INTELLECTUAL PROPERTY AND THE INTERNET: A JAPANESE PERSPECTIVE

Masanobu Katoh*

I. INTRODUCTION

A task force on industrial competitiveness and intellectual property policy convened by the Japanese Ministry of Economy, Trade, and Industry ("METI") recently issued a remarkable report. The thrust of the report is how Japan could improve its international competitiveness by becoming a more "intellectual property-based nation." The report reflects a major shift in orientation for Japan. Historically, Japan saw its comparative advantage in international trade in manufacturing. Products would be developed abroad – typically in the United States – and Japanese companies would find a way to manufacture them less expensively and with higher quality – cheaper and better. U.S. companies often accused Japanese companies of infringing on their intellectual property rights.

Now, countries with emerging economies are assuming the position once occupied by Japan. With their low labor costs and increasing technological sophistication, these emerging economies can manufacture high quality products at a low cost. Japan finds itself increasingly acting as an exporter, rather than an importer, of intellectual property. The task force correctly recognizes that Japan's economic future lies in accelerating this shift – in taking advantage of its highly educated population to become an exporter of intellectual property, as the United States is today. This requires placing a far greater emphasis on intellectual property rights than ever before.

* Senior Group Vice President, Legal & Industry Relations Group and Export Control Group, Fujitsu Limited. The views expressed in this article are those of the author and are not necessarily the views of Fujitsu Limited.

While the report does recommend specific amendments to Japanese laws, these changes typically involve improving patent prosecution or civil litigation procedures; they do not require major substantive changes to Japanese intellectual property law. Moreover, many of the report's recommendations focus on systemic issues: improving the instruction of intellectual property laws at Japanese law schools, facilitating technology transfer between universities and corporations, and making businesses think more strategically about intellectual property.

In short, the report recognizes that intellectual property does not exist in a vacuum; it is part of a larger social and legal framework. The report further recognizes that making intellectual property laws more stringent is not the only, or even the best, way to increase the level of creativity or innovation in a society. In this sense, the report is consistent with recent amendments to Japanese law necessitated by the advent of the Internet – specifically, liability safe harbors for Internet service providers and implementation of the World Intellectual Property Organization ("WIPO") Copyright and Performances and Phonograms Treaties. These amendments balance the interests of all stakeholders, rather than simply enhance protection for authors.2

In contrast to this balanced approach, some of the large U.S. content providers have advocated unbalanced proposals in the course of a vigorous campaign against copyright infringement on the Internet. Some non-U.S. content providers have joined this effort but, until now, this has largely been a U.S. initiative. The content providers have argued that the Internet's digital technology allows for the rapid reproduction and distribution of high quality, unauthorized copies of works. This rampant infringement, they contend, has suppressed legitimate sales of music CDs, and has inhibited content providers from distributing their products over the Internet. Accordingly, the content providers have advocated the adoption of new laws to protect their content. Until recently, the cornerstone of this legal strategy was the WIPO Copyright and Performances and Phonograms Treaties, which require contracting

---

2. Interestingly, the notion of balanced intellectual property protection is largely an American creation. As the U.S. Supreme Court noted in a landmark decision involving a Japanese company, Congress... has been assigned the task of defining the scope of the limited monopoly that should be granted to authors or inventors in order to give the public appropriate access to their work product... [T]his task involves a difficult balance between the interests of authors and inventors in the control and exploitation of their writings and discoveries on the one hand, and society's competing interest in the free flow of ideas, information and commerce on the other. Sony Corp. v. Universal City Studios, Inc., 464 U.S. 417, 429 (1984).

While this decision focuses on the balance between authors and society, it is becoming increasingly clear in this new millennium that the balance is far more complex. On the "society" side of the balance, at least three sets of stakeholders can be identified: distributors such as Internet service providers, second generation authors, who must build on the work of first generation authors, and end users. On the "authors" side, individual authors' interests differ from those of large corporate content providers such as book publishers, record companies, and motion picture studios. Additionally, large corporate content providers often have conflicting economic interests – music publishers and record companies, for example, often find themselves fighting over the same pot of money.
parties to prohibit the circumvention of technological protection measures. Not satisfied with implementing the treaties in the United States, Japan, and the European Union, the content providers have advocated the enactment of even more stringent laws.

Reasonable people can disagree on the economic impact of Internet infringement on the content providers. Some studies show that the availability of music on the Internet has actually led to an increase of CD sales after consumers “sampled” the music. These studies suggest that the record industry’s sluggish performance is more a result of high prices combined with uninspiring products. Moreover, the staggering cost of Internet infringement cited by the content providers is based on the arguably flawed assumption that every download is a lost sale at full retail price. Similarly, the content providers have never been able to demonstrate convincingly that the fear of infringement has actually deterred them from adopting Internet-based distribution models.

Nonetheless, there can be no question that infringement does occur on the Internet; that it does cause some marginal economic harm to some content providers; and that it does promote a sense of lawlessness and disrespect for the law that can spill over into other areas. In other words, Internet infringement is a real problem that requires real solutions.

The challenge for policy makers is to find solutions that do not cause collateral damage so severe that society is better off without them. In particular, the solutions to Internet infringement must threaten neither the fundamental operation of the Internet nor its technological development. Stated differently, policy makers must make sure that they find solutions that balance the interests of all stakeholders, rather than just clamp down on infringement.

This paper will compare the Japanese government’s initial foray into this difficult area with some of the recent proposals sponsored by the U.S. content industries. Starting with Japan, the paper will examine the METI task force’s proposed strategies to strengthen industrial

3. See, e.g., Forrester Sees $2 Billion Digital Music Market by 2007, MERCURY NEWS (San Jose), Aug. 13, 2002, available at http://www.siliconvalley.com/mld/siliconvalley/news/editorial/3856253.htm. In many retail outlets, a DVD containing a two-hour film and an additional hour of commentary, outtakes, and alternate endings costs less than a CD with thirty minutes of music. Additionally, a consumer is often interested in just one three-minute song, yet record companies no longer sell singles, in effect forcing the consumer to buy nine songs she doesn’t want to get the one she does. While CD sales have decreased over the past year, DVD sales have increased dramatically; during the first half of 2002, DVD sales and rentals generated $2.6 billion in revenue, while theatrical releases earned $1.7 billion and video $1.6 billion. Id. See Frank Ahrens, Hollywood Sees the Big Picture With DVDs, WASH. POST, Oct. 7, 2002, at A1. The high picture quality, the low price, and the additional features bundled with the movie make DVDs extremely attractive to consumers. The enormous success of DVDs demonstrates that the content industry can compete with free distribution. Id.

4. Many teenagers, for example, download songs they would never consider buying, and rarely if ever listen to the songs once they’ve downloaded them.

competitiveness through intellectual property. The paper will then
discuss the Japanese implementation of the anti-circumvention
provisions of the WIPO treaties, and the liability safe harbors for
Internet service providers.

Turning to the United States, this paper will review different
legislative proposals introduced by Senators Hollings and Biden, and
Congressmen Berman, Boucher, and Lofgren in the 107th Congress. This
paper will also review several cases brought in the United States and the
European Union under existing laws. The paper's conclusion is that, so
far, the Japanese government seems to have struck the right balance in
its initial foray into this difficult area. By contrast, some of the more
recent proposals in the United States seem out of balance, tilting toward
content providers and away from all other stakeholders.

II. JAPANESE DEVELOPMENTS

Japan's legal system is based on the civil law rather than the
common law approach. Legal change, therefore, comes from
government action, particularly statutes enacted by the Diet, the
Japanese Parliament. There is far less litigation in Japan than in the
United States, and greater adherence to industry guidelines and ministry
interpretations of statutes. Accordingly, a discussion of Japanese legal
developments rarely involves an examination of judicial opinions.

A. Industrial Competitiveness and Intellectual Property

In 2001, METI assembled a task force on industrial competitiveness
and intellectual property policy. In 2002, the task force, composed of
industry leaders and academics, issued a report containing its
recommendations. It appears that METI will undertake to implement
those recommendations.

The task force observed that Japan's industrial competitiveness has
decreased, particularly as compared to the United States and China.
During the 1970s and 1980s, in response to its perceived decline in
competitiveness, the United States adopted a pro-patent policy. This
policy helped restore it to a competitive position. The METI task force
recommended that Japan similarly launch a pro-intellectual property
("IP") initiative, with the goal of becoming one of the world's principal
IP-based nations. The task force identified four strategies to achieve this
goal.

First, Japan should establish a human foundation for the era of
intellectual creation. This means developing researchers engaged in
intellectually creative activities as well as IP service providers. Specific
approaches could involve developing IP programs at law schools and amending the Patent Law to provide incentives for employees to invent.\(^7\)

Second, universities and research institutions should create and accumulate more intellectual property. This would accelerate the creation of intellectual property in advanced technology. The task force recommended thorough enforcement of the Japanese version of the Bayh-Dole Act, which facilitates commercialization of government-funded research. Universities could also become more proactive in managing IP developed on campus.\(^8\)

Third, businesses should actively use intellectual property in corporate management. This requires developing an environment to implement intellectual property-based business strategies. Businesses must establish strategic programs to develop and protect intellectual property. Additionally, trade secret laws and trial procedures need to be amended.\(^9\)

Fourth, the overseas protection of intellectual property must be strengthened. In other words, Japanese intellectual property must be protected against foreign infringement. Specific measures would involve stronger border controls and encouraging better enforcement of intellectual property laws abroad. In the past, Japan and the United States often found themselves on opposite sides of trade disputes involving IP. This new initiative suggests that, in the near future, the United States and Japan will work together to prevent counterfeiting and other forms of infringement in developing economies.\(^10\)

The task force report avoids the easy solution of expanding intellectual property rights. It evidently recognizes that substantive changes to the law will not, by themselves, transform Japan into a leading IP-based nation. Rather, Japan must pursue a more heterogeneous strategy that also includes procedural changes, a greater emphasis on enforcement, strategic actions by universities and businesses, and the overhaul of legal education.

It is relatively simple and inexpensive to get a legislature to enact new prohibitions. But new prohibitions will not change the way a society thinks about innovation and intellectual property. Indeed, new prohibitions run the risk of inhibiting legitimate, productive activities by law-abiding people and institutions without an offsetting increase in innovation and creativity. Accordingly, the task force recommends a sophisticated mix of complex – and often expensive – strategies that are more likely to achieve the desired transformation of Japanese society than the expansion of protection. To be sure, expanded protection has its place, but only as a part of a balanced, multi-faceted strategy.

---

7. *Id.* at 10-14.
8. *Id.* at 15-22.
9. *Id.* at 23-34.
10. *Id.* at 35-39.
B. WIPO Treaties Implementation

In 1999, the Japanese government amended the Copyright Law in order to implement the anti-circumvention requirements of the WIPO Copyright and Performances and Phonograms Treaties. The Copyright Law Amendments prohibit the distribution of devices that circumvent technological measures that protect copyright and related rights (copy control measures). Additionally, the Japanese government went beyond the treaties’ requirements by adopting amendments to the Unfair Competition Prevention Law (“UCPL”) that prohibit the distribution of devices that circumvent access control measures. Taken together, these two laws prohibit the manufacture and distribution of circumvention devices to the same extent as Title I of the U.S. Digital Millennium Copyright Act (“DMCA”).

1. Copyright Law Amendment

The Copyright Law Amendment provides new criminal penalties for the manufacture and distribution of devices and software (hereinafter collectively referred to as “devices”) that have the principal purpose of circumventing technological protection measures employed by copyright owners to protect copyright and related rights. The circumvention of access control measures is outside the scope of this law, but can be subject to the UCPL, as discussed below.

An article written by an official of the Japanese Cultural Agency in the July 1999 issue of Copyright provides a section-by-section analysis of the legislation. With respect to the standard articulated in Article 120bis(1), “[d]evices or software whose principal function is to circumvent technological protection measures,” the article provides the following two insights. First, the “principal function” means that there is only a limited commercially significant function other than circumvention. The principal function test thus is similar to Section 1201(b)(1)(B) of the DMCA. Second, to the extent that a component has only a limited commercially significant function other than circumvention, a device incorporating the component is subject to the prohibition. The article mentions that a copy protection circumvention component installed in a VCR might fall within the scope of prohibition.

11. Japan, Indonesia, and the Philippines are the only East Asian countries that have become members of the WIPO treaties, so far.

12. As discussed infra, the UCPL amendments also prohibit devices that circumvent copy controls. Thus, both the Copyright Act and the UCPL provide remedies against copy control circumvention devices while only the UCPL provides remedies against access control circumvention devices.


14. Japan Copyright Office in the Cultural Affairs Ministry, Notes about “A Law Partly Amending the Copyright Act,” KOPIRAITO [COPYRIGHT] 24, 1999 (Japan) [hereinafter “Copyright Act Notes”].
under the law. Therefore, Article 120bis(1) has almost the same statutory effect as Section 1201(b)(1) of the DMCA.

Like the DMCA, the legislation does not mandate that devices respond to specific signals of technological protection measures. In his article, the Cultural Agency official discusses that it is not appropriate to require devices to respond to such signals because that would lock manufacturers into certain technological specifications. The article clarifies that the mere fact that a device does not respond to certain signals does not constitute the circumvention.

Although the Japanese Copyright Act in Article 30(1) permits reproduction for private use, the legislation prohibits private copying performed after the circumvention of a technological protection measure. The legislation does not contain all the exceptions found in the DMCA or the EU Copyright Directive. However, because the legislation provides only criminal remedies, prosecutors are likely to initiate actions only in cases involving serious copyright infringements, and will not pursue cases involving socially useful acts of circumvention, such as reverse engineering, for the purposes of achieving interoperability.

2. The Unfair Competition Prevention Law Amendment

This amendment provides civil remedies for the distribution of circumvention devices that will harm fair competition in the market. Because the law governs the fairness of competition in the market, its application is not limited to copyrighted works, but extends to other commercially-marketed digital content as well. Additionally, because it is not tied to copyright, the new provision applies to devices that circumvent both access and copy controls.

Articles 2(1)(x) and (xi) of the Unfair Competition Prevention Law ("UCPL") provide that the distribution of devices having no significant function other than to circumvent technological protection measures is prohibited. Article 2(1)(x) specifically regulates the distribution of illegal devices that circumvent measures employed by content providers to protect their business interests. Devices that circumvent standardized protection technologies automatically fall within the scope of the prohibition.15

Meanwhile, Article 2(1)(xi) applies in cases where content providers use technological protection measures, such as encryption, to restrict access by unauthorized persons. Thus, the distribution of cable descramblers is prohibited where the content providers and cable TV operators limit access to cable programs. In the July 1999 edition of

---

15. MacroVision, SCMS (Serial Copy Management System), CGMS (Copy Generation Management System), and CSS (Content Scrambling System) are standardized protection technologies that fall within this category.
Copyright, the Office of Intellectual Property Policy in the Ministry of International Trade and Industry provides guidance with respect to "devices having no significant function other than to circumvent." The article says that a device that has no commercially or economically significant purpose or use other than to circumvent would be subject to the law.

While the law exempts general-purpose devices such as personal computers (PCs) because they have a significant function other than circumventing technological protection measures, the distribution of PCs equipped with components that principally possess a circumvention function is explicitly prohibited. In addition, the law does not mandate that devices respond to specific signals. As with the copyright amendments, the UCPL amendments do not contain all the detailed exceptions of the DMCA. However, a plaintiff can prevail if he can show that the circumvention device harms fair competition in the market. This requirement will limit abuse of the new law. Thus, these provisions generally parallel the access control provisions of Section 1201(a) of the DMCA.

C. Internet Service Provider Safe Harbors

In 2001, the Japanese government adopted legislation that provides "specified telecommunications service providers" with a safe harbor from damages liability for the unlawful activities of their subscribers. In essence, this legislation provides Japanese Internet service providers with safe harbors similar to those provided by Title II of the DMCA, and Article 14 of the EU e-Commerce Directive. Prior to the adoption of the safe harbors, service providers were liable for the unlawful activities of subscribers, including copyright infringement and defamation, under general tort principles. The new law did not change the substantive standards of tort law with respect to service providers.

The new law follows a "horizontal" approach similar to that of the EU e-Commerce Directive. It applies equally to all unlawful conduct, including copyright, defamation, indecency, etc. It focuses on Web-hosting activities because other Internet functions, such as mere conduit or information location services, are unlikely to expose service providers to liability under tort principles.

The new law provides the service provider with immunity from liability to the subscriber if the service provider removes the subscriber's unlawful content under two circumstances: (1) when the service provider had "good ground sufficient . . . to believe that the right of another person would be wrongfully infringed due to the distribution" of the content; or (2) when the service provider (a) receives a notice from the

16. Copyright Act Notes, supra note 14, at 39.
harmed person that the content is harmful; (b) forwards the notice to the subscriber; and (c) within seven days, does not receive an explanation from the subscriber of why the content is not unlawful.

Additionally, the new law provides the service provider with immunity from liability to the person harmed by the unlawful content, unless: (a) the service provider knew that the right of another person would be infringed by the distribution of the content; (b) there was good ground sufficient to find that the service provider could have known that the right of another person would be harmed by the distribution; or (c) the service provider was the sender of the information. Unlike the DMCA, the Japanese law does not explicitly condition this safe harbor on compliance with a "notice and takedown" regime. However, as discussed above, the law does contemplate the harmed person (e.g., the copyright owner) notifying the service provider of the presence of the infringing content. If the service provider does not remove the content after the subscriber failed to provide a satisfactory explanation, the service provider is hard-pressed to contend that it does not have sufficient grounds to believe that the content is unlawful, and would likely fall out of the safe harbor.

Moreover, major associations of service providers and copyright owners recently agreed to voluntary guidelines that establish a self-regulatory DMCA-like notice and takedown regime. In addition to clarifying the new law’s provisions, the guidelines seek to create a mechanism to circumvent the seven-day period during which the service provider must wait for the subscriber to respond to the notice of the alleged infringement. In essence, the guidelines create a framework by which the service provider receives “good ground sufficient . . . to believe that the rights of another person would be wrongfully infringed due to the distribution” of the content. The guidelines specify the kind of notice from the rights-holder or credibility certification organization that would provide the service provider with grounds sufficient to take down the content without waiting seven days for the subscriber’s response.

Finally, the law would significantly enhance the ability of a person harmed by infringing content to enforce his rights. Under Japanese law, a lawsuit cannot be filed against an anonymous defendant, and no civil procedure previously existed to discover the identity of an unknown, would-be defendant. The new law creates a process by which the harmed person could request that the service provider disclose the identity of the subscriber posting the unlawful content. The rights-holder then could file an infringement action against the subscriber. The disclosure process under the new Japanese law is analogous to the subpoena power provided by Section 512(h) of the DMCA to identify the infringer.

In sum, like the DMCA and EU e-Commerce Directive, the Japanese safe harbor provisions try to find a balance between the
interests of the rights-holder, the service provider, and the subscriber. The provisions shelter service providers from liability for the infringing acts of their subscribers, but at the same time create a mechanism by which a service provider can remove infringing material at the request of the rights-holder. The provisions allow the rights-holder to learn the identity of an infringing subscriber, but at the same time provide the subscriber with an opportunity to respond to a rights-holder’s allegations prior to removal of the allegedly infringing material. To be sure, there are differences between the DMCA, the EU e-Commerce Directive, and the Japanese safe harbors, but the general construct is the same.

III. UNITED STATES DEVELOPMENTS

A. The Hollings Bill

In March 2002, Senator Fritz Hollings of South Carolina, Chairman of the Senate Commerce Committee, introduced S. 2048, the Consumer Broadband and Digital Television Promotion Act. The bill sparked a fierce war of words between the entertainment industry and the information technology industry — two industries that previously had supported one another in legislative efforts to increase intellectual property protection. The furor created by the bill demonstrates the counter-productive nature of one-sided legislation.

The Hollings Bill would give copyright owners, consumer groups, and the manufacturers of digital media devices twelve months to reach an agreement on “security system standards for use in digital media devices...” If within those twelve months the parties do reach an agreement, the Federal Communications Commission (“FCC”) is to adopt those standards as a legally binding regulation. On the other hand, if the parties do not reach an agreement, the FCC must initiate a rulemaking proceeding to adopt a standard. The final rule would be promulgated no more than a year after the initiation of the rulemaking. The FCC could conduct subsequent rulemakings to modify the security system standards as necessary.

The Hollings Bill is based on a complex set of related assumptions. The first assumption is that broadband Internet services and digital television are not being adopted by U.S. consumers as rapidly as they should. The second assumption is that this reduced demand is a function of the absence of attractive entertainment content on the Internet and digital television networks. The third assumption is that entertainment companies are not distributing their content in digital form because they

fear widespread infringement. The fourth assumption is that this fear would be eliminated if all the affected industries could agree on digital rights management ("DRM") systems that could prevent infringement. The fifth assumption is that an agreement has not been reached on DRM standards because of "competing business interests."

This chain of assumptions is subject to question. First, U.S. consumers are adopting broadband at a far faster rate than they adopted other technologies, including telephones, television, personal computers, and dial-up Internet access. There is significant excess broadband capacity, but that may be a function of overly optimistic projections by the telecom industry.

Second, many observers do not believe that the adoption of broadband is linked to the availability of entertainment content. These observers believe that for the foreseeable future, consumers will prefer delivery of entertainment content through existing cable and satellite distribution channels. Other applications, such as distance education, distance medicine, telecommuting, home video telephony, and e-government, will stimulate broadband demand. Additionally, many feel that demand will soar at a lower price point.

Third, there is little evidence that entertainment companies are in fact withholding their content from the Internet because of the fear of infringement. Entertainment companies are not making robust use of existing technological protections systems, such as encryption. Also, unlawful copies of most entertainment content are already available on the Internet. There is no proof that distributing more works legally on the Internet will lead to more infringement. If anything, the opposite is the case. Properly designed and priced Internet distribution systems might lead many consumers to forego low quality infringing copies for high quality lawful ones.

Fourth, no matter what DRM system is ultimately adopted, there will always be a certain amount of infringing activity on the Internet. Any DRM system can be defeated. Additionally, a significant amount of the "leakage" comes from within the entertainment companies, as low-level employees sell bootleg copies prior to official release. In the
future, these employees will sell bootleg copies prior to the application of
the DRM. Given this basic fact of life in the digital era, entertainment
companies should redouble their efforts to find business models that
offer consumers compelling alternatives to the distribution of low-quality
copies over person-to-person or "P2P" networks.

Fifth, while "competing business interests" may have delayed
agreement on DRM standards, a more significant factor is the difficulty
inherent in developing a technology that is simultaneously difficult to
rack, relatively inexpensive for content owners to deploy, not disruptive
of existing Internet systems, compatible with a broad range of computer
and consumer electronics devices, and respectful of consumer fair use
privileges.26 Indeed, the last issue may prove particularly contentious in
the future, as there is little agreement concerning the scope of fair use
in the digital era. Many technologists strongly doubt that the FCC can
develop such a standard in twelve months.

In addition to questioning the Hollings Bill's assumptions, many
observers have serious concerns about the bill's substance.27 In
particular, many U.S. technology companies strongly oppose government
involvement in the setting of technical standards.28 They believe that the
government does not have the necessary expertise to select a standard.29
Additionally, they feel that a government-directed standard setting
process will proceed too slowly, thereby retarding the innovation. Once
a standard is set, the government will be reluctant to modify or update it,
further retarding innovation.30 Technologists also believe that a
government-directed standards process will inevitably become
politicized. In particular, they fear that the Internet's speed and
efficiency will be sacrificed in favor of protecting the assets of the
politically connected entertainment companies.31 They note that the bill
would apply to many computer and consumer electronics products, given
the broad definition of "digital media device."32

---

26. Catherine Olanich Raymond, The Consumer Broadband and Digital Television Promotion
27. Letter from Barbara Simons, Ph.D. and Eugene H. Spafford, Ph.D., Co-Chairs, U.S. Ass'n
for Computing Mach., to the Honorable Ernest F. Hollings, Chairman, Senate Comm. on Com., Sci.
Transp., 107th Cong. (2002) (testimony of Leslie L. Vadasz, Executive Vice President, Intel Corp.)
[hereinafter Testimony of Leslie L. Vadasz]; Robyn Weisman, Titans Clash at U.S. Senate Digital
2002); Clark & Vaida, supra note 23.
29. See generally LAWRENCE GASMAN, TELECOMPETITION: THE FREE MARKET ROAD TO THE
INFORMATION HIGHWAY (1994).
31. Id.
32. The bill states:
The term 'digital media device' means any hardware or software that –
(a) reproduces copyrighted works in digital form;
Many of these same objections can be raised against the other alternative under the Hollings Bill: codification of an industry agreement on security system standards. Legally compelling all manufacturers to comply with one standard will likely inhibit the development of new technologies.\textsuperscript{33} Moreover, an industry-led standards process can also become politicized; standards can be selected on the basis of business alliances rather than pure engineering considerations.

Codification of a standard – whether set by industry or by the government – also represented a departure from the legislative compromise of Title I of the DMCA. The information technology industry agreed to the prohibition on the manufacture of circumvention devices and components only because of the inclusion of the “no mandate clause” in Section 1201(c)(3): “Nothing in this section shall require that the design of, or design and selection of parts and components for, a consumer electronics, telecommunications, or computing product provide for a response to any particular technological measure . . . .” Notwithstanding this provision, the Hollings Bill would require all digital media devices to respond to the security system standards established pursuant to the legislation. Segments of the technology industry viewed the entertainment industry’s attempted reversal of the DMCA’s no mandate provision as an act of bad faith.\textsuperscript{34}

While many of the U.S. technology industry’s concerns with the notion of government-mandated standards have validity, they also may be somewhat overstated. The U.S. government has often played a central role in developing the standards for infant industries – most notably the computer industry and the Internet itself.\textsuperscript{35} Many of these early government decisions are still reflected in the Internet’s architecture. There is, of course, a significant difference between establishing standards in a “green field” situation, where no industry exists and no one is prejudiced, and imposing standards on a mature industry.

Regardless of the merits of the respective positions, the introduction of the Hollings Bill caused a major eruption on Capitol Hill. At hearings on the legislation, entertainment industry executives accused the consumer electronics and information technology industries of dragging their heels on the adoption of DRM standards.\textsuperscript{36} More
pointedly, some entertainment executives stated that the technology industry's business model was based on the unlawful copying of copyrighted content.  

Accused of contributing to copyright infringement, the technology industry fired back. It charged the entertainment industry with encouraging infringement by refusing to adopt new business models. It observed that the technology industry contributes far more to the U.S. economy than the entertainment industry, yet the entertainment industry preferred to put this large sector at risk rather than invest in modernization. The technology industry also asserted that the entertainment industry wanted to stifle consumer privileges such as time-shifting and space-shifting.

The controversy concerning the Hollings Bill split the previously unified content provider front. The Business Software Alliance, which typically supported entertainment industry efforts to expand copyright protection, voiced opposition to the Hollings Bill. Additionally, Intel filed a friend of the court brief in the U.S. Supreme Court that, although purporting to be neutral, generally sided against the entertainment industry in the case concerning the constitutionality of the Sonny Bono Copyright Term Extension Act.  

Moreover, the media attention on this open dispute between the entertainment and technology industries mobilized consumers who feared the erosion of their fair use privileges. The founder of the defunct Internet service provider Excite established digitalconsumer.org and, within a few weeks, over 45,000 consumers joined this grass-roots organization. The perception that the entertainment industry was assaulting fair use was fueled by statements by industry executives that fast-forwarding through the commercials on a taped television show violated the broadcaster's copyright.

37. Clark & Vaida, supra note 23.

38. For example, the motion picture industry's practice of delaying the release of movies outside the United States until their first run is completed in the United States stimulates foreign demand for infringing copies. This practice of delayed foreign release is a function of the high cost of producing projection quality prints of film. Instead of making enough prints of a movie to use in theatres worldwide, most studios make enough prints for U.S. theatres, and then ship the prints abroad once the United States run is over. The motion picture industry could make more prints, but it doesn't want to bear that cost. Alternatively, the motion picture industry could shift to digital projectors, which would eliminate the need for expensive prints of the films. However, the movie theatres are not willing to bear the significant cost of purchasing digital projectors – $1 million per projector – and the studios are not willing to subsidize the cost of the transition. The information technology industry also noted that the motion picture industry has not aggressively pursued a customer-friendly online music distribution system. KPMG recently issued a report concluding that entertainment companies have placed insufficient energy and resources into developing new business models for the online distribution of content. Further, the study argued that innovative business models would be far more effective in reducing piracy than increased enforcement. See Reuters, KPMG Study Faults Entertainment Companies' Focus on Piracy, MERCURY NEWS (San Jose), Sept. 24, 2000, available at http://www.siliconvalley.com/mls/siliconvalley/news/editorial/4144404.htm.

Because of the controversy, the Hollings Bill made no progress. Instead, attention shifted to narrower proposals, such as the "broadcast flag." Under the broadcast flag approach, a digital watermark would be included in digital television signals broadcast over the air. Receiving equipment would be legally required to comply with this broadcast flag's instructions. Even this approach proved too controversial for Congress, and Senator Hollings and House Energy and Commerce Committee Chairman Billy Tauzin requested that the FCC conduct a rulemaking to determine whether to adopt the broadcast flag or some other copy protection system for digital television. The FCC has begun this rulemaking proceeding. In the wake of the controversy, senior leaders of the entertainment and technology industries have exchanged letters and held meetings in an effort to heal the wounds. However, much suspicion and acrimony remains.

B. The Biden Bill

Senator Biden of Delaware introduced S. 2395, the Anticounterfeiting Amendments of 2002, to extend existing anti-counterfeiting laws to holograms placed on packaging or embedded in the face of CDs and DVDs. Additionally, S. 2395 was intended to improve enforcement of the criminal anti-counterfeiting provisions by granting a private cause of action. Largely in response to lobbying by entertainment companies, however, the Senate Judiciary Committee broadened S. 2395 considerably. As passed by the Judiciary Committee in July 2002, the bill also applies to digital watermarks (e.g., identifying strings of 0s and 1s embedded in computer code). This means that the copying and transmitting of digital works could trigger liability under S. 2395. Thus, S. 2395 places an additional layer of criminal and civil liability on top of activities currently regulated by the U.S. Copyright Act. This new legislative overlay prohibits activity specifically permitted by the copyright law or imposes significantly higher penalties for technical copyright infringements. For example, while copyright protects databases, it does not protect individual facts within a database. S. 2395, however, might prohibit the extraction of watermarked facts from computerized databases. This could threaten a wide range of economic activity and scientific research.

Likewise, copyright permits the reproduction of interface specifications essential for interoperability. S. 2395, however, might allow a dominant software platform publisher to use digital watermarks in a manner that frustrates legitimate competition. A company could

42. Id.
design its software platform to permit applications to run on the platform only if they contain a digital watermark licensed by the company. An independent software company would violate S. 2395 if it copied the watermark solely for the purpose of allowing its original application to run on the platform.

S. 2395 could also harm the non-profit sector. The Copyright Act permits the limited copying of works in a wide variety of academic, library, and private consumer settings. S. 2395 would prevent these reproductions to the extent they involve making copies of works containing digital watermarks.\footnote{S. 2395's consideration requirement would be easily met because libraries often receive reimbursement for the costs involved in making copies for interlibrary loans, and scholars frequently exchange materials of mutual interest.}

In addition, S. 2395 creates inconsistencies with the remedies available under the Copyright Act. Title II of the DMCA limits the remedies that can be obtained against Internet service providers ("ISPs") for the infringing activities of their users. S. 2395 could be applied in a manner that defeats the DMCA's safe harbors, thereby exposing ISPs to remedies not available under the DMCA. Similarly, S. 2395 would impose more severe criminal penalties than the Copyright Act for identical behavior. Criminal liability under the Copyright Act attaches only for willful infringements that result in private financial gain or copies with a retail value of more than $1,000. By contrast, distributing a copy of even one song containing a digital watermark could trigger criminal liability under S. 2395. Thus, S. 2395 could lead to criminal sanctions for minor infringements, notwithstanding the bill's stated purpose of targeting "organized criminal enterprises [that] threaten [ ] the economic growth of United States copyright industries . . . ." S. 2395 also would impose more severe civil penalties than the Copyright Act for identical conduct, such as the potential for greater statutory damages and treble damages for repeat offenders.

Finally, S. 2395 could have the practical effect of requiring consumer electronics and computer manufacturers to reconfigure their products to respect instructions contained in digital watermarks. This would undermine the "no mandate" provision of Title I of the DMCA. In sum, S. 2395 has evolved into an extremely one-sided piece of legislation. It attempts to address the interests of one set of stakeholders—entertainment companies—without any consideration of its impact on other stakeholders.

C. The Berman Bill

In July 2002, Congressman Howard Berman of California introduced H.R. 5211, The P2P Piracy Prevention Act of 2002, to create a safe harbor for self-help activities targeted at frustrating the
unauthorized distribution of copyrighted content over peer-to-peer networks such as KaZaA and Morpheus. The philosophy underlying the legislation is that because P2P networks function without a central server like Napster, normal civil enforcement mechanisms do not work effectively to prevent copyright infringement. Since Napster users could share files only by using the Napster server, record companies succeeded in stopping unlawful file sharing over the Napster network by suing one defendant – Napster. In contrast, once users download P2P software such as KaZaA or Morpheus, the users can share files directly without returning to the KaZaA or Morpheus Web site. Thus, even if the record companies ultimately prevail in their litigation against KaZaA and Morpheus, the file sharing will continue. The transaction costs of suing the millions of P2P file traders would be prohibitive. Accordingly, the Berman Bill authorizes copyright owners to employ self-help technologies to interfere directly with the infringement on P2P networks.\textsuperscript{44}

Specifically, the bill provides that a copyright owner shall have no criminal or civil liability for "disabling, interfering with, blocking, diverting, or otherwise impairing" the unauthorized distribution of his copyrighted work on a "publicly accessible peer to peer file trading network...." This safe harbor does not apply, however, to an impairment that, without authorization, "alter[s], delete[s], or otherwise impair[s] the integrity of any computer file or data residing on the computer of a file trader." This limitation prevents the copyright owner from hacking into the file trader's computer and deleting or impairing the infringing copy.\textsuperscript{45}

At least two ways exist to impair the unauthorized distribution of works over P2P networks without hacking into the file trader's computer: spoofing and denial of service attacks. Spoofing – transmitting files that appear to contain the infringing content people want but which instead contain other content (e.g., a notice that lawful copies are available at a certain Web site) – arguably violates no law and thus requires no safe harbor. By contrast, denial of service attacks require a safe harbor from the federal Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, as well as state computer crime laws.

\textsuperscript{44} When Congress adopted the USA-PATRIOT Act in the wake of the September 11, 2001, terrorist attacks, it increased the criminal penalties under the Computer Fraud and Abuse Act. As Congress was deliberating these CFAA amendments, the entertainment industry attempted to obtain a broad exception from the CFAA for actions taken to protect their copyrights. Congress rejected this request.

\textsuperscript{45} This limitation on deleting files from the file trader's computer might be easy to circumvent. If copyright owners start to embed click-on and "browse-wrap" licenses in their content, a file trader that downloads a file may "agree" to permit the copyright owner onto his computer to delete the file if it is infringing. At that point, the safe harbor would apply because the copyright owner has the file trader's "authorization."
The safe harbor has several other limitations. First, the safe harbor does not apply if the copyright owner impairs the availability of non-infringing content, "except as reasonably necessary to impair the distribution" of infringing content. The bill's supporters argue that this means that the copyright owner can only launch a denial of service attack that prevents access to the infringing copy alone — unless of course, the only way to prevent access to the infringing copy is to prevent or impede the file trader's access to the Internet.

Second, the safe harbor does not apply if the copyright owner's actions cause economic (i.e., monetary) loss to any person other than the file trader. Third, the safe harbor does not apply if the copyright owner's actions cause monetary loss of more than $50 per impairment to the property of the file trader, other than loss relating to the infringing copies. Finally, the safe harbor does not apply if the copyright owner does not provide the U.S. Department of Justice with notice of the specific technology it intends to use to impair the unauthorized P2P distribution. Significantly, the copyright owner does not need to notify the Justice Department of whom the copyright owner is attacking.

If the copyright owner's denial of service attack does not fall within the safe harbor, he can be liable under the Computer Fraud and Abuse Act and any other applicable remedies. Additionally, the Berman Bill creates a new cause of action for wrongful impairment. As a practical matter, however, this cause of action has little value because of all the procedural hurdles a prospective plaintiff must overcome. One can bring a wrongful impairment action in federal court only if: (1) the copyright owner impairs the distribution of a particular file; (2) the copyright owner had no reasonable basis to believe that the distribution was a copyright infringement; (3) the file trader suffered a monetary loss in excess of $250; (4) the file trader files a claim for wrongful impairment with the Attorney General; and (5) the Attorney General either investigates the claim and concludes that there is reasonable cause to believe that the facts alleged by the file trader are true, or the Attorney General fails to make a finding within 120 days of receiving the claim. Moreover, the Attorney General can bring suit against a copyright owner "that has engaged in a pattern or practice of impairing . . . distribution . . . without a reasonable basis to believe that infringement of copyright has occurred."

The bill contains many serious problems. The class of people who could use the self-help remedies is enormous. Anyone who has ever written something down is a copyright owner. The safe harbor gives a green light to this large class to launch denial of service attacks. Some of these attacks will fall within the safe harbor and others will not. But even if they don't fall within the safe harbor and the victim can sue the copyright owner, the damage is done. Moreover, as a practical matter, few victims would sue because it would not be economically worthwhile.
Even if they did want to sue, they typically would not know whom to sue: the copyright owner has no obligation to provide its identity to the victims of its denial of service attacks. Additionally, the Berman Bill would place a large burden on Internet service providers. Victims of denial of service attacks will first turn to their Internet service provider to determine why they can’t access the Internet. The service provider will then need to expend significant resources to determine the cause and source of the impairment.

Relatedly, service providers have been upgrading their systems since the 9/11 terrorist attacks in the United States to detect and prevent cyberterrorism, including denial of service attacks. Until now, the assumption has been that all denial of service attacks are unlawful and require a response. The bill will completely undermine this approach. Now, before responding to the attack, the service provider will have to determine whether it is a legitimate or illegitimate attack. Also, the volume of attacks will increase dramatically. The net effect will be to significantly delay service providers’ response time to serious illegitimate attacks.

Finally, the bill provides content owners with an incentive to monitor user activity on P2P networks, looking for traders of infringing material. This monitoring runs contrary to recent efforts to increase privacy protection on the Internet.

In short, the Berman Bill provides a significant benefit to one set of stakeholders – entertainment companies – with little consideration of its impact on other stakeholders – the Internet service providers and innocent users who are harmed by denial of service attacks on real or suspected file traders. Moreover, the potential for harm to the Internet far exceeds the proven threat that P2P networks pose to entertainment companies.

D. Search Engine Cases

The three pieces of legislation discussed above all reflect overreaching by content providers. Because the bills do not attempt to balance the interests of all stakeholders, the U.S. Congress probably will never enact any of them in their current form. The threat they pose to the Internet and the information technology industry will hopefully never become a reality.

Unfortunately, several recent judicial decisions in the United States and the European Union pose a real danger to the Internet. In these cases, plaintiffs have succeeded in convincing courts to extend existing legal doctrines to prevent the operation of search engines, a critical Internet function.
1. *Kelly v. Arriba Soft*

Arriba Soft developed a search engine for images on the Internet. Its bot crawled the web looking for images, which were then downloaded into Arriba's server and indexed. When a user requested a certain kind of image, Arriba presented it with a group of small "thumbnail" images responsive to the query. The user could not enlarge a thumbnail image on the Arriba server without losing resolution. When the user clicked on a particular image, an inline link was formed, so the user saw the full size image from the original Web site, plus a frame and banner ad from the Arriba Web site. Arriba's search engine included photographs posted on the Web by Kelly, a photographer. He sued Arriba for copyright infringement, and the district court ruled that the thumbnail images were a fair use. Kelly appealed, and the U.S. Court of Appeals for the Ninth Circuit affirmed in part and reversed in part.

The Ninth Circuit affirmed the district court's fair use finding concerning the thumbnail images. The court concluded that the Arriba search engine made a transformative use of the images, and that the thumbnail images did not harm the market for the originals because they could not be enlarged without losing resolution. The problem is with the court's holding concerning the inline linking. The court concluded that this violated Kelly's public display right. The court stated: "By allowing the public to view Kelly's copyrighted works while visiting Arriba's web site, Arriba created a public display of Kelly's works." The flaw in the court's reasoning is that Kelly's Web site is displaying the photos, not Arriba's. Arriba is just directing the user to Kelly's site. If Arriba violated Kelly's display rights, then arguably every search engine or directory violates the display rights of the sites to which it links if it does so without the linked site's authorization.

Some of the court's language implies that the holding is limited to inline linking and framing, and not all linking - that is, there is an infringement here because the framing on the Arriba site creates the illusion that it is displaying the image: "Arriba actively participated in displaying Kelly's images by trolling the web, finding Kelly's images, and then having its program inline link and frame those images within its own Web site. Without this program, users would not have been able to view Kelly's images within the context of Arriba's site." In other words, the problem is not viewing Kelly's images, but viewing them "within the context of Arriba's site." And indeed, the context is completely different. On Kelly's site, the image is surrounded by Kelly's text explaining the image; in contrast, on Arriba's site, the image is surrounded by advertisements.

46. *Kelly v. Arriba Soft Corp.*, 280 F.3d 934 (9th Cir. 2002).
47. *Id.* at 946.
48. *Id.* at 947.
However, if the court were truly concerned about the framing, it should have relied on the right to make a derivative work, rather than the display right. Arguably, Arriba created a derivative work without authorization when it framed Kelly's images. But, by relying on the display right rather than the derivative works right, the court significantly broadened the holding and placed all search engines that link to other sites in jeopardy. Taking the decision to its logical conclusion, every unauthorized link could infringe the display right of the owner of the linked site. Hopefully, subsequent courts will limit the Arriba Soft holding to its facts, and will focus on the framing rather than the linking. Otherwise, the decision will cast a very long shadow over search engines and hyperlinking.

2. eBay Inc. v. Bidder’s Edge, Inc.

In Kelly v. Arriba Soft, the court found unlawful conduct in the unauthorized linking to another site. In eBay, Inc. v. Bidder’s Edge, Inc., the court found unlawful conduct in the gathering of the information on which to base the links.

Bidder’s Edge (“BE”) was an “auction aggregator” that combined the auction listings from numerous online auction sites so that a user could go to one site to see what was available on all the sites, rather than making separate visits to each auction site. If the user decided to place a bid in a particular auction, the user was hyperlinked to the site where that auction was occurring. To obtain the auction listings from eBay and the other auction sites, BE used software “web crawlers” that made multiple queries of the eBay auction database—sometimes as many as one hundred thousand times per day. Upon learning of BE’s Web crawling, eBay demanded that BE stop, but BE nonetheless continued. eBay filed suit, alleging numerous causes of action, including trespass to chattels. The U.S. District Court for the Northern District of California granted eBay a preliminary injunction, concluding that it was likely to prevail on the merits of its state trespass to chattels claim.

To prevail in a trespass to chattels action, the plaintiff must show (1) that the defendant intentionally interfered without authorization with the plaintiff’s possessory rights in personal property, and (2) that the interference resulted in damage to the plaintiff. This ancient English common law doctrine was first applied to cyberspace in spam cases, where Internet service providers were searching for a legal mechanism to stop marketers from flooding their systems with millions of unsolicited commercial emails.


50. When these early spam cases were brought, there were few, if any, laws regulating spam. Now, over twenty states have enacted statutes that regulate spam in some manner. Federal spam bills have been introduced in Congress, but have not yet been enacted.
Ruling in favor of eBay, the court first considered whether BE's use of eBay's site was unauthorized. BE argued that it could not trespass upon eBay's site because the eBay site is publicly accessible. The court ruled that eBay granted only conditional access to its site, and that BE grossly exceeded those conditions by making repeated queries. Additionally, eBay specifically asked BE to stop its Web crawling. The court further ruled that BE's repeated queries interfered with eBay's possessory interest. While eBay likely would not be able to show a substantial interference, all it needed to demonstrate was that BE intermeddled or made use of its property.

Turning to the question of whether BE's use caused damage, the court ruled that a decline in the condition, quality, or value of the property in question constitutes damage. The quality or value of the property can be diminished even if it is not physically damaged. eBay claimed that BE's queries consumed valuable bandwidth and server capacity, "necessarily compromising eBay's ability to use that capacity for its own purposes." BE responded that its searches represented a negligible load on eBay's system, using less than 2% of eBay's capacity. The court ruled that "[e]ven if, as BE argues, its searches use only a small amount of eBay's computer system capacity, BE has nonetheless deprived eBay of the ability to use that portion of its personal property for its own purposes." The court held that the mere interference with a possessory interest is sufficient to establish damage. The court thus collapsed the two prongs of the trespass to chattels test into one.

At the same time, the court appeared uncomfortable with its finding that BE's mere use of the site caused injury. Accordingly, the court speculated as to the injury that would result if it did not stop BE:

If the court were to hold otherwise, it would likely encourage other auction aggregators to crawl the eBay site, potentially to the point of denying effective access to eBay's customers. If...other aggregators began to crawl the eBay site, there appears to be little doubt that the load on eBay's computer system would qualify as a substantial impairment of condition or value.

The court therefore implicitly acknowledged that BE really did not cause eBay any harm, but that eBay would be harmed if many aggregators behaved in the same manner as BE.

The court's open-ended holding places any firm that uses bots to search the Web at risk. Popular Web sites that control a substantial market share can use the Bidder's Edge rationale to exclude outside searches and thereby prevent easy comparison shopping by consumers.

---

51. Bidder's Edge, 100 F. Supp. 2d at 1070.
52. Id. at 1071.
53. Id.
54. Id.
55. Id. at 1071-72.
Instead, a large group of consumers will decide that it is easier to just visit the market leader's site. This ability by market leaders to erect barriers to searches will frustrate the Internet's ability to provide what economists call perfect information to consumers, and thus will retard the growth of e-commerce.56


In 1996, the European Union adopted a database directive that prevents a person from extracting or reusing a qualitatively or quantitatively substantial part of another person's database.57 The member-state implementations of the Directive have been used in several cases to prevent the operation of specialized search engines that link users to various sites containing the information they seek.58

For example, a German court recently ruled that an online news search engine that allowed users to search and link to 100 online newspapers and databases likely violated the German implementation of the Directive. This constituted a violation because the search engine extracted the newspapers' headlines so that a user could determine whether to view the story.59 Likewise, a Danish court ruled that a search engine's repeated scouring of newspapers' Web sites to compile lists of headlines and links violated Denmark's implementation of the Directive.60 Search engine operators have had to defend themselves against similar charges in the Netherlands, but fortunately Dutch courts have not interpreted the Directive as strictly as their German and Danish counterparts.61

E. The Boucher-Doolittle and Lofgren Bills

The legislation and judicial decisions discussed above all lean in the direction of overprotection. Perhaps proving Newton's third law of

56. No court has imposed liability under the federal Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030 (2002), in a search engine case. Holdings in other cases, however, suggest that the CFAA could be used in this manner. See, e.g., EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 581 (1st Cir. 2001).
58. Some database publishers have attempted to convince the U.S. Congress to adopt database protection legislation similar to the EU Database Directive. See Jonathan Band & Makoto Kono, The Database Protection Debate in the 106th Congress, 62 OHIO ST. L.J. 869 (2001). If legislation of this sort is enacted, we could expect even more legal attacks on search engines.
59. See German Court Declines to Disturb Ruling That Search Engine's Links Violated Database Law, 7 ELEC. COM. & L. REP. (BNA) 761, 776 (July 31, 2002).
motion that for every action there is an equal and opposite reaction, at the end of the 107th Congress, Representatives Boucher, Doolittle, and Lofgren introduced interesting bills that responded to their perception that copyright law had tilted too far in the direction of the content producers, and that Congress needed to restore the appropriate balance.

1. The Boucher-Doolittle Bill

On October 3, 2002, Congressmen Boucher and Doolittle introduced the Digital Media Consumer's Rights Act, H.R. 5544, which contained two major provisions. First, the bill would require record companies to label CDs that were copy-protected or that would not play on certain devices such as the CD drives of personal computers. During 2002, record companies started to use various forms of copy protections on their CDs without notifying consumers. Consumers bought the CDs, and when the consumers couldn't play the CDs on their computers or burn copies of them, the consumers assumed that either the CDs or their computers were malfunctioning. The labeling requirement in the Boucher-Doolittle bill is intended to prevent this form of customer confusion.

Additionally, the Boucher-Doolittle Bill would amend the United States’ implementation of the WIPO treaties. Section 1201(a)(1) of WIPO prohibits the circumvention of access controls, even if done for a noninfringing purpose, unless the circumvention is specifically permitted by one of the exceptions contained in Section 1201. Likewise, Sections 1201(a)(2) and 1201(b) prohibit the manufacture and distribution of circumvention devices, even if they are intended to be used for non-infringing purposes, unless the devices fall within Section 1201’s specific exceptions. In other words, Section 1201 prohibits circumvention activity and devices, regardless of whether the circumvention results in infringement.

In introducing their bill, Congressmen Boucher and Doolittle recognized that by divorcing circumvention from infringement, Section 1201 had the effect of prohibiting lawful uses of copyrighted works. Thus, although Section 1201(c)(1) provided that Section 1201 did not affect defenses to copyright infringement, including fair use, fair use was not a defense to a circumvention offense.62 Accordingly, Congressmen Boucher and Doolittle proposed amendments that would make noninfringement a defense to circumvention liability.

Specifically, their bill would amend Section 1201(c)(1) to provide that “it is not a violation of this section to circumvent a technological protection measure in connection with access to, or use of, a work if such circumvention does not result in an infringement of the copyright in the

work." Likewise, the bill would create a new Section 1201(c)(5) that
provides that "[i]t shall not be a violation of this title to manufacture,
distribute, or make noninfringing use of a hardware or software product
capable of enabling significant noninfringing use of a copyrighted
work." This provision borrows the "substantial noninfringing use
standard" for contributory infringement from Sony Corp. of America v.
Universal City Studios, Inc., and applies it to the circumvention context.

Further, the Boucher-Doolittle Bill creates an exception to the
prohibition on the manufacture and distribution of circumvention
devices when "the person is acting solely in furtherance of scientific
research into technological protection measures." This provision codifies
an argument made by the U.S. Department of Justice during the
declaratory judgment action brought by Princeton University Professor
Edward Felten against the Recording Industry Association of America
("RIAA"). Felten sought a judicial declaration that his encryption
research was lawful, and the RIAA responded that the case was moot
because the RIAA had withdrawn its objections to his research. The
Justice Department filed an amicus brief in support of the RIAA that
argued, inter alia, that Felten's research was plainly permitted by the
DMCA. In particular, the Justice Department argued that since Felten
developed his software tools for research purposes, he obviously did not
develop them "for the purpose of circumventing a technological measure
that effectively controls access to a work protected by this title." 17
U.S.C. § 1201(a)(2)(A). In other words, even though Felten's tool
circumvented a technological measure, the actual purpose of the tool was
research, not circumvention.

Shortly after the introduction of the Boucher-Doolittle Bill,
companies such as Intel, Philips, Sun Microsystems, Verizon, and
Gateway announced their support, along with associations such as the
American Library Association, Consumers Union, and the Electronic
Frontier Foundation. Content providers condemned the bill, asserting
that the new exceptions would swallow the circumvention prohibition.

64. Id. at § 5(b)(2).
66. For a first-hand perspective, see Edward W. Felten, The Digital Millennium Copyright Act
67. Interestingly, soon after the introduction of the Boucher-Doolittle Bill, Richard Clarke, the
head of the White House Office of Cyber Security, stated that the DMCA needed amendment to
permit the research of security flaws in software. He termed threats against academic researchers as a
misuse of the law, and said "I think a lot of people didn't realize that it would have this potential
chilling effect on vulnerability research." Hiawatha Bray, Cyber Chief Speaks on Data Network
2. **The Lofgren Bill**

On October 2, 2002, Congresswoman Lofgren also introduced a bill directed at Section 1201 of the DMCA – the Digital Choice and Freedom Act of 2002, H.R. 5522. The Lofgren Bill, however, took a somewhat more narrow approach than the Boucher-Doolittle Bill. Under the Lofgren approach, a person could circumvent an access control if the circumvention was "necessary to make a noninfringing use of the work" and "the copyright owner fails to make publicly available the necessary means to make such noninfringing use without additional cost or burden to such person." Similarly, a person may manufacture and distribute the means to circumvent a technological measure if the "means are necessary to make a noninfringing use," the means are "designed, produced, and marketed to make a noninfringing use," and "the copyright owner fails to make available the necessary means . . . ." But the Lofgren Bill does not detail how a copyright owner's failure to make available the means of circumvention would operate.

The Lofgren Bill contains several other provisions unrelated to circumvention. The general thrust of these provisions is to preserve in the digital environment exceptions that exist in the analog environment. Thus, the bill would create a new Section 123 that permits a person who lawfully obtains a copy of a digital work "to reproduce, store, adapt, or access the digital work . . . for archival purposes . . . and . . . in order to perform or display the work, or an adaptation of the work, on a digital media device, if such performance or display is not public." This provision codifies the practice of "time-shifting" and "space-shifting" practiced by many consumers.

Additionally, the new Section 123 would provide that "[w]hen a digital work is distributed to the public subject to nonnegotiable license terms, such terms shall not be enforceable . . . to the extent that they restrict or limit any of the limitations on exclusive rights . . . ." This provision is intended to invalidate shrink-wrap or click-on license terms that restrict fair use and other privileges that Congress has granted to consumers. Significantly, Section 123 would not apply to software, which is excluded from the definition of "digital works." Finally, the Lofgren Bill would update the first sale doctrine for the digital age. A person could transmit a work to another person provided that he deleted his copy of the work.

3. **The Cox Resolution**

The week after the introduction of the Boucher-Doolittle and Lofgren Bills, Congressman Cox introduced House Joint Resolution 116. The resolution creates a "Consumer Technology Bill of Rights" which "sets forth the rights of all Americans to personal control of information and entertainment content that they have lawfully acquired and from
which they do not intend to profit.” The Consumer Technology Bill of Rights sets forth six separate rights: the right to time-shift; the right to space-shift; the right to make back-up copies; the right to use content on different electronic platforms; the right to translate content into comparable formats; and the right to use technology in order to achieve the other five rights.

The Consumer Technology Bill of Rights does not actually create any rights in a legal sense. A joint resolution does not establish law; rather, it is an expression of the “sense of Congress.” In essence, a joint resolution is a political statement. If adopted, the resolution would express Congress’s belief that “consumers who legally acquire copyrighted and non-copyrighted works should be free to use these works in non-commercial ways.” Presumably, Congressman Cox hoped that the adoption of the resolution would place political pressure on members of Congress who would otherwise be tempted to introduce legislation that would contravene the Consumer Technology Bill of Rights. Additionally, the Consumer Technology Bill of Rights might influence courts in their interpretation of the copyright law generally and the fair use doctrine in particular.

Because both bills and the joint resolution were introduced so late in the session, no action could be taken on them before Congress adjourned for the 2002 elections. However, the sponsors of both bills stated that they intended to reintroduce the legislation in the next Congress. Congressman Cox likely will reintroduce his joint resolution as well.

IV. CONCLUSION

Judge Kozinski of the U.S. Court of Appeals for the Ninth Circuit has written that:

Overprotecting intellectual property is as harmful as underprotecting it. Creativity is impossible without a rich public domain. Nothing today, like nothing since we tamed fire, is genuinely new: Culture, like science and technology, grows by accretion, each new creator building on the works of those who came before. Overprotection stifles the very creative forces it’s supposed to nurture.

This is why intellectual property is full of careful balances between what’s set aside for the owner and what’s left in the public domain for the rest of us. . . .

In the digital era, we must remember these wise words. The threat of copyright infringement on the Internet motivates content providers to

seek ever more intellectual property protection. But, legislators must make sure that any new protection granted is in fact warranted – that it will effectively address a demonstrated harm and that it will not cause serious collateral damage to the operation of the Internet or to user expectations.

The recent actions of the Japanese government – the report of the METI task force, the service provider safe harbors, and the WIPO treaties implementation – all reflect an appreciation for the importance of balance. Significantly, both the service provider safe harbors and the WIPO implementation are modeled on earlier United States and European Union legislation that similarly evidenced a balanced approach. In contrast, some of the recent legislative proposals in the United States depart from these precedents. Because of these proposals’ one-sided nature, the United States Congress probably will not adopt them. However, we are not completely out of the woods. Courts in the United States and the European Union are applying existing statutes and legal doctrines in a manner that threatens the viability of search engines. Hopefully, courts will correct this situation before legislative intervention becomes necessary.