents.[18] His program, called "WorldWideWeb," was first made available within CERN in December 1990 and on the Internet at large in the summer of 1991.

Berners-Lee's new technology dramatically changed the Internet. It allowed people to publish words, pictures and sounds online. It enabled businesses to exploit their information technology resources not only to share information within their own companies, but with customers, suppliers, and anyone else located anywhere in the world. Just four years after Berners-Lee introduced the World Wide Web, Internet use started to grow exponentially – a trend that has continued since then.[19]

The creation of the World Wide Web constituted the final building block of the new, information-based economy. Soon thereafter, evidence started to mount that the United States – and to an increasing degree other countries as well – were beginning to witness the most fundamental economic and social changes since the end of World War II, changes that strongly

---

[16] *See* THE NEW PARADIGM , *supra* note 12, at 9.

[17] *See* Mann, *supra* note 6, at 3-4 (referring to disparity between growth in IT investment and lack of corresponding gains in productivity as "the productivity paradox").

[18] See TIM BERNERS-LEE, LONGER BIOGRAPHY, at http://www.w3.org/People/Berners-Lee/Longer.html (last visited March 9, 2001). The term "Internet" is typically used to refer to the global information system that is logically linked together by, and is able to support communications using, two widely accepted protocols—specifically, the Transmission Control Protocol (TCP) and Internet Protocol (IP)—or their subsequent extensions, and which provide, use, or make accessible various higher-level services (such as the World Wide Web). *See* FEDERAL NETWORKING COUNCIL, RESOLUTION: DEFINITION OF "INTERNET" (Oct. 24, 1995), available at http://www.itrd.gov/fnc/Internet_res.html (last visited October 8, 2001).

[19] *See* THE EMERGING DIGITAL ECONOMY, *supra* note 5, Ch. 1, at 2 (noting that, after the Internet was opened to the public and commerce, the number of Internet users grew to 50 million within four years).

suggest the advent of a third industrial revolution. And economists and others increasingly started to point to the Internet as a principal catalyst for these changes.

One of the remarkable features of the technological advances culminating with the World Wide Web has been the breadth of their impact. Most technological innovations, even very important ones, affect only one or a limited number of industries. The jet propulsion engine, for instance, radically changed the airline industry and greatly expanded opportunities for long-distance travel, but otherwise had relatively little affect on most other industries. The Internet, by contrast, is pervasive both horizontally – in terms of how broadly it is being deployed throughout the economy – and vertically – in terms of the extent to which it is changing companies' internal organizations and external relationships with customers and suppliers. As one recent article noted,

> It took more than a century after its invention before [the steam engine] became the dominant source of power in Britain. Electricity achieved a 50% share of the power used by America's manufacturing industry 90 years after the discovery of electromagnetic induction, and 40 years after the first power station was built. By contrast, half of all Americans already use a personal computer, 50 years after the invention of computers and only 30 years after the microprocessor was invented. The Internet is approaching 50% penetration in America 30 years after it was invented and only seven years since it was launched commercially in 1993.[20]

The pervasiveness of Internet technologies is attributable in part to their steep drop in price. Since 1970, the real price of computer processing power has fallen by 99.999%, an average decline of 35% per year.[21] Telecommunications prices have likewise fallen, albeit at a slower pace. In 1930, a three-minute call from New York to London cost $300 in today's dollars; the same call now costs less than 20 cents, reflecting an annual decrease in price of roughly 10%.[22] These rapid, ongoing gains in the price/performance ratio of Internet and other relevant technologies have made it possible for even individuals and small businesses to participate in the online economy.

Another remarkable feature of these technologies is the degree to which they have fueled further creativity and innovation. This creativity is not limited to new products; it

---

[20] *See Elementary, My Dear Watson*, *supra* note 9, at 8.

[21] *Id*. *See also* THE NEW PARADIGM, *supra* note 12, at 6.

[22] *See Elementary, My Dear Watson*, *supra* note 9, at 8. *See also* THE NEW PARADIGM, *supra* note 12, at 9 ("Sending the *Encyclopaedia Britannica* coast to coast would have cost $187 in 1970, largely because of slow data-transmission speeds and the expense of a long-distance telephone call. Today, the entire Library of Congress could move across the nation on fiber-optic networks for just $40.").

includes innovations in business organization, financial services, and other areas. As described in a recent Department of Commerce study,

> [A] dynamic of cascading or continuous innovation has characterized the development and deployment of information technologies in this period. Productivity gains come not just from deploying innovative technologies that enable workers to process information faster. In addition, firms intent on taking advantage of innovative new technologies often have to rethink the way they operate and reorganize their operations, which can produce a round of organizational innovation. Many firms also have discovered that the new technologies can be used to develop and produce new goods or services for themselves, producing yet another round of innovation. Furthermore, as these areas of potential are widely recognized and the process spreads from firm to firm, this generates demand for faster information processing. This can lead to another round of innovation in IT itself.[23]

Further evidence of the importance of these new technologies is the sharp rise in U.S. productivity during the latter half of the 1990s.[24] Economists often regard productivity growth as the single best indicator of macro-economic performance because positive growth allows firms to raise wages without raising prices, thus creating real, non-inflationary growth (wage increases funded solely by higher prices for goods and services, by contrast, provide no real economic growth and, more importantly, no net gain in consumer purchasing power).[25] As the Department of Commerce study notes, "After quietly improving in speed, power, and convenience since 1969, the Internet burst onto the economic scene [in the second half of the 1990s] and began to change business strategy and investment. At the same time, the U.S. economy has enjoyed a remarkable resurgence. Productivity growth . . . doubled its pace from a sluggish 1.4-percent average rate between 1973 and 1995, to a 2.8-percent rate from 1995 to 1999."[26] Economists in the private sector have also attributed this rise in productivity to Internet-related technologies. As one economist concluded, "the recent acceleration in productivity is at least half due to the improvements in computer productivity."[27] And even with

---

[23] DIGITAL ECONOMY 2000, U.S. DEPARTMENT OF COMMERCE, at xiv (2000).

[24] *See* Mann, *supra* note 6.

[25] For two good governmental reviews of the broad economic impact of these technology advances, see DIGITAL ECONOMY 2000, *supra* note 23; THE NEW PARADIGM, *supra* note 12.

[26] DIGITAL ECONOMY 2000, *supra* note 23, at 1. The report goes on to conclude, "Evidence is increasing that these two phenomena [business use of the Internet and productivity growth] are not coincidental but derive substantially from the same phenomenon: the synergistic convergence of dramatic increases in computer power, an explosion in connectivity, and increasingly powerful new software." *Id.*

[27] Mann, *supra* note 6; *see also* Digital Economy 2000, *supra* note 23, at vi ("Six major economic studies have recently concluded that the production and use of IT contributed half or more of the acceleration in U.S. productivity growth in the second half of the 1990s.").

the recent slowdown in U.S. economic activity, the 1990s productivity surge extended for a longer duration than any similar period of productivity growth since the 1940s.[28]

Evidence of the Internet's economic impact can be found not only in macro-economic statistics but also in the experiences of individual companies. For instance, General Motors (GM) recently announced that its four-year, $1.6 billion effort to restructure its business around electronic commerce had already resulted in cost savings of $800 million annually. GM also predicted that, by 2003, its Internet-based supply and manufacturing system would enable consumers to receive a custom-ordered car in 10-15 days.[29]

Although the economic ramifications of these new technologies are perhaps easier to quantify, they are having profound social affects as well. The Internet is freeing people from time-consuming routine personal tasks and – like the two industrial revolutions that preceded it – is altering the way people use their leisure time and interact with each other. The Internet is also greatly expanding the avenues for political and cultural expression. When Serbian authorities in Belgrade took Radio B92 off the air for broadcasting information opposed by the government, the station placed its programming onto the Internet via a Dutch service provider. Radio Free Europe, Voice of America and the German Deutsche Welle then rebroadcast the programming by radio back into Serbia, where it served as an important source of independent reporting and a focal point for democratic opposition.[30] When a governmental body in the UK sought to suppress publication of an official report on child abuse, the report was published online and immediately mirrored on numerous Internet sites around the world, thus effectively preventing its suppression.[31] These examples illustrate how the Internet is shifting the traditional balance of power between individuals and those who provide (or control) access to information.[32]

Taken together, the evidence is mounting that we are indeed in the midst of a third industrial revolution. This industrial revolution has already raised important economic, social and cultural challenges and undoubtedly will continue to do so. These challenges have implications for law and lawmakers. Importantly, law and policy will not merely be affected by

---

[28] *See* THE NEW PARADIGM, *supra* note 12, at 2, 4 & n.2.

[29] *See Why GM is Going E-Crazy*, WIRED NEWS, June 22, 2000, at 1, available at http://www.wired.com/news/business/0,1367,37155,00.html (last visited March 9, 2001). *See also* THE NEW PARADIGM, *supra* note 12, at 13 ("In 1985, when Ford Motor Co. wanted data on how cars withstood accidents, it spent $60,000 to slam a vehicle into a barrier. Today, Ford's supercomputers can simulate the same collision in 15 minutes for $200. By 2001, the cost of a frontal 'crash' in cyberspace will be down to just $10.").

[30] *See* GLOBAL INTERNET LIBERTY CAMPAIGN, REGARDLESS OF FRONTIERS: PROTECTING THE HUMAN RIGHT TO FREEDOM OF EXPRESSION ON THE GLOBAL INTERNET, at Part II.C, available at http://www.cdt.org/gilc/report.html (last visited March 9, 2001).

[31] *Id*.

[32] *Cf*. ANDREW L SHAPIRO, THE CONTROL REVOLUTION 38-43 (1999) (noting the degree to which the Internet is shifting balance between consumers and producers of information).

this new industrial revolution; they have critical roles to play in enabling societies around the world to shape and participate in it.

B. Responses From the Academy

The legal and policy ramifications of the Internet have inspired a variety of governmental responses. Even before the Internet caught the eye of legislators, however, it captured the imagination of academia – and notably, law professors. In the past decade, articles and books devoted to law and the Internet have flourished as scholars from all corners of the legal community have set about tackling every imaginable issue relating to cyberspace.[33] Within this diverse universe of scholarship, two schools of thought have proven particularly robust. One school of thought has been labeled "digital libertarianism"; the other might be characterized as "digital structuralism."[34] These views are noteworthy for two reasons. First, each seems to capture certain deep-seated popular beliefs on the Internet and law's relationship to it. Second, and more interestingly, these views hold profoundly contradictory views on the Internet's most salient attributes and on the respective roles of the public and private sectors in solving problems associated with cyberspace.

Digital libertarianism has its spiritual roots in the early days of the Internet, before it was opened to commercial use and was largely the province of academics and researchers.[35] These Internet pioneers often viewed themselves as a close-knit if highly diverse community. Because few people inside or outside this community saw much need to regulate what went on there, the Internet was often viewed as a vitally free, almost anarchic place that had more in common with the mythical Wild West than with late twentieth-century society.

This anarchic impulse lives on in digital libertarianism. The hallmark of digital libertarian thought is that freedom from "outside" control, particularly legal control, is one of the Internet's defining characteristics. In part this conclusion is based on the view that the Internet occupies a unique space in which the territorial boundaries that generally are central to

---

[33] For example, a search of the Westlaw database "Journals and Law Reviews" (JLR) on October 6, 2001, for publications with "internet" or "cyberspace" in the title and published since 1990, yielded 2437 documents.

[34] The label "digital libertarianism" appears in James Boyle, *Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors*, 66 U. CIN. L. REV. 177, 177-78 (1997). Margaret Jane Radin and R. Polk Wagner apply a slightly different label in *The Myth of Private Ordering: Rediscovering Legal Realism in Cyberspace*, 73 CHI.-KENT L. REV. 1295, 1297 (1998) (referring to "cyberlibertarians," "cyberanarchists" and—Radin's and Wagner's favorite—"anarcho-cyberlibertarians"). The term "digital structuralism" does not appear to have been used previously in this context.

[35] Until 1991, the National Science Foundation prohibited commercial uses of the Internet. *See Life on the Internet Timeline*, PBS ONLINE, available at http://www.pbs.org/internet/timeline/index.html (last visited on March 12, 2001).

government definition and legitimization of power have little or no significance.[36] Because the Internet is a global network in which location has only logical rather than geographic significance,[37] any assertion of legal authority by geographically limited governments over the Internet is – the argument goes – almost by definition an illegitimate grab for power. In part, however, this view is also founded on the conviction that there is something about the very nature of the Internet that eludes control. To paraphrase a common digital libertarian theme, the Internet deals with regulation as a malfunction and roots around it.[38] As a result, attempts by public authorities to impose real-world laws onto the Internet are assertedly not only improper, but also doomed to failure.[39]

But for digital libertarianism, the implication of this view is not a virtual Hobbesian free-for-all, but a kind of spontaneous, self-ordering communitarianism. Rules for the Internet, in this view, will emerge from within the online community itself:

> Separated from doctrine tied to territorial jurisdictions, new rules will emerge to govern a wide range of new phenomena that have no clear parallel in the nonvirtual world. These new rules will play the role of law by defining legal personhood and property, resolving disputes, and crystallizing a collective conversation about online participants' core values.[40]

---

[36] *See* David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1378 (1996) ("[m]any of the jurisdictional and substantive quandaries raised by border-crossing electronic communications could be resolved by one simple principle: conceiving of Cyberspace as a distinct 'place' for purposes of legal analysis . . ."); *see also* David G. Post, *Anarchy, State, and the Internet: An Essay on Law-Making in Cyberspace*, 1995 J. ONLINE L. art. 3, par. 36 ("[T]he Internet is not merely multi-jurisdictional, it is almost 'a-jurisdictional:' physical location, and physical boundaries, are irrelevant in this networked environment in a way that has . . . no parallel elsewhere."), at http://warthog.cc.wm.edu/law/publications/jol/post.html (last visited March 9, 2001).

[37] "Location" on the Internet is determined by Internet Protocol ("IP") addresses, which map to servers rather than places. Thus, a server and its web site can be moved to the next town or half way across the world without affecting its address or online attributes. *See* Post & Johnson, *supra* note 36, at 1374.

[38] *See* John Perry Barlow, *Keynote Address*, 1994 ANN. SURV. AM. L. 355, 357 ("[T]he Internet deals with censorship as a malfunction and roots around it. And it actually deals with any regulation whatsoever as a malfunction and roots around it. It was designed to do that."). Boyle attributes this idea to John Gilmore, one of the founders of the Electronic Frontier Foundation. *See* Boyle, *supra* note 34, at 178.

[39] Lawrence Lessig has captured the essence of digital libertarianism nicely: "[There is] an idea that defines first generation thought about the [Internet]. Cyberspace, it is said, cannot be regulated. It 'cannot be governed'; its 'innate ability' is to resist regulation. . . . In its essence, cyberspace is a space of no control." LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 24 (1999). *See also* Boyle, *supra* note 34, at 178-84.

[40] Post & Johnson, *supra* note 36, at 1367.

In short, the theory is that those in the private sector who are affected by online behavior and care most deeply about what happens there will ultimately determine the rules by which that behavior is controlled.

Standing in almost antithetical contrast to digital libertarianism is digital structuralism. Although elements of digital structuralism can be found in many recent articles, two highly regarded exponents of this view are James Boyle and Lawrence Lessig.[41] Digital structuralism parts company with digital libertarianism most decisively by questioning its faith in online technologies – specifically, that these technologies somehow make the Internet immune from control. Digital structuralism contends that the Internet has no essential nature that prevents online control. On the contrary, the Internet's technological infrastructure, or "architecture" – particularly the software used to construct and navigate online space – can and often does constrain online behavior. If digital libertarianism's battle cry is "The Internet is free," the digital structuralists' rejoinder is "Code is law."[42] As Lessig has remarked, "[The Internet's] architecture will affect whether behavior can be controlled. . . . [I]ts architecture is its politics."[43]

This observation often leads digital structuralism to a further, more ominous conclusion. Because Internet technologies are developed by the private sector, and because (the argument continues) online commerce functions better in an environment of greater as opposed to less control, private-sector commercial interests will have a natural tendency to favor technologies that limit online freedom – and indeed to move toward an online universe of perfect control through technology.[44] To make matters worse, because lawmakers and bureaucrats are in the business of regulation, they will supposedly have little incentive to counter this tendency and may even encourage it.[45] One answer that has been suggested is for courts to extend Constitutional protections that were designed to prevent *governmental* abuses of power onto the largely *non-governmental* online environment.[46]

---

[41] *See, e.g.*, Boyle, *supra* note 34; JAMES BOYLE, SHAMANS, SOFTWARE AND SPLEENS: LAW AND THE CONSTRUCTION OF THE INFORMATION SOCIETY (1996); LESSIG, *supra* note 39; Lawrence Lessig, *The Zones Of Cyberspace*, 48 STAN. L. REV. 1403 (1996); Lawrence Lessig, *The Path Of Cyberlaw*, 104 YALE L.J. 1743 (1995).

[42] LESSIG, *supra* note 39, at 6.

[43] *Id*. at 20.

[44] LESSIG, *supra* note 39, at 30-42; *cf*. Boyle, *supra* note 34, at 195, 198-201.

[45] Boyle, *supra* note 34, at 188-205; LESSIG, *supra* note 39, at 43-60. For instance, Lessig examines instances in which the United States has attempted to impose technical requirements on network intermediaries and concludes, "when government regulation of the architecture of the Net is tied to the changes that commerce is already introducing, I argue, the government will need to do very little to make behavior on the Net highly regulable." *Id*. at 44.

[46] *See* LESSIG, *supra* note 39, at 217-21; 223-24.

In interesting ways, then, digital libertarianism and digital structuralism stake out opposing positions on a number of issues: The nature of Internet technologies, the relationship of these technologies to regulation, and the proper roles of the public and private sectors in addressing online behavior. So which position is right? Well, neither. Because while both offer valuable insights over the relationship of law and the Internet, each ultimately stakes out positions that fail to resolve the crucial legal and policy issues confronting online networks in a satisfying or convincing way.

Let's consider digital libertarianism first. Among digital libertarianism's greatest contributions is its insistence that the Internet's global reach should inform the manner in which online conduct is regulated.[47] Thus, it certainly is correct that, to the extent that online activities may affect users in tens or even hundreds of legal jurisdictions simultaneously, the Internet's global character must be taken into account when governments act to control these activities. Digital libertarianism is also right to emphasize the positive role that Internet users and technologies can play in solving online problems. Finally, digital libertarians correctly point out that traditional lawmaking is sometimes inadequately suited to keep pace with the innovation and dynamism of cyberspace.[48]

In other respects, however, digital libertarianism misses the mark. First, it never quite succeeds in explaining why online activity should *never* be subject to government-made law. The jurisdictional argument alone is not enough: laws and courts have been forced to confront the jurisdictional complexities of cross-border electronic transmissions since at least the invention of the telegraph and telephone.[49] While the one-to-many, interactive character of the Internet undoubtedly complicates the analysis, there is no reason to think that established doctrines of jurisdiction are too fragile to deal with this change. So long as people use the Internet to perpetrate frauds, steal property, and defame and assault one another, governments will be justified in seeking to prevent such behavior through law.

Second, the digital libertarian characterization of the Internet as a technology that invariably frustrates outside efforts at control does not accurately describe many online technologies. As Lessig and others have argued, the Internet experience is largely a function of its underlying architecture – the software and hardware through and by means of which online transmissions take place.[50] While it is certainly true that many online technologies place

---

[47] This observation has been echoed by scholars who do not otherwise fit snugly within the digital libertarian camp. *See, e.g.*, Henry H. Perritt, Jr., *The Internet is Changing the Public International Legal System*, 88 KY. L. J. 885, 895-930 (1999-2000).

[48] *See, e.g.*, Barlow, *supra* note 38, at 357 ("[Cyberspace] is a place that is in continuous, never-ending metamorphosis at a galloping rate of speed, and there is a fundamental parity mismatch between that rate and the rate by which law adapts to new social circumstance, which is second only to geology in the stateliness of its pace . . .").

[49] *See* Jack Goldsmith, *Regulation of the Internet: Three Persistent Fallacies*, 73 CHI.-KENT L. REV. 1119, 1120 (1998) (criticizing digital libertarian jurisdictional arguments against online regulation).

[50] *See* text accompanying notes 41 through 43, *supra*.

relatively few constraints on online behavior (and were designed that way), it is equally clear that many technologies *do* limit what people can do online.[51]

Finally – and perhaps most importantly – digital libertarianism's belief that a spontaneous, self-ordering structure will arise and can on its own adequately regulate online activity seems misplaced. The Internet does indeed open new avenues for self-regulation and other mechanism by which users can influence online behavior and norms. Yet even the best of these efforts can be effective only against a background set of laws that establish the ground rules and provide effective constraints on behavior that is inconsistent with those rules.[52]

Now let's turn to digital structuralism. Digital structuralism has contributed importantly to the debate on law and the Internet by emphasizing the crucial regulatory effect of technology over online behavior. This insight highlights the degree to which political and policy issues are not separate from, but indeed are sometimes woven into, the very fabric of online technologies. Yet other tenets of digital structuralism are less convincing.

First, although digital structuralism is right to criticize digital libertarianism for characterizing the Internet as unregulable, digital structuralism falls short in characterizing online technologies as potentially omnipotent instruments of control. Internet technologies are tremendously diverse, and the ways in which these technologies develop, how effective they are and – crucially – whether they succeed in a competitive marketplace are difficult if not impossible to predict. Similarly, the digital structuralist tendency to focus on the threats that online technologies may pose to civil liberties frequently seems to give insufficient regard to the extent to which Internet technologies – including those that enable and facilitate commerce – often are used to promote political and civil liberties.[53]

Related to this is digital structuralism's basic mistrust of private-sector initiatives to regulate online conduct. Online commercial interests, in this view, almost inevitably veer toward ever more restrictive mechanisms of control; market pressure for technologies that

---

[51] In many cases, this is a very good thing. Online banks, for instance, use digital signatures, encryption, and a variety of other technologies to "constrain" an account-holder's ability to access accounts that don't belong to him, transfer other people's money, and engage in a host of other activities. Without these constraints, or course, online banking would not be a viable business.

[52] *See, e.g.*, Radin & Wagner, *supra* note 34, at 1297-98. This thesis is developed in more detail in Part III.C, *infra*.

[53] This is not to say that digital structuralism does not also acknowledge that certain technologies may be useful in protecting online freedoms. Indeed, Lessig at one point contends that encryption technologies, which can be used to encode online messages in order to preserve their confidentiality, "are the most important technological breakthrough in the last one thousand years." LESSIG, *supra* note 39, at 35. Nevertheless, digital structuralism's overriding concern often seems to be that Internet technologies – though themselves effectively neutral – are so effective at regulating online action that they may be used in ways that pose significant threats to online freedoms. *See generally* text accompanying notes 40 through 44, *supra.*

prevent such control is largely viewed as insignificant.[54] But even a brief survey of private-sector initiatives in the online environment highlights the fallacy of this position. Indeed, as discussed in more detail below, there are good reasons for arguing that private-sector efforts are particularly well suited for the Internet environment and can play a vital role in safeguarding online freedoms.[55]

Digital structuralism also seems to overlook digital libertarianism's greatest contribution – namely, that the Internet's global reach should inform the manner in which we approach online regulation. Digital structuralism's proposal that courts ultimately should resolve online issues sometimes seems insensitive to the fact that judicial intervention of this sort might have significant repercussions on people beyond the jurisdiction of such courts, people who may well have different views on the appropriate allocation of rights between the State and the individual and different conceptions on the proper limits of judicial action. A successful strategy for addressing online problems should have some proposal for addressing these legal and cultural differences.

Finally, perhaps most remarkable is that even as digital libertarianism and digital structuralism espouse quite different conceptions of online technologies,[56] neither of these conceptions seems to capture the true essence of those technologies or the complexity of their relationship to online legal issues. In a manner not appreciated fully by either position, Internet technologies play a strikingly ambivalent role in the social and legal challenges that arise online today. To some extent, this is because, at their core, Internet technologies are simply tools that, like most tools, can be bent in different directions and used for various ends. Just as some people use Internet technologies to perpetrate crimes and violate rights, others use online technologies to protect themselves from such acts or to prevent these acts from occurring in the first place.[57] Another reason is that online technologies are constantly and rapidly changing, often through the efforts of people with diverging objectives, with the result that any specific portrayal of online technologies that seems accurate today might well be inaccurate tomorrow.

---

[54] Thus, only the courts can be relied upon to "regulate" online behavior – the exact opposite conclusion of digital libertarians, who think courts (and other government actors) should *not* regulate online behavior.

[55] *See* Part III.A and III.B, *infra*.

[56] While digital libertarianism frequently characterizes online technologies as subverting "outside" control over the Internet, *see* text accompanying notes 37 through 39, digital structuralism often portrays these technologies as the principal means by which such control is exerted, *see* text accompanying notes 41 through 44. Indeed, these differing conceptions of technology arguably account for many of the differences between digital libertarianism's and digital structuralism's views over how online conduct should be regulated.

[57] *See, e.g.*, FEDERAL TRADE COMMISSION, FIGHTING CONSUMER FRAUD: NEW TOOLS OF THE TRADE (1998) (documenting criminal uses of standard Internet technologies and recommending consumer responses to these threats), *at* http://www.ftc.gov/reports/fraud97/consumer.htm (last visited March 9, 2001); FEDERAL TRADE COMMISSION, THE FTC'S FIRST FIVE YEARS: PROTECTING CONSUMERS ONLINE (1999) (same), *at* http://www.ftc.gov/os/1999/9912/fiveyearreport.pdf (last visited March 9, 2001).

For these reasons, Internet technologies are not and never will be truly paramount in defining the activities of those who use the Internet, in resolving problems that arise online, or in compelling or resisting the role of law or hand of government. Instead, as with technological advances that preceded it, any effort to address public issues on the Internet must focus on the interaction between – and the contributions from – both technological advances and other private and public sector actions. The next Part examines how the public and private sectors, working together, might most successfully do so.

III. Approaching Regulatory Action for the Internet

As set forth above, this article contends that the Internet constitutes the heart of a third industrial revolution. Like its predecessors, this industrial revolution has its roots in new technologies that are fundamentally changing the face of commerce and basic patterns of human work and interaction. Part II traced the technological underpinnings of the Internet revolution and examined two responses to this revolution from leading legal scholars in this area.

This Part explores how the integration of the Internet into contemporary commercial and social life highlights the need for new approaches to solving challenges rooted in technology. The overarching thesis here is that the Internet requires a multifaceted regulatory model, one in which governments and the private sector work collaboratively to solve technology-related issues in ways that are more flexible, responsive, and market oriented than has traditionally been the case. This model envisions important roles for both the public and private sectors, and particularly sees an important role of governance as establishing a baseline of legal rules and then building on this by encouraging public-spirited, extra-legal solutions to online problems.

This new approach – referred to here as "digital pragmatism" – offers an alternative to both digital libertarianism and digital structuralism. It contends that technology-based and other market-driven mechanisms can often address online problems in ways that are more responsive and efficient than traditional regulatory intervention. At the same time, it recognizes that such private-sector mechanisms can only be effective against a background set of rules and policies that are imposed and enforced by governments – and that even then, private sector action may sometimes fall short of its aims, necessitating government intervention. Digital pragmatism thus rejects the stark division often drawn between regulators and regulated. It demands that the private sector become more deeply involved in solving technology-related problems, but also requires the public sector to assume a sophisticated, multi-faceted role, both in supporting such solutions and intervening with legislation where necessary.

Digital pragmatism neither promises nor proposes specific solutions to discrete problems that arise online. Rather, it seeks to articulate a framework through which these problems are identified, defined and resolved. The underlying principles on which this model of digital pragmatism is based are set forth below.

A. Reliance on Market-Based Mechanisms

Perhaps the most salient feature of digital pragmatism is its use of *market-based mechanisms.* The term "market-based" as used here means mechanisms that exist within, are tied to, or in some sense mimic competitive markets and that display attributes often associated with such markets. These attributes include: (1) responsiveness to consumer demand; (2) plurality of choice; and (3) structural incentives towards efficiency. A classic example of such a market-based mechanism is self-regulation – that is, a regulatory mechanism designed and operated by non-governmental actors and with which the law does not mandate compliance.

The position set forth here is distinct from that of digital libertarianism in several respects. First, in digital pragmatism a market-based solution need not in fact originate from within the Internet community; it could equally originate from an entity that has relatively little connection to the Internet. Second, whereas digital libertarianism often seems to place regulatory power over the Internet in the majority, market-based mechanisms in the digital pragmatic model may also work to protect individual rights online *against* the views of the majority.[58] Finally, digital pragmatism rejects the core digital libertarian thesis that governmental efforts to regulate online activities are inherently undesirable. As discussed more fully below,[59] governments have a vital role to play in crafting the basic rules against which private-sector activity takes place and by intervening where non-legal options alone are inadequate. Indeed, in the latter context the specter of government intervention may provide an important incentive to encourage groups with divergent interests to compromise and come to consensus.

This approach also rejects the digital structuralist conviction that private-sector (and specifically commercial) involvement in addressing online problems poses a threat to civil liberties. One of the unique aspects of the Internet, at least as we know it today, is the extent to which it is a product of private-sector action. Although the Internet was initially a creation of the public sector, the private sector has played an enormously important role in contributing to its rapid development and maintaining what goes on there. It is therefore imperative that any model for resolving online legal issues includes a significant role for the private sector.

Self-regulation, of course, has been an important part of the commercial landscape for years, and this is certainly not the first article to advocate greater reliance on

---

[58] While digital libertarianism tacitly views consensus among affected online interests as the means to achieve legitimacy for self-regulation, digital pragmatism envisions this legitimacy emerging via the market, which may often be characterized by a plurality of options, none of which alone represents a consensus or even majority view.

[59] *See* Part III.C, *infra*.

market-based mechanisms to promote public policy goals.[60] Nevertheless, a stronger case exists for reliance on market-based mechanisms with respect to the Internet than in many other areas.

First, market-based solutions are often better suited than unilateral regulatory intervention to respond to rapid technological innovation and to quickly changing commercial practices. Innovation is a hallmark of the online environment, and change is the order of the day. As technologies evolve, so do the ways in which individuals and business use them and interact with one another. Formal governmental regulation often cannot adjust quickly to these changes. As a result, regulation inadvertently may curb innovation and check the development of more efficient commercial practices. In such circumstances, market-based initiatives are more likely to provide the flexibility needed to match the dynamic, international character of e-commerce: they often can be developed quickly, are typically flexible in nature, and are more easily susceptible to revision than traditional regulatory action.

The problem of online piracy nicely illustrates this point. Innovations in digital technologies have made it possible to express almost any two-dimensional work in digital form and to make perfect, inexpensive copies. In addition, the Internet has revolutionized distribution by enabling the dissemination of digital content to an international audience at virtually no cost. These technologies have also engendered a meteoric rise in piracy. Virtually every popular recording, software program and movie can be found on pirate Internet sites. In 1999, U.S. losses attributable to pirated copies of protected works – a growing portion of which are advertised or sold online – amounted to over $3 billion.[61] The reason for this profusion of illegal online content is straightforward. Because distribution costs are low and the avenues to evade detection many, online piracy is less risky and more profitable than traditional forms of piracy.[62]

---

[60] Nor is this article alone in advocating greater reliance on self-regulation for the Internet. *See, e.g.*, MEMOS TO THE PRESIDENT: MANAGEMENT ADVICE FROM THE NATION'S TOP CEOS 171 (Esther Dyson, ed., 2000).

[61] *See* INTERNATIONAL INTELLECTUAL PROPERTY ALLIANCE, COMMENTS OF THE INTERNATIONAL INTELLECTUAL PROPERTY ALLIANCE ON ISSUES RELATED TO THE POLICIES AND AGENDA FOR THE NIPLECC (July 7, 2000) at 9, *available at* http://www.iipa.com/html/NIPLECC_070700.pdf (last visited March 9, 2001).

[62] The Internet has generated a significant body of scholarship over where to draw the line between protected and unprotected uses of copyrighted works in the online environment. *Compare, e.g.*, Keith Aoki, *Foreward: Innovation and the Information Environment: Interrogating the Entrepreneur*, 75 OR. L. REV. 1 (1996); Peter A. Jaszi, *Goodbye to All That – A Reluctant (and Perhaps Premature) Adieu to a Constitutionally Grounded Discourse of Public Internet in Copyright Law*, 29 VAND. J. TRANSNAT'L. L. 595 (1996); *with* Gary W. Glisson, *A Practitioner's Defense of the White Paper*, 75 OR. L. REV. 277 (1996); Mark Stefik & Alex Silverman, *The Bit and the Pendulum: Balancing the Interests of Stakeholders in Digital Publishing*, 16 No. 1 COMPUTER LAW. 1 (1999). That issue, while important, is beyond the scope of this article. Instead, this article examines the less controversial issue of how best to address online acts that are clearly illegal under U.S. law.

Online piracy presents a substantial regulatory challenge. In an environment where the value of a work can be decimated by its free distribution to millions of potential customers, authors and performers will have less incentive to make their works available. If left unchecked, the result is likely to be lower-quality online content, which may in turn lead to diminished demand for Internet access, less incentive to invest in Internet infrastructure and a drop in legitimate online commerce. In addition, piracy effectively forces law-abiding users to "subsidize" piracy by paying higher prices for legitimate products.

The private sector has started to take significant strides in stemming the tide of online piracy through a combination of self-regulatory initiatives. For example, to stop illegal content at its source, the International Recording Media Association (IRMA) recently launched the world's first anti-piracy certification/compliance program for the manufacture of CDs, DVDs, and CD-ROMs. This broad industry effort is designed to help manufacturing plants establish procedures to reduce the production of pirated material on optical disks, many of which ultimately are advertised and sold online.[63] The International Federation of Phonographic Industries operates a similar self-regulatory mechanism, known as the Source Identification Code System—or SID Code System—for audio recordings.[64]

Building on this approach, representatives of the content and carriage communities recently extended this model to the context of online auctions. Recognizing that the U.S. copyright statutes, revised just two years earlier, failed to contemplate all the nuances arising in the auction arena,[65] the Business Software Alliance (BSA) proposed a new self-regulatory code of conduct for online auctions.[66] Representing major software publishers, BSA persuaded eBay, Amazon.com, and Yahoo to use the code as the basis for revising their practices for the auctions of software products – many of which, according to BSA's members, in fact had constituted counterfeits.[67]

This self-regulatory model for infringing content is now being considered in other areas of potential intermediary liability as well. An increasing number of intermediaries are coming to accept, in theory at least, limited responsibility for preventing third parties from using their systems to distribute illegal online content. Yet resolving this issue in practice requires striking a delicate balance between the protection of valuable online content and preserving the

---

[63] *See* INTERNATIONAL RECORDING MEDIA ASSOCIATION, IRMA ANTI-PIRACY COMPLIANCE PROGRAM, *available at* http://www.recordingmedia.org/antipiracyidx.html (last visited March 9, 2001).

[64] *See* INTERNATIONAL FEDERATION OF RECORDING INDUSTRIES, IFPI'S ANTI-PIRACY STRATEGY, *available at* http://www.ifpi.org/ (last visited March 9, 2001).

[65] *See generally* 17 U.S.C. §512 (2001).

[66] *See* BUSINESS SOFTWARE ALLIANCE, MODEL BUSINESS PRACTICES ON INTELLECTUAL PROPERTY RIGHTS FOR INTERNET AUCTION SITES, *at* http://www.bsa.org/resources/2000-12-12.32.pdf (last visited March 8, 2001).

[67] *See, e.g.*, David McGuire, *BSA Unveils Anti-Piracy Auction Guidelines*, NEWSBYTES (Dec. 13, 2000) (noting Amazon.com's decision to comply with BSA anti-piracy auction guidelines), *at* http://www.newsbytes.com/news/00/159364.html (last visited March 9, 2001).

free flow of online information, together with sensitivity to the wide range of different types of intermediaries and their respective functions and abilities in the online environment. A rule that imposed blanket liability on intermediaries for such third-party content might "chill" online expression by leading intermediaries to block even legal content in order to avoid liability. A rule that extended blanket immunity to intermediaries for illegal content, on the other hand, might remove *any* incentive for intermediaries to block that content, which might effectively prevent meaningful enforcement action against individuals who post such content online.

Here too, self-regulation provides an attractive alternative to reliance solely on legal rules and public-sector enforcement. Thus, copyright holders have successfully joined with Internet service providers (ISPs) to draft voluntary codes of conduct whereby these intermediaries agree to block access to illegal content offered by third parties over their systems, either upon notification or under other defined circumstances.[68] Such codes of conduct can be revised quickly to keep pace with changing business practices and technologies – as well as with the increasing sophistication of online pirates.

Market-based mechanisms are also well suited for the Internet because they can be constructed to accommodate divergent viewpoints, practices and business models. Many problems that arise online involve competing legitimate interests that stand in some tension with one another. But most legal restrictions are imposed unilaterally and applied uniformly, and almost by definition they require a single perspective on the "proper" balance between the competing interests involved. Accordingly, legal rules often have difficulty embracing plurality and thus – particularly with respect to highly contentious issues – may cause a significant segment of an affected community to feel that the balance has been struck poorly.

Market-based mechanisms, by contrast, can be constructed to provide a framework for balancing competing interests. Because these mechanisms can allow users to choose among various solutions based on their individual needs and interests, competing self-regulatory options can help avoid the problems of over- and under-breadth that can characterize one-dimensional government regulation. Indeed, by permitting two or more competing self-regulatory mechanisms to emerge, market-based mechanisms enhance the likelihood that optimal solutions will prevail through the expression of consumer choice, while fostering the development of real options that reflect the Internet's inherent diversity.

Efforts to address objectionable online content illustrate this point. Although the Internet has greatly expanded the avenues through which people can communicate and express themselves, it is frequently used to disseminate content – such as pornography and hate speech – that society finds offensive, often deeply so. And while governments have long had to balance rights to freedom of expression against social standards of morality in the offline world, this task has proven particularly delicate in the online environment. China and Singapore, for instance, at times have sought to control access to material deemed to be contrary to the public interest[69] by

---

[68] *See id.*

[69] Chinese law prohibits a broad range of online material, including material that encourages "resistance to the enforcement of laws and regulations," promotes "subversion of state power," or that "fabricates (continued…)

requiring that all Internet traffic in the country be routed through government-controlled servers, known more generically as "proxy" servers.[70] Such proxy servers are designed to enable state officials to monitor Internet traffic within the country and thereby to control access by citizens to content that the government deems objectionable.[71] Although restrictive regimes such as those in China and Singapore have come under frequent attack,[72] even countries with less restrictive approaches to online content have used technology to control access to certain classes of objectionable content.[73]

In the United States, Congress has repeatedly tried to solve the problem of objectionable online content – and specifically access by children to online pornography – through legislation. In at least two instances, however, courts struck down parts of that legislation on the ground that it intruded too deeply into the First Amendment rights of adults. The first occasion was in 1997, when the U.S. Supreme Court invalidated provisions of the 1996 Communications Decency Act (CDA) that prohibited use of an interactive computer service knowingly to transmit, send, or display any indecent or obscene material to minors.[74] Congress responded with the 1998 Child Online Protection Act (COPA), which imposed restrictions on content that is "harmful to minors."[75] Although proponents hoped that the legislation avoided

---

stories, distorts facts, spreads rumors or disturbs the public order." *See* David A. Laverty, *E-Commerce Regulation and Compliance in Asia*, 5 E-COMMERCE L. REP. 7 (March 2000) at 8. Singapore prohibits material "that is objectionable on the grounds of public interest, public morality, public order, public security, [or] national harmony." *See* SINGAPORE BROADCASTING AUTHORITY, INTERNET CODE OF PRACTICE para. 4(1) (1997); SINGAPORE BROADCASTING AUTHORITY, INDUSTRY GUIDELINES ON THE SINGAPORE BROADCASTING AUTHORITY'S INTERNET POLICY paras. 9, 10 (1997).

[70] *See, e.g.*, ELECTRONIC PRIVACY INFORMATION CENTER, PRIVACY AND HUMAN RIGHTS 1999: CHINA (1999) (discussing Chinese regulations requiring use of proxy servers) [*hereinafter* ELECTRONIC PRIVACY INFORMATION CENTER]; Laverty, *supra* note 69, at 8. More recently, Chinese authorities further restricted Internet content by banning any discussion of "state secret information." *See id.* For Singapore's enforcement controls, *see id*. at 9; *see also* SINGAPORE BROADCASTING AUTHORITY, INDUSTRY GUIDELINES, *supra* note 69, paras. 7, 9.

[71] Whether proxy servers used in this manner are in fact effective in helping governments control Internet traffic has been widely questioned. *See, e.g.*, GLOBAL INTERNET LIBERTY CAMPAIGN, REGARDLESS OF FRONTIERS: PROTECTING THE HUMAN RIGHT TO FREEDOM OF EXPRESSION ON THE GLOBAL INTERNET Part C (1999) (noting that proxy servers used by governments to censor online content can be easily evaded), *available at* http://www.gilc.org/speech/report/ (last visited March 9, 2001).

[72] *See, e.g.*, ELECTRONIC PRIVACY INFORMATION CENTER, *supra* note 70; GLOBAL INTERNET LIBERTY CAMPAIGN, *supra* note 71.

[73] Australia, for instance, requires that material that is deemed suitable only for adults be channeled through Internet "gateways" that prevent access by minors. *See* AUSTRALIAN BROADCASTING SERVICES AMENDMENT (ONLINE SERVICES) ACT 1999, No. 90, Part 1, Sec. 4 (1999), available at http://scaleplus.law.gov.au/html/comact/10/6005/top.htm (last visited March 9, 2001). *See also* Stewart Taggart, *The Aussies Went and Done It*, WIRED NEWS, January18, 2000.

[74] *See Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997).

[75] *See* 47 U.S.C. §231 (2001).

the First Amendment deficiencies of the CDA, a federal district court has stayed implementation of certain key provisions of COPA on First Amendment grounds pending trial on its constitutionality.[76]

Measures such as the CDA and COPA have revealed deep-seated disagreements over the legitimacy of state efforts to regulate online content. Critics point to the sanctity of the right to freedom of expression, recognized in legal instruments around the world as a fundamental, inalienable right of every individual.[77] These critics also note that perceptions of what constitutes acceptable expression vary widely, not only between countries and cultures but also among individuals, and that it is all too common for laws justified to "protect" citizens from objectionable content to be used to suppress minority political, religious, ethnic, or cultural views as well.[78] Supporters of content restrictions, on the other hand, counter that an unregulated Internet would permit unfettered access to material that many people find unacceptable, including material that is widely condemned as illegal. When concern for the protection of children is added to this mix, the divergence of views can be even more difficult to surmount.

Yet even while governments around the world have struggled to find a solution to objectionable online content, the private sector has devised a variety of self-regulatory responses, all of which help to block access by minors to such content while respecting the First Amendment rights of adults. One such market-based solution is the adult verification service, of which many competing varieties exist.[79] Adult verification services effectively act as a gateway to online sexually explicit content. These subscription-based services make access to such content contingent on possession of a credit card, which is considered proof that the subscriber is legally an adult. By funneling users through such gateways, website operators that offer sexually explicit material can help ensure that this material does not reach minors or others who might find it offensive.[80] Another popular market-based initiative is self-rating by websites. Web sites operators voluntarily rate their sites based on certain standardized criteria. Users can then set

---

[76] *See American Civil Liberties Union v. Reno*, 31 F. Supp. 2d 473 (E.D. Pa. 1999), *aff'd*, 217 F.3d. 162 (3d Cir. 2000), *cert. granted*, 121 S.Ct. 1997 (May 21, 2001).

[77] *See generally* GLOBAL INTERNET LIBERTY CAMPAIGN, *supra* note 71.

[78] For instance, human rights observers have condemned online content bans in Burma on the ground that they include material that the Burmese authorities consider "detrimental" to government policies. *See* James Miles, *Burma Clamps Down on Web*, *BBC NEWS*, January 20, 2000. For an overview of governmental efforts to ban political or religious speech on the Internet, see GLOBAL INTERNET LIBERTY CAMPAIGN, *supra* note 77 (discussing state efforts to suppress dissident online speech); *see also* HUMAN RIGHTS WATCH, THE INTERNET IN THE MIDEAST AND NORTH AFRICA: FREE EXPRESSION AND CENSORSHIP (July, 1999) (detailing efforts by states in Middle East and North Africa to suppress dissident online speech).

[79] A recent web search identified 33 adult verification websites. *See* Yahoo, *Age Verification*, *at* http://dir.yahoo.com (last visited March 9, 2001).

[80] One service, AdultCheck, claims that it provides access to over 100,000 Internet sites. *See* ADULT CHECK, THE ADULT CHECK SYSTEM, *at* http://www.adultcheck.com/ (last visited March 9, 2001).

their browsers to locate and download only those sites whose ratings are consistent with the user's preferences.[81]

Self-regulation has also played a key role in the area of online privacy.[82] Policymakers have long struggled with how best to protect personal data in an age of computerization. A major milestone was reached in 1980 when the Organization for Economic Cooperation and Development (OECD) issued its *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*,[83] which engendered a truly international dialogue on the importance of data privacy that has produced remarkably broad consensus over basic privacy principles.[84]

Despite this consensus, efforts to implement these principles into practice have revealed divergent views on the proper roles of public and private actors. One such view – which might be called the *interventionist* approach – relies on relatively detailed legal rules enforced by public-sector bodies and relies only secondarily on self-regulation. To a significant extent, European Union law reflects such an interventionist approach.[85] The interventionist

---

[81] One of the more popular Internet rating systems in the United States is RSACi. RSACi was established in 1996 under the aegis of the Recreational Software Advisory Council and is now maintained by the Internet Content Rating Alliance, founded in 1999 to develop internationally acceptable online content labels. RSACi rates content in four categories: sex, nudity, language, and violence. *See generally* INTERNET CONTENT RATING ASSOCIATION, PRESS, ADDITIONAL INFORMATION, ICRA AT A GLANCE, ICRA(RSAC) TIMELINE, *at* http://www.icra.org/ (last visited September 27, 2001).

[82] The right to privacy is recognized as fundamental in most legal systems. *See* ELECTRONIC PRIVACY INFORMATION CENTER, *supra* note 70, Exec. Summ. (noting that "nearly every country in the world recognizes privacy as a fundamental human right in their [sic] constitution"). Privacy is equally well recognized as a fundamental human right in international law. *See International Covenant on Civil and Political Rights*, U.N. High Commission for Human Rights, Art. 17, opened for signature December 16, 1966, *available at* http://www.unhchr.ch/html/menu3/b/a_ccpr.htm (last visited March 13, 2001); *Convention for the Protection of Human Rights and Fundamental Freedoms*, Council of Europe, Art. 8, ETS 005, as amended by Protocol No. 11, ETS 155 (1994) *available at* http://conventions.coe.int/treaty/EN/Treaties/html/005.htm (last visited March 13, 2001).

[83] *See* OECD, GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (1980).

[84] These principles are often summarized as notice, choice, access and security. *See, e.g.*, FEDERAL TRADE COMMISSION, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE iii (2000) (articulating principles of notice, choice, access and security).

[85] *See Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 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 [*hereinafter Framework Directive*], *available at* http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html (last visited March 9, 2001); *Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector*, 1998 O.J. (L 24) 1 [*hereinafter Telecoms Privacy Directive*], *available at* http://europa.eu.int/eur-lex/en/lif/dat/1997/en_397L0066.html (last visited March 9, 2001).

approach has its strengths, but it has also been criticized as failing to accommodate divergent views and business practices and for leading to inefficient over-regulation of the market. Critics have also charged that this approach may raise barriers to international online trade.[86]

The *market-based* approach, by contrast, rests on the premise that private-sector mechanisms may be more responsive to consumers' privacy concerns than detailed legal rules, particularly within an environment of ongoing technological change. This approach typically places primary reliance on industry self-regulation, buttressed in some instances through sector-specific legislation. This market-based approach is most often associated with Australia, Japan, and the United States, though other nations have also begun to experiment with industry self-regulation in respect to online privacy.[87]

The United States has experienced a flurry of self-regulatory efforts in the online privacy area. One such initiative is TRUSTe, which permits companies to display the TRUSTe seal on their websites if they adhere to the organization's privacy principles and subscribe to an alternative dispute resolution process.[88] BBBOnline is another, competing voluntary trustmark program that works to establish and enforce privacy principles online.[89] Many other initiatives exist as well.[90] Many firms adhere to one or another of these programs, others adhere to more industry-specific programs, while some firms (though increasingly few) simply publish their own privacy policies, which may be stronger or looser than the policies of these other organizations.

In the off-line world, this array of self-regulatory mechanisms might well prove unworkable. Retailers might find it overly burdensome to monitor changes in the various self-regulatory options, while consumers might balk at having to travel from retailer to retailer to compare competing policies. In other words, off-line self-regulatory mechanisms arguably would not compete in any meaningful sense because practical obstacles would prevent the emergence of anything resembling a competitive market. The Internet, however, makes it possible for consumers to compare competing self-regulatory mechanisms with little effort and

---

[86] *See, e.g.*, Ernest T. Patrikis & Stephanie Heller, *The Government's Role in Electronic Commerce: A Review of the Clinton Administration's Framework on Global Electronic Commerce*, 18 ANN. REV. BANKING L. 325, 361 (1999) ("Given the differing treatment of privacy in the United States and the EU, there is considerable concern that the EU will use the Privacy Directive as a non-tariff trade barrier."); *cf*. P. Amy Monahan, *Deconstructing Information Walls: The Impact of the European Data Directive on U.S. Businesses*, 29 LAW & POL'Y INT'L BUS. 275, 287-93 (1998) (discussing claims that EU Directive may constitute impermissible barrier to international trade).

[87] *See* ELECTRONIC PRIVACY INFORMATION CENTER, *supra* note 70 (country reports for Australia, Japan and the United States).

[88] *See* TRUSTE, THE TRUSTE STORY, *at* http://www.truste.com/about/truste/about_wp.html (last visited March 9, 2001).

[89] *See* BETTER BUSINESS BUREAU, BBBONLINE PRIVACY PROGRAM, *at* http://www.bbbonline.com/privacy/index.asp (last visited March 9, 2001).

[90] *See, e.g.*, the discussion of the Platform for Privacy Preferences Project (P3P) at text accompanying notes 109 through 112, *infra.*

to determine quickly the costs and benefits of each. Thus, they can comparison shop among such mechanisms with a few clicks of their mouse, and thereby determine relatively easily which privacy policy best suits their needs.[91]

Of course, in some cases self-regulatory strategies will be appropriate even where society *does not* want to accommodate – or at least encourage – divergent viewpoints. For example, most societies ban child pornography, and many regulate particularly virulent forms of hate speech. Self-regulatory entities like the Anti Child Porn Organization combat online child pornography by tracking child pornographers and people who use the Internet to lure children,[92] while the non-profit organization HateWatch monitors online hate groups and websites containing hate speech.[93] These mechanisms are obviously not designed to respond to differing tastes regarding hate speech and child pornography, but rather to augment legal prohibitions and to help people avoid speech that is highly offensive to the vast majority of Internet users.

In many quarters, market-based mechanisms may be perceived as more legitimate than traditional legal rules acting in isolation. As digital libertarians have argued, Internet users may be inclined to view the application of law to the Internet as an illegitimate intrusion into cyberspace.[94] Such perceptions may complicate the enforcement of laws online. Market-based mechanisms, however, typically depend for their success on user acceptance and often provide a framework that can better accommodate divergent views. Thus, where practicable, self-regulation is more likely to be perceived as legitimate by many Internet users than rules imposed by the state.

Finally, market-based mechanisms are typically more responsive to changing business needs and practices than legal rules. Electronic commerce holds perhaps the world's greatest hope for continuing the exceptional productivity gains and real economic growth that have characterized much of the past decade. Market competition will drive the private sector to exploit online efficiencies and thereby increase productivity. By contrast, legal rules that are inconsistent with online commercial needs or prohibit efficient e-commerce business practices will make it difficult if not impossible for the global economy to continue its current rate of

---

[91] Recent research suggests that web sites located in countries that pursue a market-based approach to online privacy may provide greater safeguards than sites located in countries that follow a more interventionist approach. *See, e.g.*, CONSUMERS INTERNATIONAL, PRIVACY@NET: AN INTERNATIONAL COMPARATIVE STUDY OF CONSUMER PRIVACY ON THE INTERNET 6 (2001) ("Despite tight EU legislation in this [the data privacy] area, researchers did not find that sites based in the EU gave better information or a higher degree of choice to their users than sites based in the U.S. Indeed, U.S.-based sites tended to set the standard for decent privacy policies."), available at http://www.consumersinternational.org/news/pressreleases/fprivreport.pdf (last visited on March 9, 2001).

[92] *See* ANTI CHILD PORN ORGANIZATION , *at* http://www.antichildporn.org (last visited October 8, 2001).

[93] *See* HATEWATCH, *at* http://hatewatch.org (last visited September 20, 2001).

[94] *See, e.g.*, Johnson & Post, *supra* note 36, at 1394-95.

growth. Everyone will lose if online regulation does not take a form that is responsive and adaptive to the nature of the Internet itself.

B. Technology Solutions to Technology Problems

A second key element of digital pragmatism is its focus on technology. As discussed in Part II, technology plays an integral yet complex role in many of the social and legal challenges that arise online. On the one hand, bad actors often manipulate otherwise beneficial Internet technologies to commit harmful acts online. At the same time, new technology tools are constantly being developed that help people avoid falling victim to such acts and to prevent such acts from occurring in the first place.

The policymaking approach advanced here contends that any comprehensive, viable regulatory response to the problems that arise on the Internet must both acknowledge and harness this dual aspect of online technologies – that is, although technologies often are a contributing cause of online challenges, they also are a potential source of solutions to those challenges. Recognition of this fact arguably places this approach at odds with the more one-dimensional views of technology and its relationship to regulation advanced by digital libertarianism and digital structuralism. As noted above, digital libertarianism proceeds from the assumption that the Internet is inherently immune to control from "outside" sources such as law.[95] Because legal efforts to regulate cyberspace may be implemented through technology-based mechanisms, digital libertarianism suggests that technology holds little hope of modifying online behavior.[96] Thus, digital libertarianism seems to perceive technology as a relatively powerless mechanism of control and consequently takes a skeptical view of efforts to regulate online activity through technology.[97]

Digital structuralism, by contrast, views Internet technologies as extremely important instruments of online control.[98] Although digital structuralism recognizes that Internet technologies themselves are effectively neutral – in the sense that they can operate either to promote or inhibit online freedom[99] – it frequently characterizes these technologies as both

---

[95] *See* text accompanying notes 35 through 39 and notes 49 through 51, *supra*.

[96] *See* text accompanying notes 38 through 39, *supra*.

[97] *See, e.g.*, Johnson & Post, *supra* note 36, at 1373-74 ("[S]ome authorities strive to inject their boundaries into [the Internet] through filtering mechanisms and the establishment of electronic barriers. . . . But such protective schemes will likely fail . . ."). *Cf*. Boyle, *supra* note 41, at 178-79 (characterizing digital libertarian view of the Internet as largely immune from outside control).

[98] *See* text accompanying notes 41 through 46, *supra*. As Lawrence Lessig has written, "In cyberspace we must understand how code regulates—how the software and hardware that make cyberspace what it is *regulate* cyberspace as it is. As William Mitchell puts it, code is cyberspace's 'law.'" LESSIG, *supra* note 39, at 6 (quoting WILLIAM J. MITCHELL, CITY OF BITS: SPACE, PLACE, AND THE INFOBAHN 111 (1995)).

[99] *See, e.g.*, LESSIG, *supra* note 39, at 6 (noting that the technologies that comprise the Internet "present[] the greatest threat to liberal or libertarian ideals, as well as their greatest promise").

monolithic and omnipotent – either they promote control, or they promote liberty, but in either case they do what they do very effectively. Indeed, it is this conception of technology as potentially omnipotent that arguably underlies digital structuralism's core concern – namely, that commerce, in collusion with the executive and legislative branches of government, will promote technologies that allow for nearly perfect control of online behavior.[100]

In fact, however, online technologies are seldom either all-powerful or powerless. In most cases, online behavior yields a much more complex picture of Internet technologies – both in the extent to which they underlie online problems and in the degree to which they help solve them. The close connection between online technologies and online behavior, however, strongly suggests that any regulatory response to online legal problems *must* view technology not merely as part of the problem, but also as part of the solution. In addition, there are good practical reasons why policymaking for the Internet should place greater reliance on technical solutions to Internet-related problems.

First, technology solutions developed by the private sector – like self-regulatory solutions more generally – can respond more nimbly than legislation to changing technologies and evolving online business and social practices. The rapid pace of innovation and change on the Internet makes it difficult for legal rules alone to respond quickly enough to online challenges. Market-driven technology solutions can be developed and implemented in far less time than it takes to draft, debate, approve, and implement legislation. And like self-regulatory mechanisms more generally, technology solutions can be revised or amended more easily than legislation to changed circumstances.

Second, technology solutions utilize private-sector expertise and resources more effectively than traditional lawmaking. Fierce competition between Internet technology firms has created a deeply embedded culture among technologists that places a premium on rapidly analyzing and solving problems. This resource goes largely untapped when problems are addressed through traditional regulation. Technology solutions exploit this expertise and thereby harness private-sector resources to achieve public policy goals.

Third, technology solutions – again like market-based solutions more generally – are better suited than legal intervention to accommodate diverse social, commercial, and cultural needs. Legal rules typically enforce a single, uniform solution that glosses over individual differences and leaves consumers largely powerless to opt for more (or less) stringent alternatives. Technology solutions, by contrast, usually include features that respond to these differences and are thus less likely to leave large sections of the Internet community feeling unrepresented. Moreover, the development of one technology solution, particularly if it seems promising, often prompts the development of additional competing technologies which, taken together, provide choices that better reflect the diverse interests and expectations of the online community.

---

[100] *Id*. at 6 ("The invisible hand, through commerce, is constructing an architecture that perfects control—an architecture that makes possible highly efficient regulation. . .)

The private sector has already developed a range of technology solutions to address online legal problems and further specific social goals. In the area of online content, for example, "digital rights management" (DRM) tools have been developed to help authors and other copyright holders maintain the integrity of their works even as they are sold and distributed over the Internet.[101] Besides helping to protect online content against piracy, DRM technologies open up a whole new range of ways in which content providers can offer their works to consumers. Because each individual work in a compilation can be assigned a unique identifier, online music sites can offer individual tracks from an album instead of requiring consumers to purchase the entire CD, while publishers can offer a single story or article rather than having to sell the entire publication in which it appears.

As with market-based solutions more generally, however, technology solutions are often effective only within the context of broader self-regulatory efforts or regulatory frameworks. A good illustration of this is the Platform for Internet Content Selection, or "PICS." PICS was designed by the non-profit World Wide Web Consortium as a tool to help parents prevent exposing their children to objectionable Internet content.[102] PICS is not itself a rating system, but rather a template that facilitates standardization and interoperability between multiple rating systems and browsers. By establishing a basic vocabulary and allowing ratings organizations to provide further specifications, PICS can accommodate different cultural and legal approaches to objectionable content while creating an internationally consistent terminology, thereby making it easier for users and website operators to understand the ratings.[103] A single website can carry a number of different ratings based on self-regulatory standards developed by different organizations so long as they employ the basic PICS vocabulary and categories. A user can decide which ratings system to consult, set the browser accordingly, and access content that passes whatever test that rating system imposes.[104] PICS thereby gives users control over the types of online material they or their children can view, while leaving others free to view whatever content they wish.

Another area in which technology solutions have proven effective at addressing technology-based problems is in the area of online privacy. In many respects, the technologies that comprise the Internet function like a vast database that users can customize to their own needs through search engines, database programs, and other software tools. Under certain

---

[101] IBM and Microsoft are only two examples of companies that have developed media rights management systems for digital online content. *See, e.g.*, IBM CORPORATION, IBM ELECTRONIC MEDIA MANAGEMENT SYSTEM (discussing IBM's DRM technology and providing links), *available at* http://www-4.ibm.com/software/is/emms/ (last visited January 23, 2001); MICROSOFT CORPORATION, WINDOWS MEDIA RIGHTS MANAGER 7 (January 17, 2001) (discussing DRM systems built into Microsoft media technologies), *available at* http://www.microsoft.com/windows/windowsmedia/en/wm7/drm.asp (last visited January 23, 2001).

[102] *See generally* WORLD WIDE WEB CONSORTIUM, PICS FREQUENTLY ASKED QUESTIONS (April 4, 2000), at http://www.w3.org/2000/03/PICS-FAQ/ (last visited March 9, 2001).

[103] *Id*.

[104] *Id*. Another widely used Internet rating systems is RSACi. *See* note 81, *supra*.

conditions, however, these technologies can be configured to collect personal data that most people would normally consider private.[105] Software tools that utilize chatter,[106] cookies,[107] click-stream monitoring and online profiling[108] – all of which are often used benignly to collect purely non-personal data (but which enables web sites to customize online content and operate more efficiently) – may also be configured to collect personal, private data and to disseminate that information to third parties, even without a user's knowledge or consent.

As in other areas, these "misuses" of online technologies can be and are being addressed at least in part by technology itself. One example is the Platform for Privacy Preferences (P3P) Project, developed by the non-profit World Wide Web Consortium.[109] P3P software enables users to record their privacy preferences within an Internet browser and to authorize the browser to communicate with a website about its privacy practices.[110] The browser then releases personal data about the user only where the site's practices are consistent with the user's privacy preferences; if the site's practices are inconsistent with those preferences, no personal data will be transferred unless the user expressly chooses to do so.[111] Recent versions of some popular browsers give users almost complete control over the types of data that web sites may collect from them and how that data should be handled.[112]

---

[105] "Personal" data in this context refers to data that can be used to identify a specific individual. "Non-personal" data may match a specific machine to a unique IP address, but does not take the further step of matching that data to an identifiable individual.

[106] "Chatter" is the automated exchange of technical data between a user's computer (the "client") and other computers (the "hosts") through which the user accesses specific websites. Hosts may use chatter to obtain the client's Internet address and information relating to the technical capabilities of the client's browser. Website operators can also use chatter to trace individual clients over multiple sites.

[107] A "cookie" is a simple text file sent by a host to a client that may contain a unique identifier. Whenever the client accesses the same host, the host will "see" the cookie and realize that this client has visited before. Cookies can be used to tailor a website to a specific user's preferences, for example by providing weather forecasts for any location chosen by the user. Cookies may also be used to track clients across multiple websites, and may be configured to include personally identifying information.

[108] "Click-stream monitoring" effectively records the path a client's machine takes through a particular website. Hosts can use this data to generate an "online profile" that identifies patterns in the client's online activities. By combining this data with personal information provided by the user through an online transaction or registration process, a company can attach the profile to an identifiable person.

[109] *See generally* WORLD WIDE WEB CONSORTIUM, PLATFORM FOR PRIVACY PREFERENCES (P3P) PROJECT, *at* http://www.w3.org/P3P/ (last visited March 9, 2001).

[110] *Id.*

[111] *Id.*

[112] *See, e.g.*, MICROSOFT CORPORATION, MICROSOFT ANNOUNCES NEW COOKIE MANAGEMENT FEATURES FOR INTERNET EXPLORER 5.5 (July 20, 2000), at http://www.microsoft.com/PressPass/press/2000/Jul00/IECookiePR.asp (last visited March 9, 2001).

Finally, it bears mentioning that, to be truly effective, technology solutions typically must qualify as a "market-based" solution in the sense discussed above – that is, they must be responsive to consumer demand and exist within or at least mimic a competitive market. Unilateral government efforts to impose specific technology solutions onto the Internet usually do not share these qualities. Such efforts typically do not adapt well to innovation and change, and they often cannot accommodate diverse views and evolving business and social practices.

The U.S. Government's experience with encryption regulation provides a relevant case study. Modern encryption technologies offer an effective means for parties to encode their online messages and to ensure that these messages are read only by the intended recipient.[113] Yet for decades, the U.S. Government had a policy of strictly controlling the export of products with encryption functionality. These restrictions were in significant part an outgrowth of the Cold-War fear that, because encryption had important military and espionage applications, it should be classified and regulated as a civilian and military "dual-use" good, not unlike many nuclear technologies. By the early 1990s, however, the U.S. Administration came to recognize that encryption had important commercial applications and that U.S. companies were anxious to include encryption functionality in their exportable products.

Rather than simply open these technologies to the world market, however, the U.S. Government threw its legal and policy weight behind a specific technology dubbed the "Clipper Chip." Its reason for doing so had little to do with protecting users' online security. Instead, the "advantage" of the Clipper Chip, from the Administration's perspective, was that it would enable U.S. national security agencies to decipher any message encoded using the Clipper Chip technology – thereby, at least in theory, promoting U.S. national security concerns.[114] Users roundly rejected the Clipper chip technology and voiced increasing disagreement with the country's export policy, but the U.S. Government nonetheless maintained its stringent export restrictions on the theory that these controls would limit the ability of foreign terrorists and hostile nations to obtain strong encryption.

This effort was arguably misguided from the start because it sought to impose a technology on the market, rather than allowing the best technology to emerge through market competition responding to consumer demand. Ironically, the U.S. policy did more to harm than further national security interests because it led foreign consumers to rely increasingly on non-U.S. encryption, with which U.S. security agencies were less familiar. Not surprisingly, the U.S.

---

[113] For a detailed discussion of encryption technologies and regulatory responses to encryption products, see Smith, *supra* note *, at 343-48.

[114] The Clipper Chip was based on—for the time—relatively strong encryption, but it included a so-called "back door" that made it possible for U.S. authorities with the appropriate authorization and software to break the cryptographic protection it provided. *See, e.g.*, David B. Walker, *Privacy in the Digital Age: Encryption Policy – A Call for Congressional Action*, 1999 STAN. TECH. L. REV. 3, 30-32, *at* http://stlr.stanford.edu/STLR/Articles/99_STLR_3/index.htm (discussing history of the Clipper Chip).

began a gradual retreat from its restrictive policy soon after the failure of the Clipper chip.[115] The most recently adopted U.S. export regulations liberalize licensing requirements for a broad range of encryption products and permit exports to all but a handful of nations and market segments.[116]

Thus, just as legal and policy challenges on the Internet often have their genesis in technology, so too does technology often offer real and effective solutions to these problems. Any regulatory policy for the Internet that does not include technology solutions is bound to stifle online growth and face hurdles to acceptance by the community of online users.

C. The Role of Government

The preceding discussion of digital pragmatism emphasized the private-sector's role in addressing online problems through self-regulatory mechanisms and technology-based solutions. Against the background of this discussion, one may begin to wonder about the implications of digital pragmatism for government. If the private sector is to assume a more proactive role in helping to address online legal and social challenges, one might conclude that the public sector will thereby be relegated to a lesser, supporting role. But this is not what digital pragmatism in fact envisions.

Far from placing government on the margins, digital pragmatism requires that governments assume new responsibilities that in many ways are more complex and sophisticated than those they have assumed in the past. Although digital pragmatism demands deeper involvement by the private sector in addressing online challenges, the response of the public sector is often decisive in the success of these private-sector efforts. Part of government's responsibility is to facilitate private-sector initiatives and to support solutions based on them. In addition, public officials must continue to play a critical role as lawmakers – both in developing and enforcing the ground rules in accordance with which these private-sector initiatives operate, and in actively intervening with regulatory measures where extra-legal responses to online problems prove to be inadequate.

1. Public Actors as Facilitators

Digital pragmatism envisions public officials working more proactively than in the past to encourage private-sector constituencies to develop non-regulatory alternatives to online problems. This role entails three distinct aspects. First, public officials should join forces with affected private-sector interests to identify potential problems and to develop principles to guide their resolution. Public officials bring to the table capabilities in this regard that the private sector cannot match. Perhaps most obviously, governments represent the public interest. If private-sector solutions are to garner broad support, these solutions must reflect the interests of

---

[115] For an excellent survey of recent U.S. encryption export restrictions, see Ira S. Rubinstein & Michael Hintze, *Export Controls on Encryption Software*, 812 PRAC. L. INST. / COMM. 505 (2000).

[116] *See* Revisions to Encryption Items, 65 Fed. Reg. 62600 (Dept. of Commerce Oct. 19, 2000).

not only those involved in designing them, but also those who will be affected by them. Public officials are not only in the best position to articulate and represent the public interest and to ensure that there is broad-based input into the problem-solving process – in our democratic system they are constitutionally empowered to play precisely this role.

The integration of "cookie control" features into Microsoft's Internet Explorer (IE) 5.5 illustrates the type of proactive role governments can play.[117] Consumer concerns about online privacy have prompted Microsoft to make privacy a priority from both a technical and policy standpoint.[118] In an effort to make its products more responsive to these concerns, Microsoft worked closely with the National Association of Attorneys General and a number of privacy advocacy groups to learn more about specific consumer concerns and to examine possible solutions. The result of this collaboration was a set of new features in IE that gives users a clearer understanding of the different types of cookies that exist and where they originate, as well as easier ways to manage and delete cookies.[119] The public officials who worked with Microsoft were able to help manage the effort toward a solution by articulating the public concerns at issue, by specifying the types of solutions that might address these concerns, and by encouraging the company to move forward.

Second, public officials should work to encourage the diverse private-sector constituencies implicated in any given issue to cooperate in crafting workable solutions. Particularly on highly contentious issues, or on matters affecting groups that have not previously worked together, public officials are likely to be in a strong position to prompt the various parties involved to find common ground. Diverse private-sector groups may need a neutral, "outside" party to encourage them to set aside their differences and focus on common interests. Pubic officials can often provide that neutrality, as well as the problem-solving, negotiating, and even diplomatic skills that are often needed in this effort. And where diverse private-sector constituencies seem at an inescapable impasse, the threat of legislative or regulatory intervention (or litigation, for that matter) by public officials may help focus minds and soften positions in ways that foster responsive – and responsible – action.

The final aspect of government's role as facilitator asks that public officials support viable private-sector solutions and provide an environment in which they are given a reasonable opportunity to succeed. Governments are uniquely positioned to help private-sector solutions succeed by eliminating regulatory obstacles and by helping to explain the solution to the public. Many market-based and technology-based mechanisms require the beneficiaries of these efforts to be more proactive than is typically necessary in the case of traditional

---

[117] *See generally* MICROSOFT CORPORATION, MICROSOFT ANNOUNCES NEW COOKIE MANAGEMENT FEATURES FOR INTERNET EXPLORER 5.5 (July 20, 2000), at http://www.microsoft.com/PressPass/press/2000/Jul00/IECookiePR.asp (last visited March 9, 2001). For a brief description of cookies and their role in online communications, see note 107, *supra.*

[118] *Id.*

[119] *Id.*

"command-and-control" legal regimes. Governments can help spread the benefits of such mechanisms broadly by educating consumers about them and advocating their use.

2. Public Actors as Lawmakers and Law Enforcers

Even as governments assume a role as facilitators within the Internet environment, digital pragmatism recognizes that they must also retain their unique function as lawmakers and law enforcers. Law will remain an indispensable element of any viable, comprehensive response to the various social and legal problems that can arise online. Some of the tasks of law in this new policymaking approach will be familiar from the off-line world, while others reflect the unique characteristics of the types of problems that arise online.

First, laws will continue to define the background set of rules within which private-sector actors and mechanisms must operate. Although digital pragmatism emphasizes the need for private-sector actors to be involved in solving online problems, these solutions will be effective only within a broader framework of legal rules to which all parties must abide. The significance of this underlying set of legal rules for private-sector agreements has been forcefully articulated by scholars such as Margaret Jane Radin.[120] Radin criticizes the digital libertarian claim that private-sector responses to online problems can operate without any involvement by governments or laws: "Insofar as the advocates of private ordering [*e.g.*, digital libertarians] are thinking of regimes of customary norms with no enforcement and policing mechanisms other than people's continuing commitment to them, they are thinking of anarchy, not law."[121] Radin's observation seems valid. To be effective, any private-sector effort to regulate online behavior ultimately must rely on the threat of government sanction against violations of the rules that define the parameters of legitimate private-sector action. This fact has long been recognized with respect to off-line activities, and it applies with no less force to the online world.

Laws will also often be needed for the more specific task of making particular technology solutions effective. A straightforward example of this is electronic signatures. Electronic signature technologies help users authenticate the identity of other online parties and to verify the integrity of messages from those parties.[122] Even in the absence of laws recognizing

---

[120] *See, e.g.*, Radin & Wagner, *supra* note 34, at 1295-98; *see also id*. at 1295-96 ("Contrary to laissez-faire ideology, the 'private' legal regimes of property and contract presuppose a 'public' regime of enforcement and policing, a baseline of background rights. . . . [P]roperty and contact presuppose limits and enforcement shaped by a sovereign authority.").

[121] *Id*. at 1296. For a general discussion of extra-legal norms as regulators and the circumstances in which such norms are likely to be effective, see ROBERT C. ELLICKSON, ORDER WITHOUT LAW: HOW NEIGHBORS SETTLE DISPUTES (1991).

[122] The term "electronic signature" is often used broadly to denote any electronic data used to identify a party. *See, e.g.*, Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures, Art. 2(1), 2000 O.J. (L 13) 20 (defining electronic signature as "data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication"); *see also* DRAFT UNIFORM RULES ON ELECTRONIC SIGNATURES, U.N. COMM'N ON INT'L TRADE LAW, 36th Sess., Art. 2, U.N. Doc. A/CN9/WG.IV/WP.84.

their legal validity, electronic signatures can help online parties identify each other and ensure that their online messages have not been compromised. But to make online contracts as solid as their offline counterparts, electronic signatures require a legal framework that expressly recognizes their validity as a mechanism for satisfying the formality of "signing" a contract.[123] Laws that fail to extend legal recognition to electronic signatures – or that extend legal recognition only to specific types of electronic signature technologies – impede the development of online commerce by making it more difficult for parties to contract online than off-line.[124]

Laws can also provide incentives to positive private-sector action by extending certain legal benefits to such action. So-called "safe harbors," which can be found in various areas of the law, can perform precisely this function. Legal safe harbors are useful in the online context because they can encourage private actors to abide by industry best practices and standards and to pursue broader public policy goals. This not only benefits users, but also gives the private sector a stronger incentive to devise self-regulatory mechanisms that work.

An example of such a legal safe harbor can be found in the 1998 Child Online Protect Act (COPA). As noted above, early Congressional efforts to deal with online pornography were struck down by the courts on First Amendment grounds.[125] Although certain provisions of the COPA have been invalidated on similar grounds, a separate provision of the COPA has so far withstood scrutiny. That COPA provision seeks to tackle the issue of online pornography by enlisting the assistance of online intermediaries, but by means of a carrot instead of a stick. The legislation provides, in essence, that online intermediaries who act in good faith to prevent access to material that is "harmful to minors" as defined under the Act will generally be immune from liability.[126]

Finally, legal intervention will at times be necessary to accomplish what the private sector simply cannot. In the online world, just as in the offline world, problems will arise that the private sector alone lacks either the will or the means to solve. For example, while nearly everyone may agree that competition in the telecommunications sector is an important goal, the private sector may lack the ability to reach a compromise that all can accept and that

---

[123] A number of governments—including Australia, Ireland and the United States—have recently enacted legislation that extends legal recognition to electronic signatures. *See* Australian Electronic Transactions Act 1999, *available at* http://scaleplus.law.gov.au/html/pasteact/3/3328/top.htm (last visited October 8, 2001); Irish Electronic Commerce Act 2000, *available at* http://www.irlgov.ie/tec/communications/comlegislation/act27-00.pdf (last visited October 8, 2001); U.S. Electronic Signatures in Global and National Commerce Act, Pub. L. No. 106-229, 114 Stat. 464 (2000).

[124] For a discussion of legislation that limits or denies legal recognition to electronic signatures, see Smith, *supra* note *, at 333-43.

[125] *See* text accompanying notes 74 through 76, *supra*.

[126] *See* 47 U.S.C. § 231(c)(2) (2001). An even broader safe-harbor mechanism can be found in the Digital Millennium Copyright Act, which provides that online intermediaries will not be held liable for removing or disabling access to content they believe in good faith to be infringing, even if the material is not in fact infringing. *See* 17 U.S.C. § 512(g)(1) (2001).

adequately promotes the public's interest in low-cost, competitive telecommunications services. In this case, government intervention might be necessary. Likewise, the eradication of child pornography is a problem for which the private sector clearly has the will, but not the means, to solve on its own. And in some other areas, experience may reveal that self-regulation and technology solutions fall somewhat short of the aims they seek to achieve. In all of these situations as well as in others, targeted legal rules may be both necessary and appropriate, either to reinforce private-sector solutions or because only the public sector has the institutional legitimacy, competence, and force of law needed to tackle a problem effectively.

Regardless of the specific reason that stronger public-sector intervention is needed, there are strong reasons to believe that an incremental approach to lawmaking will best serve the public interest. The phrase "incremental approach" in this context means one in which lawmakers first test whether a limited response will work before adopting one that is more far-reaching or that imposes greater burdens on the Internet. Unnecessary over-regulation bears a cost in the form of restricting the growth and development of new technology and use of the Internet. Thus, laws regulating online activity should be targeted and should reach no further than necessary to remedy the problem at hand.

In those cases where regulation is necessary, lawmakers should also adhere to a presumption of technology neutrality. In the age of Moore's law, it is impossible for anyone to predict with certainty which of many competing technologies time will prove to be superior. A regulatory scheme that mandates or provides legal advantages to certain technologies may "freeze" technological innovation by removing any incentive to develop products or services that do not fit the regulatory mold. The true victims of technology-specific laws are likely to be consumers, for such rules may effectively prevent the invention of "non-complying" but superior technologies that might have been developed in a more open regulatory environment.

It is likewise important that lawmakers pursue a policy of non-discrimination toward the Internet. Governments should seek to apply the same basic principles online as off-line and should refrain from imposing requirements onto e-commerce that do not apply to other forms of commerce. The spirit of existing rules should apply to online transactions no less than their off-line counterparts, but in a manner that preserves the efficiencies and benefits that e-commerce holds. Legal requirements imposed solely or unequally on e-commerce risk artificially distorting consumer and business activities away from the Internet, which will likely result in long-term economic loss.

D. International Harmonization

The Internet does not respect national borders. This statement, today virtually a truism, bears repeating, for it captures something truly remarkable about the Internet experience. From a technical perspective, an online transaction between a buyer in downtown New York and a seller in Delhi is no different than a transaction between that same buyer and a seller down the street. This ability to transcend distance is one of the Internet's great assets. It places each and every user in a single, global marketplace with a broad range of choice and increased price competition. It likewise makes it easier for businesses to surmount barriers traditionally created by national borders.

The Internet's global reach is, of course, a focal point of digital libertarian thought. Indeed, it is principally the international aspect of online activity that leads digital libertarianism to reject efforts by domestic (*i.e.*, territorially based) lawmakers to impose their rules onto the Internet. As Post and Johnson write, "Cyberspace radically undermines the relationship between legally significant (online) phenomena and physical location. . . . The Net thus radically subverts the system of rule-making based on borders between physical spaces, at least with respect to the claim that Cyberspace should naturally be governed by territorially defined rules."[127] Even those who do not go as far as digital libertarianism in opposing all state efforts to regulate the Internet argue that its international scope may justify legal reform, at least in some areas.[128]

While digital libertarianism is surely right to point out the complexities of enforcing domestic laws online, its "solution" – to reject efforts to apply law to the Internet – seems to reach farther than makes sense. With rare exception, activities that are illegal off-line do not magically become legal when performed online. More to the point, the socials ills that any given law (*e.g.*, a prohibition on gambling) seeks to prevent (*e.g.*, destitution) typically do not disappear just because the relevant actors use the Internet.[129]

That said, it seems clear that the Internet's global reach should inform the rules by which it is governed. Just as the Internet transcends geographic borders, so too should efforts to regulate online activity seek to move beyond specific national interests. And just as the Internet furthers globalization, it also illuminates the necessity for deeper international dialogue and cooperation. In short, it demonstrates the need for lawmakers, industry, and indeed anyone who cares about the Internet and what goes on there, to seek international harmonization over the principles and norms that will apply to it.

This is true for a number of reasons. First, international consensus will promote predictability and transparency in online commerce. Stable, transparent rules are essential to basic notions of justice and fairness and help promote efficient commercial practices. Disparate rules between jurisdictions, by contrast, may make it next to impossible for online users to determine in advance whether their online activities are legal and may also dramatically increase transaction costs and business risk. For example, multi-national e-commerce firms already devote substantial resources to monitoring legal developments in many different jurisdictions.[130]

---

[127] Post & Johnson, *supra* note 36, at 1370.

[128] *See, e.g.*, Perritt, *supra* note 47, at 886 ("[T]he Internet's global character challenges traditional state-based precepts of private international law, increasing the pressure for public international law regimes to regulate Internet commerce and political activity, directly or indirectly, by providing frameworks for private ordering.").

[129] *See, e.g.*, Jack Goldsmith, *Regulation of the Internet: Three Persistent Fallacies*, 73 CHI.-KENT L. REV. 1119, 1122-27 (1998) (criticizing digital libertarian view that governments should not regulate activities in cyberspace).

[130] *Cf.* Laverty, *supra* note 69 (analyzing regulatory and compliance issues confronting firms that offer information and products online in Asia).

Inconsistent rules may place incompatible obligations on such firms, forcing them either to establish separate business divisions for each market or, where the cost of doing so is too high, to withdraw from certain markets altogether.

Dissimilar national rules, of course, increase transactions costs for any organization that operates internationally, those engaged in commerce in the off-line world as well as those engaged in online commerce. The global nature of the Internet, however, makes it more likely that an online firm will engage in conduct that a foreign country perceives to be governed by its laws and subject to its jurisdiction.[131] As the OECD recently noted in the context of online consumer protection:

> The inherently international nature of the digital networks and computer technologies that comprise the electronic marketplace requires a global approach to consumer protection as part of a transparent and predictable legal and self-regulatory framework for electronic commerce. The global network environment challenges the abilities of each country or jurisdiction to adequately address issues related to consumer protection in the context of electronic commerce. Disparate national policies may impede the growth of electronic commerce, and as such, these consumer protection issues may be addressed most effectively through international consensus and co-operation.[132]

At the extreme, disparate national rules governing e-commerce may erect barriers to international trade. The benefits of globalization and international trade are, of course, hotly contested. Developing countries often voice the concern that foreign competition is driving their economies further into debt and their native cultures further towards irrelevance while doing little to benefit local populations.

These concerns must be addressed in a serious manner. Any successful international trade strategy must ensure that the benefits of globalization extend broadly throughout the international trade community. Globalization cannot be left to create an insurmountable divide between ever-poorer and ever-wealthier nations. This would not only

---

[131] The uncertainty created by disparate national rules and jurisdictional questions was recently cited as a barrier to e-commerce in the Philippines where, although online use is growing rapidly, online commerce remains relatively stagnant. *See* WORLD TRADE ORGANIZATION, SEMINAR ON ELECTRONIC COMMERCE AND DEVELOPMENT para. 43 (1999), *at* http://www.wto.org/english/tratop_e/ecom_e/wtcomtd18.doc (last visited September 28, 2001).

[132] ORGANIZATION FOR ECONOMIC COOPERATION AND DEVELOPMENT, RECOMMENDATION OF THE OECD COUNCIL CONCERNING GUIDELINES FOR CONSUMER PROTECTION IN THE CONTEXT OF ELECTRONIC COMMERCE 1 (1999), *at* http://www.oecd.org/pdf/M00000000/M00000363.pdf (last visited October 8, 2001).

undermine the moral and economic basis on which the world trading system is based, but would almost certainly threaten regional and global security as well.[133]

Yet the Internet offers great potential for addressing these concerns. The "natural" trade barriers that firms from developing countries often face in traditional commerce – such as physical distance from purchasers, inadequate market information and higher transportation costs – are substantially less significant in the e-commerce market. These firms can use the Internet to locate low-cost suppliers, gauge market conditions, advertise and reach consumers at very low cost. As a result, these firms often will be able to compete with large, multinational corporations without the massive capital outlays and infrastructure that off-line international commerce typically demands.

E-commerce may also enable developing country firms to bypass intermediaries that are often needed to accomplish off-line international trade, thereby helping them become more competitive and profitable.[134] And because the Internet is based on open standards, the basic technology needed to engage in e-commerce is widely available and will not raise controversial proposals for compulsory technology transfers that have plagued WTO negotiations in the past. E-commerce may also allow developing countries more easily to exploit comparative advantages in labor costs and skills by facilitating online consulting between developing country consultants and developed country employers.[135]

Developing country firms will realize these benefits, however, only if they face a relatively consistent regulatory environment across jurisdictions. Unilateral actions by lawmakers that do not reflect global consensus could isolate the benefits of e-commerce to specific countries or regions, thereby frustrating efforts to bridge the Digital Divide. Moreover, rules grounded on international consensus will almost certainly be more effective than disparate national rules in the online environment. The effectiveness of domestic laws that are inconsistent with laws enacted elsewhere is likely to be uncertain at best. When mountains of

---

[133] *See, e.g.*, Marrakesh Agreement Establishing the World Trade Organization, Apr. 15, 1994, pmbl; General Agreement on Tariffs and Trade 1994, Apr. 15, 1994, pmbl.

[134] *See, e.g.*, OECD DEVELOPMENT CENTER, OECD, E-COMMERCE FOR DEVELOPMENT: PROSPECTS AND POLICY ISSUES 15 (2000) (noting that craft producers in developing countries who utilize e-commerce "should be able to bargain away any price advantage enjoyed by middlemen by virtue of asymmetric information; they may also be able to eliminate one or more layers of middlemen (a process known as disintermediation)."), http://www1.oecd.org/dev/PUBLICATION/tp/TP164.pdf (last visited October 8, 2001).

[135] *See id.* at 18-19. At a recent WTO seminar on electronic commerce and development, developing country representatives cited a number of examples in which firms from these countries had already begun to use e-commerce to tremendous success. For instance, Africa Online, a company with markets in Kenya, Ivory Coast, Ghana, Tanzania and Zimbabwe, provides online services for individuals and businesses throughout Africa, as well as African expatriates. *See* SEMINAR ON ELECTRONIC COMMERCE AND DEVELOPMENT, *supra* note 131, paras. 18-20. The CEO of Africa Online observed that the company already had 250 employees, 150,000 subscribers, and annual revenues in the tens of millions of dollars. *See id.* para. 18.

data can move from one side of the world to the other at lightening speed, it becomes more difficult for governments to control online conduct based on laws that start and stop at national borders. International coordination at all levels of policymaking and enforcement – whether by the public or private sectors – will make those rules that apply online more effective.

Recent events suggest that we may already be moving toward an era of greater global consensus on Internet-related issues. Relations between the United States and the European Union offer a case in point. The extent and depth of EU/U.S. coordination has flourished in the last five years on a number of issues affecting the Internet. One recent example is the European Commission's E-Commerce Directive,[136] which includes liability rules for online intermediaries that coincide in many respects with the rules on that issue set out in the U.S. Digital Millennium Copyright Act.[137]

Online data protection is another area in which the U.S. and EU have been able to forge compatible if not identical approaches. As noted above,[138] online data privacy in the EU is governed in large part by EU law – specifically, the Framework Data Protection Directive ("Framework Directive").[139] The Framework Directive requires EU Member States to monitor data processing in their jurisdictions and to prevent abusive practices.[140] The Framework Directive also forbids entities to export personal data to non-EU countries whose level of data

---

[136] Council Directive 2000/31/EC on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market, 2000 O.J. (L 178) 1. The Directive provides a broad exemption for transmissions, so long as the service provider does not initiate the transmission, select the recipient of the transmission, or modify the information in the transmission. *Id.* art. 12. The exemption also encompasses the automatic, intermediate and transient storage of the information being transmitted, as long as this is for the sole purpose of carrying out the transmission. And the Electronic Commerce Directive includes a safe harbor, under certain circumstances, for caching and hosting. *Id.* arts. 13-14.

[137] The DMCA provides four "safe harbors" that limit the remedies that may be imposed on Internet service providers for copyright infringements by users. 17 U.S.C. § 512 (2001). An ISP may benefit from these remedy limitations: (1) where it acts as a "mere conduit"; (2) for "system caching"; (3) for unknown storage of infringing material; and (4) for unknowingly using information location tools to refer or link users to a site containing infringing material. *Id.* For an insightful examination of the DMCA, see Jane C. Ginsburg, *Copyright Legislation for the 'Digital Millennium'*, 23 COLUM.-VLA J.L. & ARTS 137 (1999).

[138] *See* text accompanying notes 85 through 86, *supra*.

[139] *See Framework Directive*, *supra* note 85. In 1997, the EU adopted a second data protection Directive specifically governing the telecommunications sector. *See Telecoms Privacy Directive*, *supra* note 85.

[140] *See* Framework Directive, *supra* note 85, art. 28.

protection is not deemed "adequate."[141] The United States, by contrast, places primary responsibility for online data protection on industry self-regulation.[142]

After concerns were raised that these disparate approaches might impede data flows between Europe and the United States, U.S. and EU officials negotiated a "Safe Harbor" Agreement.[143] Under the Agreement, U.S. companies can commit to adhere to a set of principles that reflect the EU's substantive rules of data protection; in return, these companies will be deemed to provide adequate protection under the EU Directive and thus permitted to import data from the EU.[144]

The increasing prominence of international policy organizations provides further evidence of harmonization of the rules governing the Internet. Three of the most prominent bodies are the World Trade Organization (WTO), the OECD, and more recently the World Intellectual Property Organization (WIPO). The WTO has begun to address the specific issues raised by e-commerce in the area of international trade,[145] while WIPO has devoted much time and energy to updating international intellectual property rules to accommodate the online environment.[146] The OECD has also been active, issuing influential model rules and guidelines

---

[141] *Id*. art. 25.

[142] *Cf.* FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE 6-7, 34-35 (2000) (noting U.S. reliance on self-regulation but recommending that Congress consider augmenting this with privacy legislation).

[143] *See* U.S. DEPARTMENT OF COMMERCE, SAFE HARBOR PRIVACY PRINCIPLES (July 21, 2000) *available at* http://www.export.gov/safeharbor/SHPRINCIPLESFINAL.htm (last visited March 9, 2001); *see also* European Commission Decision C(2000) 2441 (finding safe harbor to provide adequate protections under Framework Directive), *available at* http://www.export.gov/safeharbor/nondiscrimArt31May00.htm (last visited March 9, 2001).

[144] *Id*. At least one U.S. organization has launched a self-regulatory program to assist U.S. firms in adhering to the Agreement. The TRUSTe safe harbor seal program enables U.S. firms to comply with EU data protection laws without inadvertently breaching U.S. privacy rules. *See* Steve Gold, *TRUSTe To Offer European Union Safe Harbor Seal*, NEWSBYTES, Nov. 1, 2000, *at* http://www.newsbytes.com/news/00/157551.html (last visited March 9, 2001).

[145] *See, e.g.*, WORLD TRADE ORGANIZATION, MINISTERIAL DECLARATION ON GLOBAL ELECTRONIC COMMERCE (May 20, 1998) (declaring that "Members will continue their current practice of not imposing customs duties on electronic transmissions"); WORLD TRADE ORGANIZATION, SEMINAR ON ELECTRONIC COMMERCE AND DEVELOPMENT (Feb. 19, 1999). Although the 1998 moratorium on e-commerce customs duties has formally expired, at least some WTO members have agreed to extend the moratorium. *See, e.g.*, B. Pearson, *APEC Presses for World Talks*, AUSTRALIAN FINANCIAL REVIEW (June 8, 2000).

[146] These efforts resulted in the so-called "Internet" treaties of 1996. *See* World Intellectual Property Organization, Copyright Treaty, Dec. 20, 1996, 36 I.L.M. 65 (1997); World Intellectual Property Organization, Performances and Phonograms Treaty, Dec. 20, 1996, 36 I.L.M. 76 (1997).

in a number of areas, including privacy,[147] online consumer protection,[148] encryption policy[149] and e-commerce taxation.[150] And a host of other influential international bodies has been active as well on these and related issues, including the United Nations Commission on International Trade Law (UNCITRAL) and the Association of South East Asian Nations (ASEAN).[151]

The private sector has also been engaged broadly in seeking internationally harmonized Internet rules. In fact, hundreds of private-sector industry and consumer bodies have been active in this area. One group that focuses solely on the international implications of e-commerce rules is the Global Business Dialogue on Electronic Commerce (GBDe). The GBDe grew out of a request by the European Commission for the private sector to identify barriers to e-commerce and to propose solutions.[152] GBDe working groups focus on a number of policy and legal issues affecting international e-commerce, including online privacy, consumer protection, trade and taxation, and intellectual property rights.[153] Yet another noteworthy organization in this area is the International Chamber of Commerce (ICC), which is an active private-sector advocate on a range of Internet-related matters.[154]

All of these initiatives reflect a growing recognition that online activities cannot adequately be dealt with purely on a local, national, or even regional basis. The Internet

---

[147] *See* OECD, GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (1980), *available at* http://www.oecd.org//dsti/sti/it/secur/prod/PRIV-EN.HTM (last visited March 9, 2001). *See also* text accompanying notes 83 through 84, *supra.*

[148] *See* OECD, GUIDELINES FOR CONSUMER PROTECTION IN THE CONTEXT OF ELECTRONIC COMMERCE (1999), *available at* http://www.oecd.org/dsti/sti/it/consumer/prod/guidelines.htm (last visited March 9, 2001); OECD, CONSUMER PROTECTION IN THE ELECTRONIC MARKETPLACE (1998), available at http://www.olis.oecd.org/olis/1998doc.nsf/LinkTo/DSTI-CP(98)13-FINAL (last visited March 9, 2001).

[149] *See* OECD, CRYPTOGRAPHY POLICY: THE GUIDELINES AND THE ISSUES (1997), *available at* http://www.oecd.org/dsti/sti/it/secur/prod/gd97-204.pdf (last visited March 9, 2001).

[150] *See* OECD, CLARIFICATION ON THE APPLICATION OF THE PERMANENT ESTABLISHMENT DEFINITION IN E-COMMERCE: CHANGES TO THE COMMENTARY ON ARTICLE 5 (2001), *available at* http://www.oecd.org/daf/fa/treaties/Clarif_e.pdf (last visited March 9, 2001).

[151] *See, e.g.*, ASEAN, E-ASEAN FRAMEWORK AGREEMENT (2000), available at http://www.aseansec.org/ (last visited March 9, 2001); UNCITRAL, DRAFT UNIFORM RULES ON ELECTRONIC SIGNATURES (2000), *available at* http://www.uncitral.org/en-index.htm (last visited October 8, 2001); UNCITRAL, MODEL LAW ON ELECTRONIC COMMERCE (1996), *available at* http://www.uncitral.org/en-index.htm (last visited October 8, 2001).

[152] *See* Communication on Globalization and the Information Society, COM(98)0050.

[153] *See* GLOBAL BUSINESS DIALOGUE, GBDE 2000 WORKING GROUPS ISSUES SUMMARY, *at* http://www.gbd.org/structure/working/issues.html (last visited March 9, 2001).

[154] *See, e.g.*, INTERNATIONAL CHAMBER OF COMMERCE, TAX ISSUES AND RAMIFICATIONS OF ELECTRONIC COMMERCE (Document No. 180/421) (1999), available at http://www.iccwbo.org/home/statements_rules/statements/1999/tax_issues_and_ramifications_of_electronic_commerce.asp (last visited March 9, 2001).

demands that the public and private sectors reach out to their counterparts in other parts of the world to develop rules and mechanisms that will be both effective and consistent with the global nature of contemporary Internet communications and commerce.

IV. Conclusion

Although accurately predicting the future is never simple, doing so with respect to information technologies is even more daunting. Not only are these technologies changing quickly, but their future is highly dependent on three other factors that inject additional uncertainty. The first is the dependence of so many technologies on each other, meaning that an unforeseen advance in one area can quickly lead to unanticipated changes in many other areas as well. The second is the decisive role of the consuming public in determining whether a particular technology will succeed, or whether it will fall by the wayside and into obscurity. And the third is the geometric rate of change in technology performance that a new advance can unleash.

All of this holds particularly true with respect to the Internet. It is rapidly becoming apparent that the Internet is likely to change significantly in the coming years. In many respects the Internet today is a "read-only" experience in which users can access vast amounts of data, but can do relatively little to edit, analyze, or incorporate these data into their work.[155] Personalization is possible, but it typically requires that one repeatedly enter the same personal data and effectively surrender control of that data to each site one visits. Individuals are being forced to adapt to the technology because the technology has not yet adapted to them.

The next generation of the Internet is likely to change this. One aspect of this change will likely put more power in the hands of users, so that it will be easier for people not only to collect information from the Internet but to do more with this information once they have it. To achieve this, much of the technological focus behind the Internet will likely shift from individual websites or devices to constellations of computers, devices, and services that work together to deliver broader, richer solutions.[156]

There are also likely to be changes in the way people interact with computers. The next several years will bring technologies that let people talk to their computers, communicate through hand gestures, even take notes on a tablet PC and transpose those notes instantly into typewritten text. Other advances will make it easier for computers to read text aloud. With these changes, computers will become more useful tools for people, making information on the Internet more accessible and usable anywhere, at any time, and on any computing device.

---

[155] *See* MICROSOFT CORPORATION, MICROSOFT.NET: REALIZING THE NEXT GENERATION INTERNET – A MICROSOFT WHITE PAPER (2000).

[156] *Id.* at 3.

As the Internet evolves and its impact on daily life grows in depth and complexity, the economic and social implications of the Internet are likely to grow as well. Indeed, it is no understatement to suggest that the legal and policy issues for those in government may match in difficulty and importance the challenges faced by the technologists and engineers bringing these new inventions to market.

This article has attempted to provide a roadmap of sorts to addressing these issues by articulating a new policymaking framework for the Internet. This approach rests on the premise that the Internet demonstrates the need for a new way to identify and address problems rooted in technology, involving greater collaboration between the private and public sectors.

Specifically, digital pragmatism advocates significant reliance on self-regulation and other market-based solutions to solve problems that arise online and envisions a greater role for technology solutions to such problems. At the same time, digital pragmatism envisions a more complex, multi-faceted role for governments. This role requires public actors to collaborate with affected private-sector constituencies to identify potential risks, encourage viable solutions that represent the public interest, and support such efforts with the public at large. Of course, government's traditional functions of lawmaker and law enforcer also remain essential, particularly in articulating the baseline rules governing private-sector conduct and in enacting measures that support workable private-sector solutions – or in intervening when such solutions fall short of their aims. In doing so, however, it is important for governments to proceed incrementally with laws that are technology neutral, non-discriminatory and flexible so as not to restrict unnecessarily the substantial economic and social contributions that the Internet can make. Finally, digital pragmatism advocates greater international dialogue and harmonization of online regulatory efforts in order to minimize legal disparities and avoid online users being subject to inconsistent and potentially contradictory rules.

Digital pragmatism demands a great deal from both the public and private sectors, but perhaps what it underscores most of all is the need for greater and more meaningful political dialogue. On the one hand this challenge is daunting. Recent years have witnessed a general decline in political civility in some capitals, including Washington, D.C. And one would be hard pressed to claim that industry has had an impressive track record in acting proactively to provide public officials with sufficient information about ongoing and upcoming technological changes and their potential implications. Those of us in the private sector need to do more to share information on technological innovations and developments with people in government; and we all need to do more to discuss together the best ways to address the public policy issues these innovations and developments are creating.

In this type of environment, discussion is likely to be more enlightening than litigation. And a combination of public leadership, industry initiative and self-regulation is likely to be more effective than new laws or regulations enacted alone. This does not mean that the law – or the role of lawyers, for that matter – will become less important. To the contrary, the broad and complex nature of the challenges at hand makes issues of law and public policy as important and formidable as ever.

The Internet is already an extraordinary phenomenon. But we are not yet even halfway through this remarkable new chapter of human history. If we can innovate with respect

to our forms of political dialogue, even while engineers and scientists continue to improve the technology itself, then we will take a major stride towards ensuring that this third industrial revolution realizes its full potential.