January 2004

Deconstruction a Robotic Toy: Unauthorized Circumvention and Trafficking in Technology

Katherine C. Hall

Follow this and additional works at: http://digitalcommons.law.scu.edu/chtlj

Part of the Law Commons

Recommended Citation

Available at: http://digitalcommons.law.scu.edu/chtlj/vol20/iss2/5

This Article is brought to you for free and open access by the Journals at Santa Clara Law Digital Commons. It has been accepted for inclusion in Santa Clara High Technology Law Journal by an authorized administrator of Santa Clara Law Digital Commons. For more information, please contact sculawlibrarian@gmail.com.
DECONSTRUCTING A ROBOTIC TOY:
UNAUTHORIZED CIRCUMVENTION AND TRAFFICKING IN TECHNOLOGY

Katherine C. Hall†

I. ABSTRACT

Section 1201(a) of the Digital Millennium Copyright Act governs legal protection for "access control" technologies that safeguard intellectual property in digital and analog form. The provision creates a new tort that is separate from copyright infringement. Illegal conduct may be subject to civil remedies or criminal penalties, depending on a defendant’s intent. This survey article applies § 1201(a) to published facts about a toy hack in order to analyze the statute’s structure and language. The article is written for non-specialists. It provides basic vocabulary and concepts, making the statute widely accessible and offering an early view of potential issues.

† The author thanks Professor Lackland Bloom, Dedman School of Law, Southern Methodist University, Dallas, Texas for sponsoring and encouraging the directed research that led to this article; Peter van der Linden, Jeffrey Gibbons, Andrew Staats, The Furby Coroner, Furby Autopsy at phobe.com, and Alan Freedman, author of The Computer Desktop Encyclopedia for gracious permission to quote from their works; and the enthusiastic and helpful Editors of the Santa Clara Computer and High Technology Law Journal. The author gained immeasurably from all who encouraged this research and especially from the international law students who attended the Dedman School of Law in 2000-2001 and who shared information about how their own legal systems work. The author dedicates this article to her beloved family and friends. The SMU Underwood Law Library, Dallas, Texas has been provided with a notebook containing a print-out of all Internet resources cited in this article, including those on file with the author. Sources cited are current as of December 2003. The author can be contacted at khall@smu.edu.
II. INTRODUCTION

Intellectual property pirates annually divert billions of dollars from businesses all over the world. They sell and give away illegal copies of software, movies and songs, transferring creative works across the Internet in a ceaseless flow of data. Copyright owners struggle to protect their works, using encryption and other technological measures to control access and copying. But experience teaches that all these measures may be evaded.

The United States Congress enacted the Digital Millennium Copyright Act\(^1\) ("DMCA" or "Act") to supplement technological safeguards with legal protection. Although the Act became effective October 28, 1998,\(^2\) Congress delayed the effective date of § 1201(a)(1) until October 28, 2000.\(^3\) Subsection 1201(a)(1) provides "No person shall circumvent a technological measure that effectively controls access to a work protected under this title." Subsection (a)(2) prohibits manufacturing, importing, offering to the public, providing or otherwise trafficking in technologies that are created, used or marketed to circumvent technological measures ("trafficking in technology").\(^4\) Few courts have interpreted these provisions.

This article explores how the statute works, analyzing the published details of efforts to hack and alter the operations of a life-like computerized toy. The article presents basic vocabulary and

---


4. The words "trafficking" and "traffic," and their associated forms, play two important roles. Sections 1201(a)(2) and 1201(b) prohibit certain conduct, using the verbs: "manufacture, import, offer to the public, provide, or otherwise traffic." In that context, the verb "traffic" has a specific meaning. See definitions infra notes 222 and 223. "Traffic" may also refer generally to the subject matter of the cited subsections, which some have labeled the "anti-trafficking provisions". Universal City Studios, Inc. v. Corley, 273 F.3d 429, 440 (2d Cir. 2001). Cf. HOUSE COMM. ON THE JUDICIARY, 105TH CONG., SECTION-BY-SECTION ANALYSIS OF H.R. 2281 AS PASSED BY THE UNITED STATES HOUSE OF REPRESENTATIVES ON AUGUST 4, 1998, at 9 (Comm. Print 1998) [hereinafter SECTION-BY-SECTION ANALYSIS OF H.R. 2281] ("trafficking" used to refer to §§ 1201(a)(2) and 1201(b)). In the latter context, these words serve as an abbreviated reference to all of the conduct covered by the two subsections.
concepts for non-specialists. The goal is to seek a logical, methodical way to apply the statute. The analysis focuses on a copyright owner's ability to protect his literary work, source code,\(^5\) embodied on epoxy-coated microchips as object code.\(^6\) The article comments on historical background, notes evolving technological vocabulary, and examines the foundational elements that plaintiffs must prove, i.e., the existence of a "protected work" and a "technological measure." It then considers the elements of illegal conduct (unauthorized circumvention and trafficking in technology), touching briefly on civil remedies and criminal penalties for that conduct.

III. BACKGROUND

Copyright laws often fail to protect digital works effectively.\(^7\) Laws developed decades ago were not designed to address digital

---

5. "Source code" is defined as "[p]rogramming statements and instructions that are written by a programmer. Source code is what a programmer writes, but it is not directly executable by the computer. It must be converted into machine language by compilers, assemblers or interpreters." ALAN FREEDMAN, COMPUTER DESKTOP ENCYCLOPEDIA CD-ROM, version 16.4, current through Fourth-Quarter 2003, available at www.computerlanguage.com/. Reproduced with permission from Computer Desktop Encyclopedia © 1981-2003 The Computer Language Co., Inc.

6. "Machine language," called "object code" by early programmers, is essential because a "computer only understands machine language, which is a set of instructions built into its circuits and is specific to that CPU model or family. The programs that it executes are made up of binary-coded instructions in that machine language..." FREEDMAN, supra note 5 (emphasis added). Software, which is re-programmable and can be modified, also consists of instructions for a computer. "A series of instructions that performs a particular task is called a 'program.' The two major categories of software are 'system software' and 'application software.'" Id. (emphasis added to designate elements that may contain original expression protected under title 17 of the U.S. Copyright Act).


The pace of technology was accelerating beyond the point where courts could easily adapt traditional copyright concepts to new challenges created by the emerging digital medium. This is not to suggest that traditional copyright concepts were inadequate, but only that there needed to be clarification and refinement of how they would apply in the digital age).
communications that can cross the world in seconds.\textsuperscript{8} Earlier laws were enacted when unauthorized reproductions (of print, film or audiotape) resulted in inferior copies. Digital reproductions, however, can give rise to identical and virtually identical copies every time. The millionth copy of software can perfectly duplicate the first. Moreover, by merely tapping on a keyboard, unauthorized persons can start, literally in the blink of an eye, the distribution of millions of perfect copies across multiple channels of distribution, including the Internet. Analog works, also protected under the statute, can be converted to, and distributed in, digital form. The ability to transmit millions of reproductions at lightening speed serves, in essence, to compress commercial time. This alters product availability and costs, affecting economic relationships and opportunities all over the world. Manufacturers and producers, among others, can obtain commercial control of all of these works as if the person who authored the creative original work of authorship did not even exist.

These changes affect consumer markets. Given the choice of a perfect "original" or a perfect pirated reproduction at little or no cost, millions of consumers now refuse to pay for the copyright owner's version. This reverses traditional purchasing patterns. It can also create financial problems and disincentive for creative people. They must consider the possibility of losing immediate control over their works when choosing whether to produce and market film, music, medical or scientific books, software or other works. Some may conclude that their time is better spent on different activities.\textsuperscript{9} Those who produce original works of authorship, as in past centuries, often seek to protect their works. They rely on technological measures, seeking to obtain compensation for what they have created and to prevent unauthorized access to digital and analog forms of the work.

Other innovative persons, however—whose livelihoods may also depend upon producing original or derivative works of authorship—prefer unrestricted access to information. They have a stake, and

\textsuperscript{8} Moving at the "land-speed record for sending data over the Internet" computer users "could send full-length DVD movies . . . from halfway across the world in less than 20 seconds, or the entire Library of Congress in 14 hours." Press Release, Los Alamos National Laboratory, Internet Speed Mark in Guinness World Records Book (July 24, 2003), http://www.lanl.gov/worldview/news/releases/archive/03-100.shtml.

\textsuperscript{9} See generally Paul A. David and Dominique Foray, Economic Fundamentals of the Knowledge Society, 1 POLICY FUTURES IN EDUCATION 20, 39 (2003), at http://www.triangle.co.uk/pfie/ ("If [creative producers] had no rights enabling them to derive income from the publication of their works, they might create less, and quite possibly be compelled to spend their time doing something entirely different but more lucrative.").
society may have a stake, in the ability to obtain and use information of all kinds. Thus, there is a constant tension between the competing interests of authors trying to protect, and unauthorized users trying to utilize, works that consist of original expression.

People all over the world have debated for years how best to address these problems. The World Intellectual Property Organization ("WIPO") adopted a Copyright Treaty in 1996, requiring legal protection for technological measures, those methods or systems using technology to protect creative works. Subsequently, the United States Congress enacted the Digital Millennium Copyright Act, bringing U.S. law into compliance with the Treaty. The copyright laws, when applicable, continue to protect creative works as before. The new statute adds protection for technological measures that safeguard those works.

Section 1201 does not "affect rights, remedies, limitations, or defenses to copyright infringement, including fair use." Its purpose is to establish "a new kind of legal protection for authors." This applies only to those measures that guard works protected under Title 17 of the U.S. Code, which contains U.S. copyright laws. Section 1201(a), characterized as a form of "paracopyright," protects rights that differ from but are associated with copyright. It bears a

---

10. Id. at 40-41 ("[T]here will be a greater flow of entailed discoveries if the knowledge upon which they rest remains more accessible and widely distributed."). Information users seek unauthorized access to protected works for many reasons. Some intend to engage in conduct that may be permitted under statutory exemptions. See, e.g., 17 U.S.C. § 1201(f) (2000) (reverse engineering of software). Others have different motives. See M.E. Kabay, Ph.D, CISSP, Studies and Surveys of Computer Crime (2001), http://www2.norwich.edu/mkabay/methodology/crime_studies.pdf.

11. Article 11 of the WIPO Copyright Treaty states:

Contracting Parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law.


relationship to other copyright laws that is analogous to the relationship between a lock and the property that it secures.

Subsection (a) defines the scope of protection for access control measures. Civil remedies and criminal penalties apply to conduct that violates this provision. Several other subsections share related vocabulary and concepts, some providing defenses or exceptions to liability. Lack of interpretive guidance hinders analysis for all of these. All require some certainty in applying the law. But certainty is an elusive goal. Copyright owners can safeguard literary and graphic works, movies, video games, and music on a wide range of media, using many kinds of technological measures. Thus, courts will undoubtedly adapt the statute and tailor definitions for particular technologies. Complicating the task, in some fields, such as that of computer security, specialists may not share a common vocabulary. Other protective technologies and the words describing them have yet to be invented.

The world’s legal systems strain to regulate technological activities and markets. Lawmakers urgently try to deal with evolutionary changes before receiving judicial guidance for even obsolete technologies. Because the courts have only begun to address § 1201(a) issues, a process that may take decades, judicial guidance is sparse. The public domain example considered here, however, is available for all to investigate. It provides an opportunity to experiment with statutory analysis, offering an early view of potential issues.

15. 17 U.S.C. § 1201(a)(1)(A) (2000) (unauthorized circumvention); § 1201(a)(2) (trafficking in circumvention devices); § 1201(b) (trafficking related to unauthorized copying); § 1201(d) (exemption for nonprofit libraries, archives and educational institutions); § 1201(f) (reverse engineering ); § 1201(g) (encryption research); § 1201(h) (exceptions regarding minors); § 1201(i) (protection of personally identifying information); and § 1201(j) (security testing).


IV. THE FACTS

Overview

Shortly after the DMCA was enacted, hackers started trying to alter the operations of the Furby, a robotic toy. Two years later, a Canadian computer consultant claimed success. He then advertised upgrade kits, an operating system and software manual on the Internet. His work sometimes brought him to Chicago, Illinois, and he sold products to U.S. purchasers via the Internet. While jurisdictional issues are beyond the scope of this article, U.S. courts would presumably have jurisdiction of U.S. purchasers who duplicated his actions. This analysis assumes that all these persons acted without authority and without any legal right to circumvent or to engage in prohibited dealings in the relevant technologies.

Although many people, such as business rivals, pirates, and engineers, may have tried to access the toy’s source code, only hackers publicized what they did. Using websites and media outlets, they published news releases, instructional text, photos, and other data (referred to as “evidence”). This data offers a useful landscape for mapping how the statute may operate. Public records naturally do not have all vital information so the analysis is illustrative rather than definitive. The facts, however, offer a platform for vigorous debate about § 1201(a) and other issues associated with the conduct described.


20. No “evidence” was provided under oath. “Plaintiffs” and “defendants” herein are hypothetical parties.
The creative spark

David Hampton created a small animated character with artificial vision, hearing, speech, and sensitivity to touch. He used software embodied on computer chips to govern the toy's movements and emission of sound, enabling each toy to give the appearance of interacting with people. Every Furby seemed to have its own personality; if one became angry, another might sing to calm it.

Furby, a patented toy, differed from prior art in several ways. Differences included its miniature size and use of specialized sensors. The sensors enabled it to respond to data gathered from its environment so that it seemed to interact intelligently with children who played with it. Sensors also allowed toys to interact with each other. Earlier toys used cyclical interactions generated by a single direction motor, but Furby's reversible motor controlled the toy's movements with precision in a "non-cyclic life-like manner," simulating different states such as sleep, waking or excitement. The toy's embedded processor and sound generating circuitries gave it the appearance of talking in conjunction with its movements. Using sensors and predetermined inputs, the little robot could learn to play games and do tricks.

Furby was more than just another toy. Hampton, a talented hardware and software engineer, wanted to create something as close to life as possible.

21. See generally Scott Kirsner, Moody Furballs and the Developers Who Love Them, WIRED NEWS, Sept. 6, 1998, http://www.wired.com/wired/archive/6.09/furby.html. The Copyright Office registration names Hampton and Schulz as source code authors. Since all other publications that the author located describe only Hampton's creative activities, this article focuses on his actions.

22. "Chip" is defined as:
A set of microminiaturized, electronic circuits that are designed for use as processors and memory in computers and countless consumer and industrial products. Small chips can hold from a handful to tens of thousands of transistors. They look like tiny chips of aluminum, no more than 1/16" square by 1/30" thick, which is where the term 'chip' came from.

FREEDMAN, supra note 5. Chips are also known as integrated circuits. Id.


24. U.S. Patent No. 6,149,490 (issued Nov. 21, 2000), Summary of the Invention.

25. Id.

26. U.S. Patent No. 6,149,490, supra note 24, Detailed Description of the Preferred Embodiments.

27. Id.

28. See Kirsner, supra note 21 (this article used the pseudonym "Eric" for Hampton).
work from similar alteration, incorporating protective measures in the toy’s design.

**The toy company**

By November 1997, Tiger Electronics of Illinois, Ltd. (“Tiger”) had agreed to help develop and market the toy. Working at top speed and planning retail store deliveries by August 1998, they designed Furby with extraordinary complexity. Tiger planned to create a collectibles market with lots of colorful versions. Hoping to create an enduring and profitable brand, the company manufactured the toy in China, where labor and resources cost less. The toy’s computer chips were laminated with a hard, opaque epoxy resin as a protective measure. Tiger encountered a few legal and public relations problems while developing the toy. The company reportedly paid Warner Brothers a sizeable settlement because Furby’s ears resembled those of another fantasy creature, the Gremlin. Hackers also criticized Tiger harshly, accusing it of employing poorly-paid workers overseas.

**Value of the franchise**

Hasbro, then the world’s second-largest toy company, bought Tiger for $335 million in February 1998. Excited about the toy’s prospects, Hasbro increased its TV advertising budget by $7 million

---

30. Furby was designed to be:
   capable of at least 300 different unique combinations of eye, ear, and mouth movements, all generated by a set of cams driven by a single 8,000-rpm motor and controlled by two microprocessors. The toy would have attitude sensors that could tell whether it was standing or being held upside down. Light sensors would tell it when to go to sleep, a microphone would enable it to respond to sound, and pressure sensors would let it know when it was being petted.  
   *Id.* Microprocessors were reportedly programmed in assembly language code. *Id.*
31. *See id.*
32. Barbie, for decades the dominant brand in the toy industry, generated 40% of Mattel’s total sales. *Id.*
35. Brand, *supra* note 34.
dollars for a total of $70 million that year, promoting Furby heavily.\textsuperscript{37} The toy was a hit. Toys’R’Us ordered half a million.\textsuperscript{38} The suggested retail price in November 1998, was $35.95.\textsuperscript{39} But consumer demand went through the roof. Egift priced the toys first at $99.95 and then at $123.95.\textsuperscript{40} Internet auctions reportedly offered them for hundreds of dollars.\textsuperscript{41} Tiger worked hard to maintain the brand’s significance, offering free email to buyers and celebrating Furby’s one-year birthday with a marching band that paraded down New York’s Fifth Avenue.\textsuperscript{42}

Within a relatively short time, profits began to decline. Even though the fad had waned by Christmas 1999,\textsuperscript{43} Tiger persisted.\textsuperscript{44} TV stations broadcast a children’s public service campaign (“Furby for the Presidency”) for the Fall 2000 U.S. Presidential election.\textsuperscript{45} But major retailers reduced prices from $30 to $15, and by year-end 2000, major retailers were using the toys as $5.00 loss leaders.\textsuperscript{46} Undaunted, Tiger maintained a website, advertising the next generation of interactive playthings built on “the Furby technology.”\textsuperscript{47}

\textit{Uninvited visitors}

The company initially targeted four to eleven-year-old girls as likely purchasers,\textsuperscript{48} later modifying the toy to emit burps and belches to attract little boys. Hackers,\textsuperscript{49} engineers, and artificial intelligence

\textsuperscript{37} Id.
\textsuperscript{39} Bob Brand, Finally, Furby Hacked, THE BEE, Dec. 2, 2000 (on file with author).
\textsuperscript{40} Woody, supra note 38.
\textsuperscript{41} Id.
\textsuperscript{42} THE FURBISH TIMES, Oct. 14, 1999 (on file with the author). This website displayed Furby-related products and news of interest to toy collectors.
\textsuperscript{43} See, e.g., Brand, supra note 39.
\textsuperscript{44} See generally THE FURBISH TIMES, supra note 42.
\textsuperscript{45} THE FURBISH TIMES, July 6, 2000, supra note 42.
\textsuperscript{47} THE FURBISH TIMES, Feb. 23, 2000, supra note 42.
\textsuperscript{48} See Kirsner, supra note 21.
researchers were also interested.\textsuperscript{50} Research labs invest millions to develop robotic devices and Tiger had spent perhaps $5 million developing Furby.\textsuperscript{51} Programmed with 160 or more "words and sounds," the toy could form an estimated 800 to 1,000 phrases.\textsuperscript{52} Hackers who wanted to experiment with its advanced technology created websites to exchange tips.\textsuperscript{53} Peter van der Linden, a software engineer employed by a well-known U.S. company and author of computer programming books, sponsored a "Hack Furby" contest. He offered $250 to anyone who could reprogram the toy\textsuperscript{54} to "emit arbitrary speech and to move through arbitrary motions subject to the physical limitations of the device."\textsuperscript{55} Hackers worked hard and speculated about components. Complaining they could not gain access to the software, they blamed this on the opaque epoxy resin,\textsuperscript{56}

\textsuperscript{50.} Denis Susac, \textit{Furby}, ARTIFICIAL INTELLIGENCE, Oct.13, 1998, About the Human Internet ("robotics enthusiasts . . . can learn about sensors, propulsion and control") (on file with the author).

\textsuperscript{51.} See Kirsner, \textit{supra} note 21.


\textsuperscript{53.} See, e.g., HackFurby.com (on file with the author) and Furby Autopsy, at http://www.phobe.com/furby/.

\textsuperscript{54.} Cook, \textit{supra} note 49.

\textsuperscript{55.} van der Linden, \textit{supra} note 33. Hackers exchanged brainstorming ideas about how to alter the toy:

\begin{quote}
By changing the bits stored in the EEPROM, one could likely change a furby's name, memory, states, crash the processor, etc. But, like the IR spoofing, you can only trigger pre-programmed behavior and not create new vocabulary or actions.

What about 'hacking' the IR communication? Besides the basic switches and digital inputs, the Furby has a source of bi-directional I/O—the IR port. By using remote controls or any other source of IR signals, it is possible to fool the Furby's processor into responding to those signals as if it was another Furby. Of course, you can only trick the Furby into responding to one of its preprogrammed responses — you aren't going to have it speaking Mandarin or swear words this way.
\end{quote}

Furby Autopsy, HackFAQ, \textit{supra} note 53.

\textsuperscript{56.} One hacker wrote:

\begin{quote}
Even if a standard processor or microcontroller design was used, the main processor chip(s) in the Furby are custom made for the Furby. \textit{Under a homely blob of opaque, protective epoxy is a single chunk of IC that includes its CPU, ROM, RAM} (if any), \textit{audio data, and I/O interfaces such as driver transistors, an ADC or a DAC. The Furby's software and sound data is generally inaccessible for reading, disassembly, removal, replacement, or even examination. There are no data/address busses, interrupt lines, surplus i/o lines, etc. other than what is needed to operate the Furby — making it unrealistic for end users to create a new ROM for the Furby.}
\end{quote}
broadcasting the technical details on their websites. They were stumped for two years.

Success at last

Thirty-three year old Canadian Jeff Gibbons, a computer consultant, tried to gain access to the toy’s software and reprogram it for months. He finally used a hardware hack after concluding that the epoxy blocked reverse engineering and reprogramming of the software. The open source software community helped. Chris Brown developed a circuit diagram schematic, which he posted on the Internet; Andy Staats and van der Linden developed a software manual. Other individuals also created websites and posted hacking tips. Media outlets all over the world publicized the event when Gibbons won the “Hack Furby” contest.

Gibbons gained control of the toy by taking several actions. First, he removed the plastic shell covering the computer components and mechanics. Inside were two daughterboards containing

Making a custom chip mask may sound expensive, but remember they are making a few million of these things: the savings in reduced assembly complexity, component supply and mark-up, circuit board size, etc. offsets the initial set-up cost. Additionally, it protects their invention from being easily copied or reverse engineered, since in order to get to the juicy bits, one needs acid, powerful microscopes, lots of time and specialized skills. (Of course, doing this would destroy the chip and ruin any hacking opportunities). For most companies, it would probably be cheaper for them to hire an engineer to design something original.

Furby Autopsy, HackFAQ, supra note 53 (emphasis added to designate language referring to technological measure and awareness of its function).

57. See, e.g., Furby Autopsy, supra note 53.

58. Business rivals with specialized equipment probably gained access quickly. Statutory requirements, though, would be erratic if based on variable resources or skills.

59. Howes, supra note 19; Email from Jeffrey Gibbons to Bob Brand (Nov. 14, 2000 13:56:02 MST), Re: [The Furby Kit] (on file with the author).

60. Peter van der Linden, Outline of User-Programmable Furby [tm], at http://www.afu.com/furby/tech.html; Clive Thompson, Hackers are reprogramming everything from scanners to toys, GLOBETECHNOLOGY.COM, Mar. 2001 (on file with the author).

61. See generally Brand, supra note 39; see also Email from Andy Staats to Bob Brand (Dec. 1, 2000, 23:52:39–0800 (PST)), Re: Furby upgrade kit assembly information (on file with the author).


63. FREEDMAN, supra note 5 ("printed circuit board that plugs into another printed circuit board to augment its capabilities."). A printed circuit board is a flat board that holds chips and other electronic components. The board is made of layers (typically 2 to 10) that interconnects components via copper pathways.
computer chips. Hackers had speculated that these contained a central processing unit, or CPU, and a memory chip. Gibbons desoldered and disconnected the boards, replacing them with new printed circuit boards holding new chips. He published instructional text and photographs on the Internet to show what he had done. He and associates posted programming and systems operation tips, offering samples of downloadable computer code. The new chips enabled anyone to program toy movements and sound emissions.

The human interest in Furby's uses

Educators were also interested. Speculating that "Computer Science departments can now base their real-time programming courses on this very low-cost equipment," van der Linden elicited

The main printed circuit board in a system is called a 'system board' or "motherboard," while smaller ones that plug into the slots in the main board are called "boards" or cards.

Id.

64. "Tiger electronics used what looks like ASIC chips bonded directly to two separate PCB boards. It is these boards, which carry the ASIC chips, that the upgrade kit replaces to make the Furby reprogrammable and add the new InfraRed/ RS-232 capabilities." Furby Background and Quick Technical Overview (on file with the author). ASIC chips "(Application Specific Integrated Circuit)" are "custom designed for a specific application rather than a general-purpose chip such as a microprocessor." FREEDMAN, supra note 5.

65. FREEDMAN, supra note 5 (the "computing part of the computer" which consists of "the control unit and ALU.") The ALU, arithmetic logic unit, calculates and compares. Id.

66. One new pcb held an "Intel-designed 8051 8-bit processor" while the other held "64KB of flash PROM... along with 1K of RAM." See van der Linden, supra note 60; ANDREW STAATS & PETER VAN DER LINDEN, HACKED FURBY [TM] (HURBY) PROGRAMMERS GUIDE, version 1.1, at http://www.appspec.net (products).

67. Originally displayed on the Internet at a website that has disappeared, these are presently maintained at the Furby Upgrade homepage, at http://www.appspec.net/ (products).

68. STAATS and VAN DER LINDEN, supra note 66.

69. See, e.g., Brand, supra note 39.

70. See van der Linden, supra note 62. Educational institutions have limited protection. 17 U.S.C. § 1201(d)(1) (2000) (gaining "access to a commercially exploited copyrighted work solely in order to make a good faith determination of whether to acquire a copy"); 17 U.S.C. § 1203(c)(5)(B)(ii) (2000) (court may reduce or remit damages if "institution... was not aware and had no reason to believe that its acts constituted a violation"); and 17 U.S.C. § 1204(b) (2000) (exempt from fines and imprisonment for criminal conduct). But see § 1201(d)(3) (willful violations for "commercial advantage or financial gain" subject institution to civil remedies and may, for repeated violations, cause it to forfeit exemptions under § 1201(d)(1) and under § 1201(d)(4) (must not "manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, component, or part thereof, which circumvents a technological measure").

71. van der Linden, supra note 62, stated:

The potential for Furby to become a general purpose computing device was immediately obvious. The thing already has a CPU and is bristling with peripherals including infrared I/O, several motion detectors, eye and mouth
both laughter and agreement. A different vision, though, captivated others. An autistic four-year-old boy improved his ability to talk and interact with people by playing with the responsive toy. His mother was searching for an upgraded toy, hoping to help him still more.

_Furby upgrade kits_

Gibbons and Staats advertised a $65.00 Furby upgrade kit on the Internet, later raising the price to $74.00. They sent bulk mailings to potential purchasers. Estimating four hours for hardware assembly, they offered “free programming tools and example code.” They researched commercial possibilities and by early 2001 had sold about 100 kits, shipping them all over the world, including Scotland, Ireland, the Netherlands, and the U.S. Journalists reported that Gibbons hacked the toy for fun and not for profit. He was quoted as saying “I’d be surprised if it kept me in beer money.”

Purchasers obtained hardware and software, hands-on experience, and a chance to learn and have fun. A couple of websites showed how to deconstruct the toy. Kit purchasers then had to program the toy themselves in a difficult-to-use language. Despite some improvements, offers of “basic programming API’s,” and a
software manual, individuals still must do most of their own programming.  

*Potential economic impact*

Gibbon’s total gross revenues through early 2001 probably ranged from $6,500 to $7,400. His “beer money” assessment sounds accurate after inventory, shipping, and other costs. He continues to market Furby upgrade kits. A hi-tech business website with which he is associated links to Paypal where the kits can be purchased. It also links to deconstruction text, photographs, and programming tips. Thus, the Furby hack has been commercialized as a marketing tool. Whether this has generated business for Gibbons or his employer is unknown.

Viewed in isolation, the hack probably did not significantly impact prices charged for Furby products then on the market. Prices had already decreased by 1999, a year before Gibbons announced his success. The world-wide publicity for his announcement might even have stimulated sales. Assuming upgrade sales of only 100 kits, it would appear that little harm was done by those whose activities were reported in the media.

*Community relations and legal rights*

The toy company, fielding media phone calls, was between a rock and a hard place. Spokeswoman Lana Simon announced Tiger’s position: “Once the consumer purchases the toy, it’s really out of our hands” but “we don’t recommend tinkering with or playing with any of the electronic components.”

Sony Electronics, manufacturer of the Aibo (a robotic dog), was then struggling with a similar, very public problem. The company had instructed a hacker to stop distributing alternative toy software. The hacker posted this letter on the Internet, infuriating Aibo.

---

82. See generally Furby Upgrade webpages, http://www.appspec.net (products); STAATS & VAN DER LINDEN, supra note 66. An API is an “Application Programming Interface,” enabling communication with, e.g., an “operating system or some other control program such as a database management system . . . or communications protocol.” FREEDMAN, supra note 5.


84. Cook, supra, note 49.

purchasers who had paid $1,500 per robotic dog and wanted to play with different software “dog personalities.” Internet-savvy consumers retaliated, boycotting Sony products.

Tiger had to choose between avoiding a possible public relations fiasco or protecting assets under a new law of unknown dimensions. While toy prices were declining, it had to weigh the prospect of years in court, lack of precedent, and hostile press releases by media-savvy hackers. Some companies may be more sensitive to these considerations than others. But all are affected by uncertainty when gauging how the statute will operate.

V. THE LAW AND TECHNOLOGY: ACCESS CONTROL

Summary of statutory scheme

Section 1201(a) protects technological measures that effectively control access to protected works. The statute creates liability for two forms of conduct. Subsection (a)(1) prohibits unauthorized circumvention, defined as unauthorized acts to avoid, bypass, remove, impair, or deactivate a technological measure. It also prohibits unauthorized decrypting or descrambling of encrypted or scrambled works, activities not relevant to this analysis. Subsection (a)(2) makes illegal the unauthorized design, production, use or marketing of means for circumventing technological measures. That provision addresses the commercialization that magnifies the scope of individual illegal conduct, enabling millions of people to engage in unauthorized circumvention. Under each provision, plaintiffs must first establish that a protected work exists and that a technological measure, a padlock of sorts, controls access to the work. Only then does violative conduct by the defendant become an issue. Courts may grant injunctions and award actual or statutory damages for violations of § 1201(a). Conduct is also subject to criminal penalties when a person violates § 1201(a) “willfully and for purposes of commercial advantage or private financial gain.”

VI. SECTION 1201(A): FOUNDATIONS

Overview

If plaintiffs prove the existence of a protected work and a technological measure safeguarding access to it, and no exemptions are invoked, the statute applies.

Section 1201(a)(1), sometimes referred to as the "anti-circumvention" provision, states: "No person shall circumvent a technological measure that effectively controls access to a work protected under this title." The language prohibits only unauthorized circumvention; those engaging in authorized acts need not worry. Unauthorized circumvention, on the other hand, has been analogized to "breaking into a locked room in order to obtain a copy of a book." The nature of that conduct differs from copyright infringement, which focuses on improper use of a work, such as copying. The epoxy-resin in this case controlled access to, and ability to use, the computer code inscribed on the chips. This article focuses on the access control issues.

The evolution of technological language

Meanings set the boundaries of understanding and liability. Yet like rivers whose courses meander over time, meanings change. Technological vocabularies are evolving rapidly. Witnesses (who

---

89. The statute provides several exemptions, although none cover the reported activities. Additional exemptions, based on rulemaking proceedings conducted by the U.S. Copyright Office, are published as regulations. Exemption to prohibition against circumvention, 37 C.F.R. § 201.40 (2003).


91. Note that doctrines that help balance competing interests in infringement cases are not always transferable to a digital context. For example, § 1201 does not incorporate the rule under Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417 (1984). See SECTION-BY-SECTION ANALYSIS OF H.R. 2281, supra note 4, at 9 ("The Sony test of 'capacity of substantial non-infringing uses,' while still operative in cases claiming contributory infringement of copyright, is not part of this legislation. . ."). and at 24 ("The first sale doctrine does not readily apply in the digital networked environment. . ."). See also Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, at 317, n.137, 323 (S.D. N.Y. 2000) (first sale and fair use), aff'd sub nom. Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001).

92. Cf United States v. Davis, 978 F.2d 415, 417 (8th Cir. 1992). In a satellite cable TV piracy case, defendant removed epoxy covered chips, substituting new chips with modified software so non-subscribers could view TV signals.

93. Cf HOWARD & LONGSTAFF, supra note 17; Autogiro Co. of Am. v. United States, 384 F.2d 391, 397 (Ct. Cl. 1967) ("Often the invention is novel and words do not exist to
may be software engineers, programmers, or hackers, whether novices or highly skilled) use terms interchangeably, whether properly or not. Even common words, such as “access,” have many definitions, which can be altered by idiosyncratic use or may vary depending on context. Current dictionaries often lack definitions for important technological and legal terms. Since even experts may lack a common vocabulary, it is essential to exercise caution both in ascertaining definitions and in relying on published precedent for the meanings of words.

Components and their functions.

Protected works embodied in the form of computer code\(^4\) can be stored or processed on a variety of hosts or components. The code may reside in these in a permanent, volatile or ephemeral state.\(^5\) Microprocessors can be used to perform many kinds of tasks.\(^6\) In a device using several microprocessors and other devices, a protected work could reside on one and not another. The work might instead be stored on a CD-ROM or a home video. Maybe it’s stored in a database on a secure server. It is necessary to identify the medium in which a protected work is fixed.

Communicating how a measure guards a protected work.

The relationship between a protected work and the technological measure is significant. To prove that a measure effectively controls describe it. The dictionary does not always keep abreast of the inventor. It cannot. Things are not made for the sake of words, but words for things.”).

94. FREEDMAN, supra note 5 (a code is a “set of machine symbols that represents data or instructions.”).

95. Volatile memory “does not hold its contents without power. A computer’s main memory, made up of dynamic RAM or static RAM chips, loses its content immediately upon loss of power.” FREEDMAN, supra note 5. “Ephemeral” refers to the transient existence in RAM of a software program that vanishes when the computer is turned off. Advanced Computer Services v. MAI Systems Corp., 845 F. Supp. 356, 363 (E.D. Va. 1994). A defendant could argue that he intercepted a work in unprotected transit or after transfer to an unprotected component and, consequently, did not circumvent a technological measure. Imagine an unauthorized person who avoids the security guard at the front gate and enters through a back window. Unauthorized access is prohibited without regard to method of circumvention. Cf. Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, at 318 (the district court rejected “defendants’ construction, [which] if adopted, would limit the application of the statute to access control measures that thwart circumvention, but withhold protection for those measures that can be circumvented.”).

96. See JOSEPH WILLIAMS, AN INTRODUCTION TO COMPUTING INFRASTRUCTURE: HARDWARE AND OPERATING SYSTEMS 34 (1997). A microprocessor is a “CPU on a single chip.” FREEDMAN, supra note 5.
access, it is important to explain how the measure operates.\textsuperscript{97} Much depends upon context. Consider an airplane industry product. The Boeing flight management control system for a 757/767 system is “composed of 80 distinct functional microprocessors (300 when redundancy is accounted for).”\textsuperscript{98} Defendants would demand to know which chips contained the protected work, how they were protected, and what evidence proves unauthorized circumvention. Chip location, work embodied and work-measure relationship can vary widely. An example with multiple chips makes this easier to visualize, but work and measure can also be combined on a single chip. Multiple works and measures may be combined on a single chip. Here, the Furby hackers focused on two daughterboards as the components that held the microchips they wanted to hack.\textsuperscript{99}

The statute cannot be applied to the toy hack without some grasp of the underlying technology. Analogies to past or present forms of communication can be useful. Just as ancient Egyptians once painted hieroglyphics on temple walls, later inscribing symbols on the Rosetta Stone’s black basalt, and publishers print literary works on paper, so software manufacturers etch or build code (instructions or programs) into integrated circuits. This is accomplished on such a miniature scale that the human eye cannot perceive the work. The code is not embodied in a traditional language. Computers do not understand human languages. But they can recognize, or process, electrical impulses or signals, existing in two states (which, like light switches, are referred to as “on” and “off”).\textsuperscript{100} These signals are expressed in text such as this by a binary code (zeros and ones). The electrical signals (in aggregate form called software, source code, or machine code) represent an evolutionary step in communicating. As for the epoxy resin, just as a laminate covers a writing pen’s exterior and the brand name inscribed on it, coating a chip covers the instructions or code built into the circuits.

\textsuperscript{97} But cf. Universal City Studios, Inc. v. Corley, 273 F.3d 429, 438 n.5 (2d Cir. 2001) (“The record leaves largely unclear how CSS protects against the copying of a DVD, as contrasted with the playing of a DVD on an unlicensed player”).

\textsuperscript{98} Jean-Claude Laprie et al., Fault-Tolerant Computing in 1 ENCYCLOPEDIA OF SOFTWARE ENGINEERING 526 (John J. Marciniak ed., 2d ed. 2002). See also WILLIAMS, supra note 96, at 34 (“it is possible to use hundreds of microprocessors in a computer”).

\textsuperscript{99} The patent disclosure indicates several integrated circuits and related circuitry. See infra note 106.

\textsuperscript{100} See WILLIAMS, supra note 96, at 17.
VII. TESTING § 1201(a)—APPLYING THE LAW TO FACTS

Protected Work

Overview

Section 1201(a) requires an original work of authorship fixed in tangible form and protected under Title 17 ("protected work"). While people can touch a book’s pages or look at celebrities’ faces and bodies on a screen, and easily understand how those are tangible, they cannot "see" the signals that direct computer operations. Yet the work’s fixation in a tangible medium—no matter how it is perceived or communicated—must be proved. Location or other aspect of fixation, e.g., whether embodied in digital or analog form, may also be relevant when proving that a measure controls access to a work.

Fixation of Furby’s code in a tangible medium

Hampton started creating the toy’s language in 1997, drawing on Japanese, Thai, Hebrew, and Mandarin Chinese. Working with a rudimentary device reminiscent of electronic Heathkit boards he had used as a boy, he developed an action script ("if you rub his back, he’ll purr"). To control movement and sound, he wrote source code, which was later etched or built into integrated circuits placed in the toy’s interior. The Furby patent discloses several memory components, including SRAM, ROM, and EEPROM. Memory components are important because most computer instructions and

102. 17 U.S.C. § 102 ("Copyright protection subsists . . . in original works of authorship fixed in any tangible medium of expression"); 17 U.S.C. § 101 (2000) ("A work is ‘fixed’ in a tangible medium of expression when its embodiment . . . is sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for a period of more than transitory duration.").
103. See Kirsner, supra at note 21.
106. For those interested in details about the toy, the patent references a RISC controller, control circuitry, CPU, co-processor, information processor, audible speech synthesis processor, sound detection circuitry, infrared signal filtering and receiving circuitry, optical servo control circuitry, power control circuitry, light detection circuitry, and memory (SRAM, ROM and EEPROM). U.S. Patent No. 6,149,490, supra note 24, Detailed Description of the Preferred Embodiments.
107. Computer lexicographer Alan Freedman writes vividly:
data are stored in memory (like information in a book on a shelf), usually in the RAM or the ROM. The CPU temporarily copies the information from memory to another location, e.g., to a code or data cache, and there processes data in accordance with its instructions. The toy’s computer components provided the tangible medium on which were fixed the work—the computer code or programs (instructions for execution)—and the data records for processing (sensory data detected in Furby’s environment). Hampton registered the source code with the U.S. Copyright Office in March 1999. He obtained a certificate of registration (prima facie evidence of copyright validity) and can assert that the chips contain a protected work.

---

Memory is like an electronic checkerboard, with each square holding one byte of data or instruction. Each square has a separate address like a post office box and can be manipulated independently. As a result, the computer can break apart programs into instructions for execution and data records into fields for processing.

***

Although there are memory chips that do hold their content permanently (ROMs, PROMs, EPROMs, etc.), they’re used for internal control purposes and not for the user’s data.

FREEDMAN, supra note 5. See also WILLIAMS, supra note 96, at 15 ("That which specifies what is to be processed is called an instruction. That which gets processed is called data. Instructions tell the CPU what to do, which usually involves processing data.").

108. RAM or Random Access Memory chips function “as the computer’s primary workspace.” ROM (Read Only Memory) is “a memory chip that permanently stores instructions and data.” ROM chips are “used to store control routines in PCs (ROM BIOS), peripheral controllers and other electronic equipment.” FREEDMAN, supra note 5.

109. See generally WILLIAMS, supra note 96, at 34–59; FREEDMAN, supra note 5 (memory).


Technological Measures

Background

The statute does not define "technological measures." DMCA hearing witnesses complained about the omission. Their testimony and written submissions illustrate the range of measures Congress had before it when drafting the statute. These included hardware and software keys based on encryption and scrambling.


The Committee on Commerce was concerned that the lack of such a definition could put device and software developers, as well as ordinary consumers, in an untenable position: the bill would command respect for technological measures, but without giving them any guidance about what measures they were potentially prohibited from circumventing. Given that manufacturers could be subject to potential civil and criminal penalties, the Committee felt it was particularly important to state in our report that those measures that would be deemed to effectively control access to a work would be those based on encryption, scrambling, authentication, or some other measures which requires the use of a 'key' provided by the copyright owner to gain access to a work. Measures that do not meet these criteria would not be covered by the legislation, and thus the circumvention of them would not provide a basis for liability.


114. Committee witnesses mentioned a "dongle," which is a hardware key that is: a copy protection device supplied with software that plugs into a port... on a PC. The software sends a code to that port, and the key responds by reading out its serial number, which verifies its presence to the program. The key hinders software duplication, because each copy of the program is tied to a unique number, which is difficult to obtain, and the key has to be programmed with that number.

FREEDMAN, supra note 5.

115. Id. Encryption means the "reversible transformation of data from the original (the plaintext) to a difficult-to-interpreten format (the ciphertext) as a mechanism for protecting its confidentiality, integrity and sometimes its authenticity." Encryption was not the only significant security method considered. See, e.g., H. Rep. No. 105-796. at 66 (1998). (In discussing § 1201(g) and (j), the Conference Report noted "Not every technological means that..."
authentication measures,¹¹⁷ water-marking, and game cards with security codes.¹¹⁸

Statutory elements: "technological"

Congress realized that different kinds of technological measures could be invented. To preserve freedom of design for manufacturers, legal protection was not limited to measures then used or on the "drawing board."¹¹⁹ Legislators refrained from even defining "technological measures," aware that a definition would soon be outdated. But they did describe relevant criteria or functions characterizing those measures protected by the statute. These criteria are the benchmarks that determine whether a measure effectively controls access in the manner required. Plaintiffs must prove that (1) a technological measure, (2) in the ordinary course of its operation, (3) requires the application of (a) information, (b) a process or (c) treatment, (4) with authorization of the copyright owner, (5) to gain access to the work. Arguably, any device, system, plan, or course of action satisfying elements (2) through (5) could be a "technological measure."¹²⁰ Because the statute does not contain a separate definition for "technological," plaintiffs can argue that they need not actually provide proof of element (1).

Some defendants, in any kind of case under the statute, could disagree with this approach. "Technological," in popular usage,
commonly refers to current innovations, the very latest products, especially those that involve computers or semiconductors. Defendants might demand that plaintiffs prove a measure is "technological." They might also argue that § 1201(a) excludes obsolete measures. Resins have been used for hundreds of years. Surely, they might argue, Congress did not intend to cover outdated technologies. That argument is not supported by the statute's language or legislative history. Neither passage of time nor obsolescence block § 1201(a) legal protection for any form of technological measure. Definitions for "technological" and associated terms, however, merit consideration since they are used throughout the statute.

Definitions

"Technological" means "of, relating to, or using technology." 123 "Technology" means "the application of scientific knowledge to practical purposes in a particular field." 124 A "measure" can be defined as "a plan or course of action taken to achieve a particular purpose." 125 These are among the simplest of many possible definitions.

Furby's technological measures

Two known Furby components block unauthorized access. 126 Both components resulted from the practical use of scientific knowledge and were incorporated in millions of toys. The first component is a plastic shell. Beneath the toy's colorful fur, the shell encases computer components on which the protected work resides. Hackers quickly removed the shell to examine the code. Litigants

---

121. See Freedman, supra note 5 ("high technology" refers to "the latest advancements in computers and electronics, as well as to the social and political environment and consequences created by such machines.").

122. In the 1400s, an Arab encyclopedia identified several cryptographic systems; ancient Egyptians, Hebrews and Assyrians had also devised cipher systems thousands of years earlier. See Gustavus J. Simmons, Cryptology in 16 The New Encyclopedia Britannica 860, 870 (15th ed. 1998). Encryption is not considered outdated. Researchers constantly improve encryption methods. Yet the statute does not limit protection to methods "not yet defeated."


126. Public records may not reveal all of Hampton's access control measures. Although encryption seems unlikely, he could have used a password or authentication sequence.
may dispute whether the shell is a "technological measure," although that is not central to this analysis.127

The other measure, the focus of this article, is the epoxy resin that coated the computer chips. Manufacturers apply conformal coatings, or lacquer systems, to protect printed circuit board assemblies from humidity, temperature extremes, condensation, and contamination.128 The U.S. military and others also use epoxy resins to conceal integrated circuit layouts and block access to software.129

127. Like a TV casing, the shell serves a utilitarian purpose, but that does not necessarily exclude it from qualifying as a technological measure. As some commentators have noted:

Often the objectives of information security cannot solely be achieved through mathematical algorithms and protocols alone, but require procedural techniques and abidance of laws to achieve the desired result. For example, privacy of letters is provided by sealed envelopes delivered by an accepted mail service. The physical security of the envelope is, for practical necessity, limited and so laws are enacted which make it a criminal offense to open mail for which one is not authorized.

ALFRED J. MENEZES ET AL., HANDBOOK OF APPLIED CRYPTOGRAPHY § 1.2, pp. 2-3 (1997). Reprinted with permission from CRC Press, LLC, Boca Raton, Florida. Cf. Judiciary Comm. Hearing, supra note 113, at 47 (statement of Marybeth Peters, Register of Copyrights, Copyright Office of the United States), quoted in note 153 infra; WIPO Copyright Treaties Implementation Act, Hearing on H.R. 2281 Before the Subcomm. on Telecommunications, Trade, and Consumer Protection of the Comm. On Commerce, 105th Cong. (1998) at 34 (statement of Chris Byrne, Director of Intellectual Property, Silicon Graphics) (The statute should only cover a measure that is "robust, strong and active." If not, he commented: "It could be as strong as encryption or scrambling of content or as weak as a coded message to the computer that says 'don’t copy files X, Y and Z,' but does nothing to otherwise protect them."). The Furby shell, analogous to an addressed envelope, bears the inscription "© 1998 Tiger Electronics, Ltd." Defendants would scoff at such an ineffective "measure." The Reimerdes opinion, however, rejected as "indefensible as a matter of law" the argument that a "weak" encryption key failed to effectively control access to a work. Reimerdes, 111 F. Supp. 2d at 317–18 (S.D. N.Y. 2000), aff’d sub nom. Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001). Inscribed notices, while not required by law, could indicate intent to use something as a technological measure. Thus, a plastic shell could display the notice: "Unauthorized Circumvention and Trafficking Prohibited and All Rights Asserted under 17 U.S.C. § 1201."


129. Chip operations can be observed, and crypto keys recovered, provoking countermeasures:

The response of the protection community to attacks of this kind has been to develop ‘conformal glues,’ chip coatings that are not merely opaque and conductive but which also strongly resist attempts to remove them, usually damaging the underlying silicon in the process. These coatings are referred to in a FIPS standard [17] and are widely used by the U.S. military, but are not generally available.

Access: context and meanings.

Access control measures are the bedrock underlying § 1201(a). While the concept of "access" is relevant in some copyright infringement cases, it is always relevant in § 1201(a) cases. The two usages may differ and should be distinguished. Copyright infringement cases address improper uses of an author's protected expression. Plaintiffs in those cases—when trying to counter an "independent creation" defense—seek to prove that defendants "had access" to the protected work. In that context, the word means an "opportunity to view or copy a copyrighted work." 130

Section 1201(a), however, provides a non-infringement cause of action. 131 It applies to technological measures that, like security gates, control access to a protected expression embodied in digital or analog form. The statute requires that plaintiffs establish several elements of proof that differ from those in a § 106 copyright infringement case. The security gate analogy conveys an important aspect of the relationship between the two types of cases. To merit legal protection, the gate must "effectively" control access to a protected work. If the gate is circumvented, the work may become vulnerable. There is a clear association between the two. But no one would confuse, say, a gate with a valuable orchard enclosed within. Similarly, access control issues differ from post-access infringement issues that relate to the guarded work.

With statutorily limited time periods in which to profit from their works, those entitled to claim protection under the copyright laws do not ordinarily authorize consumers to examine, duplicate, or alter their software or computer code. 132 The act of purchasing a product does not establish a right to gain access to a protected work in digital...
form.\textsuperscript{133} Instead, selling a product in which access is protected by a technological measure can be equated with posting a sign marked "No Trespassing."\textsuperscript{134} Thus, 1201(a) issues occur in a unique context. In this very different environment, "access"\textsuperscript{135} can be used as a verb or a noun. It generally means to establish "logical or physical communication or contact."\textsuperscript{136} This would embrace activities beyond mere opportunity to view or copy.

Other words can be combined with "access" to describe control over contact with software ("access control") and operations performed on software ("access modes" or "access operations"). Section 1201(a) access control issues differ from those that arise under another subsection, § 1201(b), which governs unauthorized conduct relating to use of a work. Yet evidence of activities under both of these subsections may be presented with words that are or sound similar. Thus, jurors in cases with multiple causes of action

\textsuperscript{133} See, e.g., Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 317, n.137 (S.D. N.Y. 2000), aff'd sub nom. Universal City Studios, Inc. v. Corley, 273 F.3d 429, 444 (2d Cir. 2001). Defendants argued that sales of copyrighted DVD's conveyed right to circumvent and "perform all acts with it that are not exclusively granted to the copyright holder." 111 F. Supp. 2d at 317, n.137. The court rejected this "corruption of the first sale doctrine." \textit{Id.}

\textsuperscript{134} See United States v. Davis, 978 F.2d 415, 419 (8th Cir. 1992) (encryption shows intent to prevent unauthorized viewing).

\textsuperscript{135} HOWARD & LONGSTAFF, supra note 17, at § 5.1.1, at 8. Many definitions exist. D. Brent Chapman, \textit{Network (In) Security Through IP Packet Filtering}, \url{http://www.deter.com/unix/papers/packet_filt_chapman.pdf}, 3RD USENIX SECURITY SYMPOSIUM (Sept. 1992), at 2 ("definitions of 'unauthorized access' and 'authorized access' vary widely from one organization to another."). \textit{See NATIONAL COMPUTER SECURITY CENTER, GLOSSARY OF COMPUTER SECURITY TERMS, NCSC-TG-004-88 (Oct. 21, 1988), at http://packetstormsecurity.org/docs/rainbow-books/NCSC-TG-004.txt} ("Access" means a "specific type of interaction between a subject and an object that results in the flow of information from one to the other."). \textit{Cf.} Lexmark Int'l, Inc. v. Static Control Components, Inc., 253 F. Supp. 2d 943, 967 (E.D. Ky. 2003) ("access" given "ordinary" meaning). \textit{But see NORMAN J. SINGER, 2A STATUTES AND STATUTORY CONSTRUCTION § 47.27 (6th ed. rev. 2000) (use ordinary meaning unless language has "acquired technical meaning or unless a definite meaning is apparent or indicated by the context of the words."). See also id. at § 47.29. Cf. TEX. PENAL CODE ANN. § 33.01(1) (2003) ("'Access' means to approach, instruct, communicate with, store data in, retrieve or intercept data from, alter data or computer software in, or otherwise make use of any resource of a computer, computer network, computer program, or computer system."). For a more extensive discussion of "access control", see Ravi Sandhu and Jaehong Park, \textit{Usage Control: A Vision for Next Generation Access Control (2003), at http://www.list.gmu.edu/park/paper/MMM03-UCON-vision.pdf} (expanding concepts relevant to access matrix model).

\textsuperscript{136} HOWARD & LONGSTAFF, supra note 17, at § 5.1.1, at 8. "Logical" has a special meaning within the field of computer science. FREEDMAN, supra note 5 (definitions of "logic" and "logical vs. physical"). The terms "logical" and "physical" differentiate between the user's and computer's "view." "Users relate to data logically by data element name; however, the actual fields of data are physically located in sectors on a disk." \textit{Id.}
under §§ 1201(a)(1), (a)(2) and (b) may need to distinguish between words that are or sound alike but that have different legal significance.

In this case, the epoxy resin blocked both access and post-access uses. Had it been ineffective, hackers could have performed several post access operations (i.e., exercised a series of access rights) on the code in violation of § 1201(b). These operations are usually referred to with the words: "read,"137 "write,"138 "modify,"139 "delete,"140 "create," and "execute."141 Even "reading" could infringe by duplicating a work unless otherwise permitted.142 Unable to engage in any of these activities, individuals tried to examine the chips to discern what they could of the computer code. Those who can examine, or perform access operations on, a work can obtain control of it as if no technological, statutory, or contractual protections exist. An opportunity to examine chips can enable reverse engineering of the object code (the machine language) in order to reconstruct the source code (the version humans read more easily). Hampton’s epoxy served its purpose. Consequently, hackers found that “software and sound data is not accessible for reading, writing, disassembly, replacement, or even examination. There are no exposed data/address busses, interrupt lines, or i/o lines other than what directly drives the peripherals.”143

137. “Read” means:
To input into the computer from a peripheral device (disk, tape, etc.). Like reading a book or playing an audio tape, reading does not destroy what is read. A read is both an input and an output (I/O), since data are being output from the peripheral device and input into the computer. Memory is also said to be read when it is accessed to transfer data out to a peripheral device or to somewhere else in memory. Every peripheral or internal transfer of data is a read from somewhere and a write to somewhere else. 

Id. See also HOWARD & LONGSTAFF, supra note 17, at § 5.1.1, at 10 ("read" means to “obtain the content of data in a storage device, or other data medium”).

138. “Write” means to “store data in memory or record data onto a storage medium, such as disk and tape.” FREEMAN, supra note 5.

139. HOWARD & LONGSTAFF, supra note 17, at § 5.1.1, at 10 ("change the content or characteristics”).

140. “Delete” means to “remove an item of data from a file or to remove a file from the disk.” FREEMAN, supra note 5. See also HOWARD & LONGSTAFF, supra note 17, at § 5.1.1, at 10 ("remove . . . or render it irretrievable”).

141. FREEMAN, supra note 5 ("Execute" means to “run a program (follow instructions in the program). Same as run.”).


143. van der Linden, supra note 33.
These comments reveal more than inability to bypass the epoxy resin. They reflect a single-minded drive to gain access. But "access" is not an isolated "no impact" event. Accessing a digital work is not comparable to picking up and reading a nineteenth century book. Access effectively shifts almost complete power from copyright owners to hackers, pirates or business rivals with respect to an individual copy. This enables virtually unlimited ability to reproduce, modify, and distribute the work, with no physical restraint on method, price, or place of distribution. These activities may be restrained by injunction or remedied by damages in time. Yet during the passage of that time, countless reproductions could be flowing across multiple channels of communication. The enormity of this potential power shift highlights the importance of defining "access" and charting its reach.

The boundaries of "circumvention"

Whether "circumvention" covers only conduct that enables access to a protected work, i.e., which successfully evades access control, or also includes conduct that does not gain access can be debated. The statute's language appears to cover both kinds of conduct.

(i) No express language requires that "access" be gained.

Section 1201(a)(1) prohibits persons from circumventing technological measures, not from gaining access. The §
1201(a)(3)(A) definition of "circumvent" likewise does not expressly require that a defendant gain access.\textsuperscript{146} It simply describes a technological measure that "effectively controls access to a work" and the need to use a key (information, process, or treatment) "to gain access to the work." Carefully delineating forbidden conduct and purposes, Congress used far more explicit language in other DMCA provisions.\textsuperscript{147} It is significant that § 1201(a)(1) does not expressly prohibit gaining access.

(ii) Language that suggests gaining "access" was contemplated.

Section 1201(a) describes acts that by circumventing technological measures enable persons to gain access to a work. The verbs "decrypt" and "descramble" suggest that gaining access, while not explicitly required, is implicitly intended.\textsuperscript{148}


\textsuperscript{147} 17 U.S.C. § 1201(d)(1) (2000) (exemption for archives, nonprofit libraries and educational institutions refers to an institution that "gains access to a commercially exploited copyrighted work"); § 1201(g)(5) (encryption research exemption refers to "protection of copyright owners against the unauthorized access to their encrypted copyrighted works"); § 1201(h)(2) ("prevent the access of minors to material on the Internet"); § 1201(i)(1)(A) ("a natural person who seeks to gain access to the work,"); § 1201(i)(1)(C) ("no other effect on the ability of any person to gain access to any work"); § 1201(j)(1) ("the term 'security testing' means accessing a computer"). \textit{Cf.} 18 U.S.C. § 1030(a)(1)(2000) (imposing criminal sanctions on those who have "knowingly accessed a computer").

\textsuperscript{148} See infra text accompanying note 185 for language of 17 U.S.C. § 1201(a)(3)(A) (2000). \textit{But cf. Reimerdes,} 111 F. Supp. 2d at 315 (Posting a decryption program on the Internet "is analogous to the publication of a bank vault combination in a national newspaper. Even if no one uses the combination to open the vault, its mere publication has the effect of defeating the bank's security system, forcing the bank to reprogram the lock."). Liability might be asserted for prohibited dealings in technology under § 1201(a)(2). Defendants may contend that the law is vague, arguing that it is unclear whether acts failing to gain access violate the statute; the statute does not mention "attempted." \textit{See generally Catherine Therese Clarke, From CrimlNet to Cyber-Perp: Toward an Inclusive Approach to Policing the Evolving Criminal Mens Rea on the Internet,} 75 OR. L. REV. 191, 203 n.56 (1996) ("The constitutional law doctrine of void-for-vagueness is the primary means for overturning criminal laws that are unclear to ordinary men and women," citing Connally v. General Constr. Co., 269 U.S. 385 (1926)). \textit{Cf. United States v. Elcom Ltd.,} 203 F. Supp. 2d 1111, 1122 (N.D. Cal. 2002) (court denied motions to dismiss, rejecting claimed failure "to provide . . . notice that will enable ordinary people to understand" prohibited conduct).
(iii) Two-factor authentication issues

Consider a two-factor authentication system that controls access to an encrypted work. This provides a useful hypothetical for thinking about a system in which some control elements might be breached while others are not. Authorized users must provide passwords and, as an added safeguard, are scanned biometrically. An individual could by trickery obtain the decryption code and post this on the Internet. He might circumvent the password system, obtaining a password through social engineering. Lacking the proper fingerprints, signature or retina scan, he presumably would be unable to gain access to the work (although biometric devices can be fooled and he might have other avenues for gaining access). A plaintiff aware of these activities would seek an injunction, not waiting for someone to gain access to a work and certainly not conceding that the statute requires access. The statute protects both works and measures. The language is broad enough for alert plaintiffs to assert that a person avoided, bypassed or impaired a technological measure, whether or not every access control element is successfully breached or circumvented.

(iv) Legislative history

Some legislative history describes § 1201(a) as a "general prohibition against gaining unauthorized access to a work by circumventing a . . . measure." Whether Congress intended to prohibit unauthorized access or merely referred to a general prohibition against gaining unauthorized access, which took the limited form of forbidding circumvention (an approach based on

149.  Kemmerer, supra note 117, at 209 (many biometric devices are “used in a two-factor authentication system, such as with passwords.”).
151.  H.R. REP. NO. 105-551, pt. 1, at 17–18 (1998) (“general prohibition against gaining unauthorized access to a work by circumventing a technological protection measure”); SECTION-BY-SECTION ANALYSIS OF H.R. 2281, supra note 4, at 5 (“general prohibition against gaining unauthorized access to a work by circumventing a technological measure”). Cf. id., at 5 (“Subsection (a) of new Section 1201 applies when a person who is not authorized to have access to a work seeks to gain access by circumventing a technological measure put in place by the copyright owner that effectively controls access to the work.”) (emphasis added); H.R. CONF. REP. NO. 105-796, at 63–64 (1998) (WIPO Treaties “require contracting parties to provide ‘adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors . . . .’”) (emphasis added).
method rather than outcome) can be debated. Courts have yet to address the issue.

There are reasons for concluding that persons may violate § 1201(a)(1) without gaining access to a work. First, the language of § 1201(a)(3)(A) protects both measures and works. Failure to gain access to, or decrypt, a work, therefore, might affect only part of the analysis. Additionally, even with respect to the language that protects a "work," software is already legally protected under 17 U.S.C. § 106. That provision grants copyright owners an exclusive right to reproduce or otherwise use their own works. To demand that plaintiffs prove unauthorized circumvention by demonstrating defendants gained access, in the sense of the word relevant to infringement, would unnecessarily and improperly duplicate infringement prohibitions since § 1201(a) creates a tort separate from infringement.\(^{152}\) Moreover, the act of disseminating a decryption program on the Internet can inflict severe damage. The act of posting decryption code, without gaining access, could be more destructive to a copyright owner's present and future economic interests and technological resources than the single act of an individual who successfully decrypts a work gains access for isolated viewing.

Ordinary course of operation: Overview.

Like a security guard required to perform several duties, a technological measure must accomplish specific tasks "in the ordinary course of its operation."\(^{153}\) Its critical mission is controlling access to the protected work. This is achieved by: (1) blocking unauthorized access and (2) permitting access, when authorized, only in accordance with established procedures. Section 1201(a)(3)(B) essentially provides a job description: a qualifying measure is one that "controls access" and "requires the application" of a key in order "to gain access." This description does not characterize the measure's tasks as "sole," "primary," or even "non-incidental," although these tasks must be performed to merit protection under the statute. Failure to defeat all methods of attack will not necessarily disqualify the

---

153. 17 U.S.C. § 1201(a)(3)(B) (2000). Cf. BLACK'S LAW DICTIONARY, supra note 130, at 1125 ("Ordinary" means occurring "in the regular course of events; normal; usual."); Judiciary Comm. Hearing, supra note 113, at 47 (statement of Marybeth Peters, Register of Copyrights, Copyright Office of the United States) (opining that "ordinary course of its operation" excludes technologies "that may have the incidental or unintended effect of controlling access, or do so only when used in an unusual way.").
measure. It must simply function to prevent access when it is not circumvented.

The statute requires that one of three "keys" (consisting of information, a process or treatment) must be applied as a method for enabling authorized access. Defining effective "control" by requiring application of keys, from one perspective, is like grading the effectiveness of a lock on whether it can be unlocked. The measure, however, is operating as intended if it controls access so well that a key is required to gain access to the work. Because the key applies to the copyright owner's designated gate for access, the existence of other avenues is irrelevant. The statute, moreover, does not mandate any level of difficulty, sophistication, or secrecy for keys. Regardless of how they are made or function, the technological measure must require their application.

A security guard traditionally allows access through a particular entry way. Visitors with proper keys and a token of authority may be waved through the security point. At other times, the guard could direct visitors to alternative access routes ("not the front door but the back door near the loading dock" or "not this building, but the blue glass building two blocks north"). So, too, a technological measure, by blocking an entry way, could require that access be obtained in alternative ways. ("Go to the next station and show the guard there your badge.")

The "ordinary course" standard suggests minimal criteria for determining whether the measure operates as required. The measure must (1) block unauthorized access to the work, \(154\) (2) require that authorized access be gained by using one of three keys, and (3) be operating normally.

The "actually works" standard.

In *Universal City Studios, Inc. v. Reimerdes*, Judge Kaplan, of the Southern District of New York, analyzed the meaning of "effectively controls" access and "ordinary course of operation."\(^{155}\)

---

\(^{154}\) *Reimerdes*, 111 F. Supp. 2d at 318 ("As CSS, in the ordinary course of its operation—that is, when DeCSS or some other decryption program is not employed—'actually works' to prevent access to the protected work, it 'effectively controls access'").

\(^{155}\) See *Reimerdes*, 111 F. Supp. 2d at 317-18. *See also* SECTION-BY-SECTION ANALYSIS OF H.R. 2281, supra note 4, at 10 (if, in the ordinary course of its operation, a technology actually works in the defined ways to control access to a work, or to control copying, distribution, public performance, or the exercise of other exclusive rights in a work, then the 'effectiveness' test is met, and the prohibitions . . . are applicable).
The case, filed before the effective date of § 1201(a)(1), addressed § 1201(a)(2) issues relating to unauthorized decryption of movies. Both § 1201(a)(1) and (a)(2) use the same definition of "circumvent." Thus, some Reimerdes holdings are relevant to the Furby's non-encryption analysis.

In Reimerdes, several major motion picture studios protected their copyrighted movies with CSS ("Content Scrambling System"). This system was designed to block unauthorized access and unauthorized copying. The studios distributed the protected movies on digital versatile disks (DVDs) for home use. A teenager, with the assistance of others, cracked the system by discovering its encryption algorithm and related keys. He posted his decryption program, "DeCSS," on the Internet, empowering others to break the system and to make unlimited copies. This damaged studio control over the movies, jeopardizing their profits. The studios sought to enjoin defendants from posting and linking to the decryption program on the Internet.

Judge Kaplan analyzed the relevant legislative history, which stated that "a technological measure 'effectively controls access' to a copyrighted work if its function is to control access." He concluded that "effectively" requires only a minimal showing. To demand a "successful or efficacious" technological means of controlling access, would "gut" the statute. Thus, plaintiffs need only show that a measure "actually works" when not circumvented. CSS did actually work and the court granted the injunction.

The law punishes those who engage in illegal conduct, not those with imperfect security systems. A measure's sophistication should be irrelevant, although this seems counter-intuitive. A copyright owner ought to adopt the most effective means for protecting his work. To do otherwise is contrary to his best interests. But if unable to afford the best, he should not forfeit statutory protection. Both economic fairness and the "logic" of not requiring the impossible support this conclusion. Consequently, § 1201(a) may protect an outdated, unsophisticated or easily circumvented measure. The test is whether § 1201(a)(3)(B) criteria are met, not whether a measure successfully prevents all instances of unauthorized access.

156. Reimerdes, 111 F. Supp. 2d at 318.
157. Id. "Efficacious" means "successful in producing a desired or intended result; effective." NEW OXFORD AMERICAN DICTIONARY, supra note 123, at 543-44.
158. See Reimerdes, 111 F. Supp. 2d at 318 (anything that can be "encrypted or scrambled often may be decrypted or unscrambled."). While future technologies might be more effective, those unable to afford expensive measures would continue to use vulnerable systems.
Application of process or treatment as a “key”

The measure must require that a “key” (requiring the application of information, a process, or treatment) enable access. “Application” differentiates between knowledge and use.159 “Process” means “a series of actions or steps taken in order to achieve a particular ending.”160 “‘Treatment’ can be defined as ‘subjection of something to the action of an agent or process.’”161 Several processes or treatments can remove epoxy resin.162 The copyright owner can authorize any or all of these applications. Litigants can debate whether the authorized processes or treatments constitute “keys” under the statute.163

Application of information as a “key.”

Information can also be applied to gain access. Information keys include digital communications such as authentication or data sequences,164 handshakes,165 encryption keys, and passwords.166 Keys enabling access can be strong or weak.167 Whether additional technological measures, not described in the public domain, regulate

159. NEW OXFORD AMERICAN DICTIONARY, supra note 123, at 75 (“Application” means “the action of putting something into operation.”).
160. Id. at 1358.
161. WEBSTER'S THIRD NEW INTERNATIONAL DICTIONARY, supra note 7, at 2435.
162. Methods for removing epoxies include applying thermal or heating methods, grinding and scraping, and microblasting. Coating Identification and Removal Method Tables, CIRCUITS ASSEMBLY, Oct. 2002, http://www.circuitsassembly.com/mag/mag_archive.shtml; Anderson & Kuhn, supra note 129, at 3–4 (Remove epoxy by using “fuming nitric acid (> 98 percent \(HN\_03\)),” accelerating the process by heating the acid. “[D]ry etching with hydrogen fluoride” and “microprobing needles” can remove other protective layers.).
163. Cf. Reimerdes, 111 F. Supp. 2d at 317–18 (“One cannot lawfully gain access to the keys except by entering into a license... under authority granted by the copyright owners...”). Many epoxy removal formulas are public knowledge. Litigants may dispute whether copyright owners must have complete control of keys although the statute is silent on this point.
164. See, e.g., Sega Enterprises Ltd. v. Accolade, Inc., 977 F.2d 1510, 1515 (9th Cir. 1992) (initialization code).
165. Handshaking, or identification of authenticating data, refers to signals “transmitted back and forth over a communications network that establish a valid connection between two stations.” FREEDMAN, supra note 5. See also RealNetworks, Inc. v. Streambox, Inc., 2000 U.S. Dist. LEXIS 1889, Findings of Fact, ¶12 (W.D. Wa. Jan. 18, 2000) (“Secret Handshake” was authentication sequence protecting against unauthorized access).
166. See generally FREEDMAN, supra note 5 (encryption algorithm keys).
167. MENEZES ET AL., supra note 127, at § 10.2, p. 388 (“Conventional password schemes involve time-invariant passwords, which provide so-called weak authentication.”); Reimerdes, 111 F. Supp. 2d at 317–18 (defense that “weak cipher” failed to effectively regulate access to work “indefensible as a matter of law”).
access to the Furby's protected work by using information keys, is unknown.

"Keyholes"

Because "keys" are essential, it is worth considering "keyholes" (the location for, or manner of, applying the key). Congress sought to avoid a "pay-per-use" world, fearing copyright owners would lock up works and deprive information users of access to, and fair use of, works.168 The statute mandates that access be possible if a key is applied. Litigants can argue whether keys must be applied to the measure or to some component subject to a purchaser's control. Qualified measures, though, take many forms. They may consist of stand-alone devices or software operating on a computer network and may utilize several means for communicating. Some products contain a signaling or conversion device, while the copyright owner retains control with a computer or device separate from the product.169 The statute does not require that keys be applied to any item possessed by purchasers. Keys may be applied elsewhere in some other fashion so long as access can thereby be gained. This reasoning would apply whether a measure is a stand-alone device or is connected by electronic, wireless, or optical networks to other components or systems. By prohibiting entry at one gate, a technological measure can thereby "require" that persons use, or apply keys, at other security clearance venues.

Normal functioning: no "glitches."

Imagine a measure that actually works when not circumvented, but something goes wrong. "Ordinary course" suggests that a measure is functioning properly as designed. Errors and uses not intended as part of the ordinary course of operation should not alter the standard. It is possible to induce malfunctions170 and

---

170. In a "glitch attack:" we deliberately generate a malfunction that causes one or more flipflops to adopt the wrong state.... of the many fault-induction attack techniques on smartcards that have been discussed in the recent literature, it has been our experience that glitch attacks are the ones most useful in practical attacks.

Oliver Kommerling and Markus Kuhn, Design Principles for Tamper-Resistant Smartcard Processors, §2.2.1, at 15, USENIX WORKSHOP ON SMARTCARD TECHNOLOGY PROCEEDINGS (May 10–11, 1999),
programmers can leave "backdoors" for unauthorized access. Where appropriate, these would presumably be addressed as circumventing acts. Holdings based on naturally occurring or engineered glitches, however, would deprive decisions of predictability. Thus, at a minimum, measures evaluated should be considered when functioning normally and used as intended.

Copyright owner's authority

It is necessary to address the role of authority in two instances. First, plaintiffs must prove that a technological measure can enable access to the protected work on applying a required "key" when and if authority is granted. Next, when establishing a subsection (a)(1) or (a)(2) violation, they must prove that the prohibited act occurred without such authority.

"Authority" is generally defined as the "right or permission to act legally on another's behalf." A copyright owner could grant authority in several ways, authorizing application of a key or permitting otherwise prohibited conduct. Additional avenues may be possible. In a case such as this, individuals could argue that Tiger's press release (stating "it's really out of our hands" after toys are purchased) acknowledges or conveys "authority" to circumvent. A court that found them to be "innocent" violators could reduce or remit all damages. Public records, however, do not reveal that anyone sought, or copyright owners granted, express authority to apply a
required key or to engage in any prohibited conduct.\textsuperscript{176} Whether authority has been granted is a critical factor when distinguishing legal from illegal conduct.\textsuperscript{177} Thus, future plaintiffs will likely insist that express rather than implied authority is required, while defendants will seek to persuade a court otherwise.\textsuperscript{178}

This analysis earlier considered whether a "key" must be applied to a technological measure that is subject to a purchaser's or user's control. A similar question arises when considering how "authority" might be communicated. A component within a user's control could serve as a contact point for authorization. An authorized person, for example, could insert a game card or apply information "keys" such as tokens or passwords to a system within his control. An initial grant or repeated grants of authority might be required. Necessary exchanges could be handled by clicking an "accept" button onscreen, or by communicating with software over the Internet or through other means controlled by a copyright owner.\textsuperscript{179} Notices to users and traditional practices may be relevant when determining whether authority has been granted.\textsuperscript{180} But the statute does not require a particular method of controlling authorization.

\textit{Technological measures: digital, analog or other embodiment}

Section 1201(a) protects works in digital and analog form.\textsuperscript{181} Individuals could argue that epoxy—an inert substance applied to, but not operating as, such a device—is not protected. Form and

\begin{itemize}
\item \textsuperscript{176} Cf. United States v. Davis, 978 F.2d 415, 419 (8th Cir. 1992) ("encrypting or scrambling a satellite signal evinces . . . intent to prevent unauthorized persons from viewing the transmission and communicates this intent unequivocally to persons receiving the encrypted or scrambled signal").
\item \textsuperscript{177} See, e.g., Universal City Studios, Inc. v. Corley, 273 F.3d 429, 444, n.14 (2d Cir. 2001) (Subsection 1201(a)(3)(A) "frees an individual to traffic in encryption technology designed or marketed to circumvent an encryption measure if the owner of the material protected by the encryption measure authorizes that circumvention.").
\item \textsuperscript{178} See The Chamberlain Group, Inc. v. Skylink Techs., Inc., 68 U.S.P.Q.2d (BNA) 1009, 2003 U.S. Dist. LEXIS 15298 (N.D. Ill. Aug. 29, 2003) (where copyright owner previously allowed purchasers to use alternative means of access, defendant argued authorization was not required).
\item \textsuperscript{179} See, e.g., Time Warner Cable of New York City v. Cable Box Wholesalers, Inc., 920 F. Supp. 1048, 1049 (D. Ariz. 1996) (converter/decoders required to descramble cable television services were "addressable" and could be "remotely programmed" from the transmission center).
\item \textsuperscript{180} Skylink Technologies, 68 U.S.P.Q.2d (BNA) 1009, 2003 U.S. Dist. LEXIS 15298 (purchasers traditionally allowed to use alternative means of access).
\end{itemize}
composition, however, are irrelevant if the measure meets all statutory criteria. Manufacturers need not adopt any particular design. Moreover, protected works (software) and technological measures (epoxy-resin, security cards or encryption) may differ in purpose and function. The statute’s open-ended language and legislative history provide grounds for treating the epoxy resin as a technological measure.

Summary of foundation analysis

The toy’s software, a literary work fixed on computer chips, is protected by a hard, opaque resin that controls access to the work. The resin can be eliminated by applying a process or treatment. No public records reveal express authority to apply a required key or engage in prohibited conduct. The protected work and technological measure provide the needed foundation to allege that the statute applies. The inquiry now turns to whether violations have occurred.

VIII. SECTION 1201(A)(1) VIOLATIONS: UNAUTHORIZED CIRCUMVENTION

The statute lists but does not define prohibited acts of “circumvention.” That language provides the touchstone for § 1201(a)(1) unauthorized circumvention and § 1201(a)(2) prohibited trafficking in technology. To “‘circumvent a technological measure’ means to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner.” This section investigates whether § 1201(a)(1) prohibits removing and replacing the Furby computer chips.

184. WEBSTER’S THIRD NEW INTERNATIONAL DICTIONARY, supra note 7, at 410 (“Circumvention” means “overcome or avoid the intent, effect, or force of... check, or defeat by ingenuity or stratagem: make inoperative or nullify the purpose or power of esp. by craft or scheme”).
185. 17 U.S.C. § 1201(a)(3)(A) (2000). The statute prohibits acts to decrypt and descramble “or otherwise to avoid, bypass, remove... a technological measure.” “Otherwise” is an adverb that means “in circumstances different from those present or considered... in a different way.” NEW OXFORD AMERICAN DICTIONARY, supra note 123, at 1212. Litigants can argue whether the subsequent acts should be construed under the rule of ejusdem generis. That rule is defined as “A canon of construction that when a general word or phrase follows a list of specific persons or things, the general word or phrase will be interpreted to include only persons or things of the same type as those listed.” BLACK’S LAW DICTIONARY, supra 130, at 535.
Removal

Unauthorized persons may not remove technological measures. "Remove" means to change or shift location or position. Relevant changes could include: (i) separating the measure (epoxy resin) from the work inscribed on computer chips, (ii) changing the measure's original position, or (iii) separating the combined two from an original location. In this case, individuals disconnected the leads permitting the software to operate. Then they extracted the epoxy-covered chips from the toy's interior. When they initially removed these, they sought access to the software. On failing to gain access, they decided to experiment with toy components and to create new software instead.

Some may argue that the epoxy still safeguards the work. Seeking neither to gain access to, nor use, the software, they would contend that removal is not a violation. But motive is irrelevant. Unauthorized removal is improper. No language immunizes a combined removal of both work and measure.

Defendants may argue that additional acts should be limited to the same class as decryption or descrambling, urging that acts affecting epoxy-resin are not covered. Plaintiffs may disagree. The subsequent acts can be characterized as specific rather than general. Decryption and descrambling, moreover, can be interpreted narrowly (as a limited type of unauthorized circumvention) or broadly (as part of a larger class of circumventing acts limited only in scope by the statutory criteria). Nothing limits the statute's scope to encryption and scrambling systems. See H.R. REP. NO. 105-796, at 66 (1998) ("Not every technological means that is used to provide security relies on encryption technology, or does so to the exclusion of other methods.").

186. WEBSTER'S THIRD NEW INTERNATIONAL DICTIONARY, supra note 7, at 1921 ("Remove" means "to change or shift the location, position, station or residence of... to move by lifting, pushing aside, or taking away or off: put aside, apart, or elsewhere.").

187. The leads, or pins, are the connections through which electrical signals (including data, instructions, and power) flow. WILLIAMS, supra note 96, at 35.

188. The § 1201(f) reverse engineering exemption is probably inapplicable. It applies to persons who have "lawfully obtained the right to use a copy of a computer program." 17 U.S.C. § 1201(f)(1)(2000) (emphasis added). The exemption facilitates "interoperability" between computer programs, a potential problem here since the hackers discarded computer chips. Interoperability, however, could be analyzed (1) individually, limiting focus to the toy that is hacked, or (2) communally, considering how a new or altered computer program might affect a toy's interactions with other devices. See also SECTION-BY-SECTION ANALYSIS OF H.R. 2281, supra note 4, at 14 (lawful acquisition of such a program means "the computer program must be acquired from a legitimate source, along with any necessary serial codes, passwords, or other such means as may be necessary to be able to use the program as it was designed to be used by a consumer of the product.") (emphasis added).

189. In some instances, a removed measure may represent part of a larger system, consisting of multiple measures that provide protection based on the removed object and remaining components.
Allowing defendants to sweep acts under the rug, by asserting subjective thoughts and motives, would make the statute impotent. The statute's scope and breadth, however, require thoughtful analysis. Section 1201(a)(3)(A) can be viewed as ambiguous in some respects. Defendants can argue that the statute should apply only to separation of measure from work, not a combined separation of the two from the toy's interior. Until a court agrees with this interpretation, which seems unlikely, however, plaintiffs may rely upon the statute's plain language to allege that individuals violate § 1201(a)(1) by disconnecting, shifting, and extracting chips. Significant unauthorized circumvention may begin with chip removal, making this a reasonable act to address and not beyond the statute's scope.

Deactivation and impairment

Unauthorized persons may not deactivate a technological measure, that is, make it inactive or ineffective. Nor may they impair or reduce its effectiveness. Eliminating the epoxy by removing it might be viewed as deactivating conduct. To avoid redundant use of statutory terms or confusion between removal and deactivation, perhaps "deactivate" could be limited to active rather than passive measures, to circumstances where removal is not a concurrent issue, or to instances where removal and deactivation represent distinguishable approaches.

Efforts to remove the epoxy (by applying heat, or by grinding, scraping and microblasting) could impair it. In some circumstances, this might raise a question whether the physical integrity or form of a measure is relevant to its ability to operate normally. Defendants will urge a narrow interpretation of "impair," finding actionable conduct only if an act damages a measure's effectiveness. It is unclear how

190. See, e.g., United States v. Davis, 978 F.2d 415, 417 (8th Cir. 1992) (defendants removed epoxy-covered chips, replacing them with new chips that contained modified software).

191. Webster's Third New International Dictionary, supra note 7, at 579.

192. Webster's Third New International Dictionary, supra note 7, at 1131 ("to make worse: diminish in quantity, value, excellence, or strength: do harm to"). Computer crime statutes offer more useful descriptions. Cf. 18 U.S.C. § 1030(e)(8) (2000) ("damage means any impairment to the integrity or availability of data, a program, a system, or information" that causes a specified dollar loss, causes injuries, or threatens public health or safety); Tex. Penal Code Ann. § 33.01(14) (2003) ("'Harm' includes partial or total alteration, damage, or erasure of stored data, interruption of computer services, introduction of a computer virus, or any other loss, disadvantage, or injury that might reasonably be suffered as a result of the actor's conduct.").
courts will interpret "impair." To minimize redundancy, courts may inquire how impairment differs from other circumventing acts in method or outcome.

Avoid or bypass: meanings

The statute prohibits acts that avoid or bypass a technological measure. "Avoid" can be defined as to "keep away from" or prevent the effectiveness of something. "Bypass" can be defined as to use an alternate method to access. Both are non-technical words adapted to describe acts relating to security vulnerabilities. Computer security specialists have used "bypass" for years, but dictionaries rarely provide a technological meaning, although some Internet glossaries are helpful.

193. Impairment could have many facets. As with other circumventing acts, impairment could affect whether, or how effectively, a technological measure, or a component or subroutine of the measure, operates. Like a small town that continues in isolated existence after an interstate highway loops around it, though, a measure may continue to operate even though it does not control routes beyond its immediate reach. Effective control of access does not require command of all conceivable avenues. See Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, at 318 (S.D. N.Y. 2000), aff'd sub nom. Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001) (district court held that "effectively controls access" is determined by examining the technological measure when it is not circumvented). Moreover, just as a security guard posted at the front gate might not see someone enter through a back window, a particular observer might not immediately discern evidence of what has occurred. An impairing act, whatever its nature, would appear to be something less than a totally effective act of circumvention. That raises questions of degree and incremental progress or baton-passing by persons seeking unauthorized access or engaging in prohibited conduct. Defendants will urge that all such issues be viewed through a narrow lens.

194. But see United States v. Thompson/Center Arms Co., 504 U.S. 505, 520-21 (1992) (Scalia, J. concurring) ("As for the phrase 'otherwise producing,' that may well be redundant, but such residual provisions often are.... They are a prime example of provisions... for which an inflexible rule of avoiding redundancy will produce disaster.").

195. Webster's Third New International Dictionary, supra note 7, at 151 ("to keep away from: stay clear of... to prevent the occurrence or effectiveness of").

196. Howard & Longstaff, supra note 17, at § 5.1.1, at 10 (an action taken to "avoid a process by using an alternative method to access a target"); WEBSTER'S THIRD NEW INTERNATIONAL DICTIONARY, supra note 7, at 307 ("bypass" means "to make a circuit or detour around... get around... to go around and beyond (an enemy) without attempting to attack"). "Detour" means "a turning aside: a circuitous route: a deviation from a direct course or the usual procedure." Id. at 617.

197. See, e.g., National Computer Security Center, Glossary of Computer SECURITY TERMS, supra note 135 ("attack" means "trying to bypass security controls on a system").

198. See, e.g., New Oxford American Dictionary, supra note 123, at 237 (non-technical definition of "bypass" includes "avoid or circumvent").
To prevent redundancy, "bypass" can be distinguished from "avoid," by defining "bypass" narrowly as a kind of "detour." One bypasses a city in that context by charting a course with specific reference to that location, indicating at least a conceptual association. One can avoid a city, however, by staying away from the nation or continent where it is located. In order to establish distinctive meanings for these two words, therefore, courts could designate whether an act is unrelated (avoids) or related to (bypasses) a measure. The two terms have recognized technical meanings in some fields. In those instances, the technical meaning would control. Although this approach offers ways to minimize statutory construction problems, in all likelihood, until sufficient judicial guidance is provided, pleadings and court opinions will probably use the terms jointly, as in "defendants avoided or bypassed the measure."

**Insertion of new chips as “avoidance” or “bypass”**

Removal, in this instance, with this technology, could represent an act or point in time after which no further violations can occur. Upgrade kits allow purchasers to manipulate the toy's hardware by using new software. Thus, individuals charged with violating the statute could argue that the new chips and code are not covered. Since no statutory exemption appears applicable, liability, if any, would depend on whether § 1201(a) applies to their conduct.

Post-removal activities provoke discussion about whether the statute, through language such as "avoid" or "bypass," protects something beyond the measure, i.e., the overall concept or technological "system" of protection represented by, but not limited to, a particular measure.¹⁹⁹ That such a question can even be posed illustrates the tension between the statute's purpose (protecting works and measures) and its language (creating liability for acts that may not directly impact these). Acts can logically defeat a measure's purpose, however, even without direct or physical impact. Section 1201(a) need not be interpreted expansively here to reach something beyond

---

¹⁹⁹. The titles of both Chapter 12 of the DMCA, "Copyright Protection and Management Systems," and § 1201, "Circumvention of copyright protection systems" refer to "systems" rather than "measures." Cf. Joint Hearing supra note 171, at 38 (Statement of Bruce A. Lehman, Commissioner of Patents and Trademarks, Patent and Trademark Office, Dept. Of Commerce) ("technology can be used to defeat any protection that technology may provide.... [T]echnological protection likely will not be effective unless the law also provides some protection for the technological processes and systems used to prevent or restrict unauthorized uses of copyrighted works."). (emphasis added). Early drafts of § 1201 prohibited circumvention of "any process, treatment, mechanism or system." Id.
the epoxy. It is sufficient that installing new chips may not violate the statute if all protected work has been removed. Conduct involving the upgrade kits, therefore, considered below, might not constitute prohibited dealings in technology unless other factors enter the picture.

Other perspectives are possible. If remaining toy components contain protected work, or enable communication with protected work in other toys or devices, then chip replacements would be more troubling. Chip removal and replacement, moreover, could be integral parts of the same circumvention. Hackers recommended both, each requiring the other to fulfill its purpose. Few people would remove original chips without purchasing a kit and most would not buy a kit unless they intended to remove the chips. If there is a significant relationship between removal and replacement, their joint purposes and association may be relevant to statutory analysis.

In a satellite or cable TV piracy case, new chip insertion plainly circumvents a measure, decrypting or descrambling television signals for unauthorized viewers. Nothing so obvious appears here. Each Furby, though, communicates with its fellows by transmitting and receiving signals. While those signals seem unlikely to lend themselves to circumvention, modifications, including new chip insertion, might enable avoidance or bypass in ways not considered above. Whether Title 17 protects expressive elements other than source code (e.g., emission of sounds, expressed as the primitive vocabulary that Hampton created) may be relevant. It is plain, however, that § 1201(a) does not protect the toy’s gears and sensors. Nothing prohibits later acts affecting those, at least insofar as the acts are unrelated to unauthorized circumvention or trafficking. Subsequent conduct affecting the work or measure, whatever their location, could be actionable.

200. Both initial software and later hardware hacks sought to control the toy’s mechanisms. Both require chip removal. The chips were initially removed, however, because individuals targeted the copyright owners’ code as a means for controlling the toy. Their attorneys would focus on the later hardware hack, arguing it should be exempt. See SECTION-BY-SECTION ANALYSIS OF H.R. 2281, supra note 4, at 9 (“This provision is designed to... simultaneously allow the development of technology.”). But they must prove that a particular exemption applies.

201. Persons seeking access to the code would remove chips without replacing them.
IX. SECTION 1201(a)(2) VIOLATIONS: UNAUTHORIZED TRAFFICKING IN TECHNOLOGY

Overview

Section 1201(a)(2) makes unauthorized dealings in certain products and services ("items") illegal. Violations require a combination of items, acts, and purposes—none prohibited alone. This provision supplements § 1201(a)(1). It is designed to provide "meaningful protection and enforcement" of a copyright owner's access control rights. It is not intended to cover "normal household devices" that have "obvious and numerous commercially significant purposes and uses other than circumvention."

Items

The six listed items are "any technology, product, service, device, component or part thereof." These include hardware or software tools. An item's stage of development, its use and the descriptive terms applied by attorneys could affect how the courts label it.

(i) Technology

"Technology" (application of scientific knowledge to achieve a practical purpose) is a word that can apply in some sense to all Furby items. It can also serve as a "catch-all" description for items whose proper label is disputed; or, as used here, it refers generally to the statute's listed items as a group.

---


203. Section-By-Section Analysis of H.R. 2281, supra note 4, at 8.


205. 17 USC § 1201(a)(2) (2000). Section 1201(b), which targets prohibited conduct relating to copy control rather than access control, uses terms identical to those of § 1201(a)(2) when describing listed items and acts. The two provisions also use similar language when describing aspects of the prohibited purposes.

206. Section-By-Section Analysis of H.R. 2281, supra note 4, at 15 (§ 1201(a)(2) (circumvention tools include software and hardware)).

207. See Webster's Third New International Dictionary, supra note 7, at 2348. "Technological measure" (relevant to § 1201(a)(1) and (a)(2) foundations and violations) and "technology" (relevant to § 1201(a)(2) violations) might sound confusingly similar to jurors.
(ii) Product

“Product” (the result of work or thought)\textsuperscript{208} applies here to the toy’s circuit boards, later upgrade kits and computer code.

(iii) Service

“Service” (useful work)\textsuperscript{209} can apply to several items. These could include instructional text and photos to teach toy deconstruction, consulting, linking to other helpful websites\textsuperscript{210} (directing visitors to component suppliers, and to articles about hacking and upgrade kits), providing general support and software tips,\textsuperscript{211} and posting a programming manual.

Congress placed “service” in the list of items or material objects (products, devices and components) rather than in the list of activities. The term should thus refer to something that can be the object of a listed act. Persons can “provide” or “offer the public” educational text and photos, links, consultation and circumvention services.\textsuperscript{212}

(iv) Device

“Device” (something formed by design)\textsuperscript{213} can apply to printed circuit boards, chips, and the fully assembled upgrade kit.

\textsuperscript{208} WEBSTER’S THIRD NEW INTERNATIONAL DICTIONARY, supra note 7, at 1810 (“something produced by physical labor or intellectual effort: the result of work or thought”).

\textsuperscript{209} Webster’s Third New International Dictionary, supra note 7, at 2075 (“the performance of work commanded or paid for by another” or “action or use that furthers some end or purpose”).

\textsuperscript{210} Websites can offer or market expertise (service) as a product, offering skills, for money or notoriety, to test/circumvent other measures. See Hacking Furby, SLASHDOT (“Try coding something good and giving it away. The recognition you get might land you a job you wouldn’t have dreamed of.”) (on file with the author).

\textsuperscript{211} See generally Furby Upgrade homepage, supra note 67.

\textsuperscript{212} Internet postings teaching circumvention techniques may give rise to allegations of prohibited conduct. There is disagreement whether these represent a “service” (primarily designed to circumvent, or with only limited commercially significant purpose or use other than to circumvent) or the exercise of a first amendment right to publish a critique of a computer security measure. Cf. John A. Halderman, Analysis of the MediaMax CD3 Copy-Prevention System, Version 1.1, Oct. 6, 2003, at http://www.cs.princeton.edu/~jhalderm/cd3/. See generally Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001).

\textsuperscript{213} Webster’s Third New International Dictionary, supra note 7, at 618 (“something that is formed or formulated by design and use with consideration of possible alternatives, experiment, and testing . . . a piece of equipment or a mechanism designed to serve a special purpose or perform a special function”). See also FREEDMAN, supra note 5 (“Any electronic or electromechanical machine or component from a transistor to a disk drive. The term “device” always refers to hardware, never to software.”).
(v) Component, or part thereof

"Component" (a constituent element)\textsuperscript{214} has special meaning as it relates to software.\textsuperscript{215} A complete device (computer chip) can be a component in a larger computer system. Furby products or devices (circuit boards and kits) can also be viewed as components of the toy's interior mechanisms.

(vi) Summary of items

Several labels can be applied, redundantly, to the Furby upgrade mechanisms and services. This article treats the boards and kits as "products" and the information and support as "services." Dealing with items, however labeled, is actionable only if the items are associated with listed acts and purposes.

Acts

Five categories describe prohibited conduct or dealings in technology. While two of these are relatively narrow, three are broad and could encompass many activities not considered here. Subsection (a)(2) has been referred to as the "anti-trafficking" provision, although the acts covered are far broader than trafficking.

(i) Manufacture

"Manufacture" (to make something into a usable product)\textsuperscript{216} here describes construction of Furby's printed circuit boards and kits.

(ii) Import

"Import" (brining goods or services from abroad)\textsuperscript{217} applies to actions undertaken to obtain kit components such as the toy's printed

\textsuperscript{214} Webster's Third New International Dictionary, \textit{supra} note 7, at 466 ("a constituent part" and "either of the sequences defining an alphabet in cryptography"); \textit{id.} at 62 ("alphabet" means "\textit{j. cryptography}: a set of one-to-one equivalences between a sequence of plaintext letters and the sequence of their cipher substitutes: sometimes: one of these sequences—called also \textit{substitution alphabet, see VIGINÈRE CIPHER}).

\textsuperscript{215} Freedman, \textit{supra} note 5 ("One element of a larger system. A hardware component can be a device as small as a transistor or as large as a disk drive as long as it is part of a larger system. Software components are routines or modules within a larger system.").

\textsuperscript{216} Webster's Third New International Dictionary, \textit{supra} note 7, at 1378 ("Manufacture" means "to make (as raw material) into a product suitable for use.").

\textsuperscript{217} Webster's Third New International Dictionary, \textit{supra} note 7, at 1135 ("to bring from a foreign or external source . . . esp.: to bring (as wares or merchandise) into a place or country from another country"). Profit may not be required. \textit{Cf. United States v. LaMacchia}, 871 F. Supp. 535, 536 (D. Mass. 1994) (MIT student loaded copyrighted software onto the Internet, making it available to others at no charge).
circuit boards and chips. Circuit boards and chips, standing alone, however, have many commercially significant and legitimate purposes and uses. Plaintiffs must prove that such "neutral" items were imported for a listed purpose. While some hackers discussed conduct bearing the indicia of prohibited purposes, the author found no evidence associating those purposes and listed items with the act, importation. U.S. residents obtaining the kits, however, could have violated that prohibition.

(iii) Offer to the public

"Offer" (present or hold out for consideration) applies here to advertising Furby boards and kits on the Internet, communicating prices to journalists, and linking to a PayPal purchase site. (The computer code and manual were free.)

(iv) Provide

"Provide" (supply) applies here to shipping, mailing, or otherwise delivering the circuit boards and kits. It also refers to supplying the public with information by maintaining Internet websites with computer code, programming manual, and links.

(v) Traffic

"Traffic" (engage in dealings with) is a broad term, which could refer to selling or shipping, or to smuggling or posting on the Internet at no charge.

218. See, e.g., Furby Autopsy, supra note 53.
220. Webster's Third New International Dictionary, supra note 7, at 1827 ("to supply"). See also Reimerdes, 111 F. Supp. 2d at 325 ("to make it available or furnish it").
221. Reimerdes, 111 F. Supp. 2d at 324-25 (linking, in some instances, may constitute offering, providing, or otherwise trafficking in circumvention devices).
222. See Webster's Third New International Dictionary, supra note 7, at 2423 ("to engage in commercial activity: buy and sell regularly: TRADE or "to engage in illegal or disreputable business or activity" or "to carry on communication or negotiation: DEAL, BARGAIN"). Cf. United States v. Brady, 820 F. Supp. 1346, 1357 n.21 (D. Utah 1993) ("traffic," for purposes of access devices enabling unauthorized access to computers under 18 U.S.C § 1029(e)(5) (2000), is statutorily defined as "transfer, or otherwise dispose of, to another, or to obtain control of with intent to transfer or dispose of.")
223. Judge Kaplan defined traffic as follows:

To "traffic" in something is to engage in dealings in it, conduct that necessarily involves awareness of the nature of the subject of the trafficking. . . . The phrase "or otherwise traffic in" modifies and gives meaning to the words "offer" and "provide." In consequence, the anti-trafficking provision of the DMCA is
(vi) Summary of acts

There are grounds for alleging that some individuals manufactured, offered, and provided products (upgrade boards, kits, computer code) and provided services (programming manual, consultations, a moderated list, text and photos). Plaintiffs would apply every conceivable label to acts and items. Those charged would deny the applicability of these, offering their own labels, which do not fall under the statute. In any event, a violation occurs only if each combined act and item are associated with a prohibited purpose.

**Purposes**

Persons may not manufacture, import, offer to the public, provide or traffic in items that are (1) primarily designed or produced for unauthorized circumvention, (2) of only limited commercially significant purpose or use (except for circumvention), or (3) marketed for unauthorized circumvention. Purposes are thus considered at the level of design or production, purpose or use, and marketing. The tests are disjunctive; combined acts and items that fall within any one of these categories violate the statute. 224

(i) Primarily designed or produced for unauthorized circumvention.

Section 1201(a)(2)(A) prohibits actions to manufacture, import, offer to the public, provide or traffic in items (products or services) that are “primarily designed or produced for the purpose of circumventing.”225 Whether any individual primarily designed or produced for the purpose of circumventing.

---

225. 17 U.S.C. § 1201(a)(2)(A) (2000). Designing and producing are listed in the context of purposes, not acts. This suggests that one could design or produce an item if he does not manufacture, import, offer to the public, provide or traffic in it. The statute prohibits dissemination of items (products and services), not conception of them.
226. Webster's Third New International Dictionary, supra note 7, at 1800 (“primarily” means “first of all”). See also SECTION-BY-SECTION ANALYSIS OF H.R. 2281, supra note 4, at 10–12 (manufacturers should refrain from designing products primarily for circumvention).
227. Webster's Third New International Dictionary, supra note 7 at 611 (“design” means “to conceive and plan out in the mind” or “to create, plan, or calculate for serving a predetermined end”).
produced\textsuperscript{228} items to circumvent the epoxy coatings is the issue. Any method would suffice, including a direct attack on the measure or seeking alternative avenues around it. If other purposes were of primary significance, defendants may deny liability under this provision.

Some individuals coordinated their activities and shared a common purpose. Yet liability, if any, for design and production conduct must be considered independently for each person. The statute’s only “in concert” language applies to \textsection1201(a)(2)(C) marketing. Liability for vendors or production mills must also be individually determined. Each person could have engaged in a variety of acts for different purposes.

Furby hackers designed and produced kits in order to manipulate unprotected toy hardware and sensors. By then, some had abandoned efforts to circumvent the epoxy. The Internet text and photos\textsuperscript{229} could have been used, however, for both circumventing and non-circumventing purposes. A court may enjoin posting of text and photos if those are seen as “part of a course of conduct the clear purpose of which is the violation of law.”\textsuperscript{230} Individuals who can assert a primary non-circumventing purpose for designing and producing the upgrade kits have a promising defense. Plaintiffs could assert, however, that the conduct is permissible only if an exemption is established under \textsection1201(f). Evidence of previous commercial activity and non-circumventing uses furthered by the new design might enhance their position. Ideas posted only while a technological measure is a “hot item” may be less persuasive.\textsuperscript{231} In any event, since

\begin{footnotesize}
\bibitem{228} Webster’s Third New International Dictionary, supra note 7 at 1810 (“produce” means “to cause to have existence or to happen: bring about” or “to compose, create, or bring out by intellectual or physical effort”).

\bibitem{229} Furby Upgrade homepage, supra note 67, Prepping the Baseboard (“The boards may be held in place with some silicone (sic) adhesive - you can pry this stuff off before continuing.... The desoldered boards should slip out of their slots in the base board.... Cut the wires.... Remove.... Replace....”). Arguably, chip removal was incidental; the kits were primarily created to teach others to develop and use new software to control the toy’s mechanics. Removal, however, was the required basis for kit use. The statute does not exempt incidental, or de minimis, circumvention. Those charged with a violation could counter that the kits were not designed or produced for the purpose of removing the chips and epoxy; they were simply installed afterwards.


\bibitem{231} Some courts may not find “research” (interwoven with comments about hacking, spoofing, tricking the toy, and crashing the processor) characteristic of non-circumventing activity.
\end{footnotesize}
the three purposes tests are disjunctive, any defendant’s acts must also be considered under the remaining two provisions.

(ii) Limited commercially significant purpose or use beyond circumvention.

Section 1201(a)(2)(B) prohibits conduct to manufacture, import, offer to the public, provide or traffic in items that have “only limited commercially significant purpose” or use other than” circumvention. An acceptable item must have a purpose or use other than circumvention. What if it has multiple purposes or uses, both circumventing and non-circumventing? The statute’s language may be viewed as ambiguous. The following analysis approaches §1201(a)(2)(B) as a two-pronged test, requiring that an item have: (a) purpose or use other than circumvention and (b) more than “only limited” commercial significance. Items that clear both hurdles are safe, although the hurdles’ dimensions are uncertain.

Purpose or use other than circumvention.

The listed item—“any technology, product, service, device, component, or part thereof”—must have purpose or use other than circumvention. A few decisions indicate that the statute does not protect multiple purpose or use items (“multi-purpose items”). Litigants, however, can assert conflicting interpretations of this provision.

Section 1201(a) extends legal protection to qualified technological measures. It’s illogical to ignore circumventers who intend to make a lot of money just because they can demonstrate an additional non-circumventing purpose or use. Congress did not provide an express exemption for multi-purpose item production or manufacturing.
design. Requiring commercial significance for these, moreover, would not adequately protect copyright owners. Defendants would happily offer evidence of their personal yardsticks for measuring commercial significance. Congress drew boundaries for freedom of design, which, under § 1201(c)(3), must "not otherwise fall within the prohibitions of subsection (a)(2) or (b)(1)." Additionally, an interpretation favoring lucrative multi-purpose items would conflict with §1204. That statute criminalizes § 1201 violations committed "willfully and for purposes of commercial advantage or private financial gain." Thus, from a plaintiff's perspective, all of these things suggest that § 1201(a)(2)(B) does not protect multi-purpose items.

The statute's language, however, does not modify "purpose" or "use" with any article or adjective (such as "a," "the," "only," or "sole,") that suggests Congress contemplated only single purpose or use items. The language can be interpreted to permit multi-purpose items if a non-circumventing purpose or use has more than "only limited" commercial significance.\(^2\)\(^3\)\(^5\) The statute does not expressly prohibit the design, production, purpose or use of any multi-purpose items. Consider the § 1201(a) and (b) examples described in the legislative history. These can be thought of as marking the furthest boundaries of the acceptable and unacceptable under the statute. The statute is not "aimed at widely used staple articles of commerce, such as the consumer electronics, telecommunications, and computer products—including videocassette recorders, telecommunications switches, personal computers, and servers—used by businesses and consumers everyday for perfectly legitimate purposes."\(^2\)\(^3\)\(^6\) Instead, it

---


A device is prohibited under section 1201 only if it is primarily designed or produced to circumvent, has limited commercially significant use other than to circumvent, or is marketed specifically for use in circumventing. This formulation means that under H.R. 2281, it is not enough for the primary effect of the device to be circumvention. It therefore excludes legitimate multi-purpose devices from the prohibition of section 1201.


is aimed at "so-called 'black boxes'—devices with no substantial non-infringing uses that are expressly intended to facilitate circumvention of technological measures for purposes of gaining access to or making a copy of a work." Congress did not intend to block the manufacture of "normal household devices" with "obvious and numerous commercially significant purposes and uses other than circumventing." The legislators held the door open for new technological developments. Legislative comments about businesses and consumers, those interested in purchasing, refer to changeable customers. Marketable items can be considered along a continuum, ranging from legislatively favored items (widely used staple articles with ordinary legitimate uses) to disfavored ones (those with a circumvention purpose or use only). One can easily imagine an item with characteristics between the two extremes, available for ordinary uses by consumers and providing an additional circumventing use.

The above arguments illustrate possible conflicting interpretations of § 1201(a)(2)(B). Future cases are likely to consider whether multi-purpose items should be allowed if non-circumventing and circumventing aspects have more than "only limited" commercial significance. It takes more than a circumventing purpose or use to violate this provision. That purpose or use must lack commercial significance.

In this case, Peter van der Linden, the Furby contest sponsor, articulated the first purposes or uses beyond or "other than" circumvention. He described educational uses, speculating that an altered toy could be used to teach engineering students or autistic children. The public record doesn't indicate whether these things

---

Cir. 2001) (district court opinion noted that "statute . . . prohibits 'any technology,' not simply black boxes")


240. In one instance, a felt tip marker was used to circumvent Key2Audio, a technology that prevented copying and conversion of songs to MP3 files. Cheap pen cracks 'copy-proof' CD, REUTERS, May 20, 2002, at http://zdnet.com.com/2102-1105-917908.html; Brendan I. Koerner, Can You Violate Copyright Law With a Magic Marker?, SLATE, June 3, 2002, at http://slate.msn.com/id/2066527. No one has proposed outlawing felt tip markers. The unanticipated circumventing use was incidental to a long-established alternative purpose.
were actually done.\textsuperscript{241} Those who duplicated Gibbons’ actions could also claim an educational purpose and use, arguing that they tried to learn valuable information by working with the toy, creating computer code for new uses and later seeking to teach others.\textsuperscript{242} They could characterize the chip removal text and photos as part of their efforts to create pioneering computer code and teach others how to program their own toys. If they could also establish commercial significance, that might protect them from § 1201(a)(2)(B) charges.\textsuperscript{243}

\textit{Commercial significance}

Actual or hoped-for profits alone are not a defense. Commercial purposes, large or small, create a risk of criminal penalties for persons who willfully violate § 1201.\textsuperscript{244} The statute’s language is sparse. No dollar limit or percentage provides a yardstick by which to measure “only limited” commercial significance. Revenues meaningless to a large business could be very important to individuals. But some evidence must be provided. Remarks here about hacking for fun and gaining only “beer money” do not suggest “obvious and numerous commercially significant purposes and uses other than circumventing.” Whether § 1201(a)(2)(B) covers single or multi-purpose items, prohibited conduct that lacks commercial significance poses a risk of liability.\textsuperscript{245}

\textsuperscript{241} Cf. Universal City Studios, Inc. v. Reimerdes, 82 F. Supp. 2d 211, 217 (S.D. N.Y. 2000) (prelim. injunction) (“no evidence of any commercially significant purpose of DeCSS other than circumvention of CSS”).

\textsuperscript{242} Query whether self-education and “educating” roughly 100 other people would be treated as non-circumventing purposes. Cf. 144 Cong. Rec. E2136, E2137 (daily ed. Oct. 13, 1998) (statement of Rep. Billey) (“widely used staple articles of commerce, such as the consumer electronics, telecommunications, and computer products”). Teaching might be an acceptable “service” if unauthorized circumvention is not the skill taught. Commercial significance must also be established.

\textsuperscript{243} In all kinds of cases under the statute, defendants’ initial strategy would be to deny that each item, act, and purpose falls within the prohibited categories. Alternatively, they would claim that even prohibited items, acts or purposes do not expose them to liability under § 1201(a)(2)(B) if these had an additional commercially significant purpose or use.


\textsuperscript{245} Charts can help analyze the statute’s elements. Items with single and multiple circumventing and non-circumventing purposes or uses could be placed on one axis while categories with commercial significance or financial gain are placed on another. Each item’s intersection of purpose or use with commercial value—or its failure to intersect—can be examined when analyzing a § 1201(a)(2)(B) or § 1204 allegation.
(iii) Marketing a product for use in circumventing technology.

Section 1201(a)(2)(C) prohibits conduct to manufacture, import, offer to the public, provide or traffic in items (products or services) that are "marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing" a technological measure. Published articles, email and websites name several people who helped develop, publicize and link to the original upgrade boards and kits, as well as linking to a PayPal purchasing site. More than two individuals, therefore, could be charged with acting in concert to market the products.

Plaintiffs could argue that marketers need not know of, and plaintiffs need not prove, a purchaser's actual use. Plaintiffs need only establish the use promoted. In this case, that strategy would benefit defendants. Some individuals marketed upgrade kits by posting information, creating links, and communicating with journalists. One journalist wrote that the toy's "original programming is unavailable as the hack replaces the original chips and circuit board." A hacker was reportedly "working on developing a standard software interface for the Furby modification [to] allow less technical programmers to control the robotics." These reports suggest something beyond efforts to gain access to a protected work or to otherwise circumvent a technological measure. Individuals

246. 17 U.S.C. § 1201(a)(2)(C) (2000). The statute doesn't define "marketed." One authority defines "market" as "to expose for sale in a market; traffic in; sell in a market." WEBSTER'S THIRD NEW INTERNATIONAL DICTIONARY, supra note 7, at 1383. Trafficking is of concern, however, even when no money changes hands. Digital and analog works are often taken without authorization and distributed at little or no charge. It is unclear whether "market" will be defined to require an exchange of consideration. Many things have value other than money, including future employment opportunities, reputation or notoriety. As the "Hack Furby" sponsor noted, "The cash prize [of $250] is just a token.... The real prize is the bragging rights to the accomplishment, and the benefit of sharing it with the world." van der Linden, supra note 62. Instances of little or no compensation, however, can be addressed under §1201(a)(2)(B) ("providing" items with "only limited commercially significant purpose or use").

247. Cf. United States v. Gee, 226 F.3d 885, 897 n.11 (7th Cir. 2000) ("jury was not required to find that the black boxes were sold for the sole and specific purpose of cable piracy, nor that the boxes were actually used illegally. ... only needed to find that [defendant] intended the black boxes to be used for the unauthorized reception of cable service when he sold the boxes to [his customer].") (quoting United States v. Gardner, 860 F.2d 1391, 1399 (7th Cir. 1988)). Hackers can argue that they promote a use other than circumvention.


249. Id.
charged with a violation would face a problem, however, since the statute prohibits removal of a measure.

The statute requires that the items be marketed "for use in circumventing." Arguably, the upgrade kits were not used to remove the chips, and the text and photos were not "marketed." The statute, by referring to "use in circumventing, however," does not seem to require that a device or item be used for each act of circumvention. Using an item at any step of the way, as one part of a series of related acts, might suffice. There are many unknowns. Liability could depend on whether acts that occur after circumvention are treated as occurring in isolation or as part of a related transaction or process.

Summary of potential violations

The facts support at least one § 1201(a)(1) allegation of unauthorized circumvention, probably removal. A plaintiff could also assert that new chip installation avoids or bypasses a technological measure if some protected work remains or removal and replacement are treated as integral parts of a related transaction. If a new chip enables communication with other Furbys or devices, and thereby circumvents additional technological measures, that would also be relevant. Since efforts to hack the toy occurred over a two year period, other evidence of prohibited conduct may exist.

Hackers have potentially good arguments to defend against § 1201(a)(2)(A) charges of prohibited kit design and production. Their goals were far more ambitious than simple chip removal. In circumstances where new chips circumvent technological measures, however, such as in certain kinds of signal piracy, this conduct would expose defendants to greater risk of liability and probably would require compliance with § 1201(f). It would also be hard to defend against § 1201(a)(2)(B) charges of improper purpose and use. A jury is not likely to see "beer money" revenues as commercially significant. The record is silent about additional efforts to help autistic children, with or without commercial significance. The facts and arguments seem more evenly balanced with respect to § 1201(a)(2)(C) charges that the kit is marketed "for use in circumventing."

250. Webster's Third New International Dictionary, supra note 7, at 1139 ("in" can be defined as "used as a function word to indicate activity, occupation, or purpose").
X. COUNTING VIOLATIONS AND WEIGHING COSTS

Actual or statutory damages are based on "each violation." Criminal fines and imprisonment are based on a "first offense" and "any subsequent offense." The number of acts, and how these are counted, affects liability. In the case of Furby, two daughterboards with coated chips were removed from each toy. Many different prohibited acts probably occurred over the two year period before the contest was won.

Descriptions and labels matter. A client could describe his activities as "hacking" and sharing tips with his buddies. But a judge might view Internet postings as providing or otherwise trafficking in services. Different perspectives may affect choice of statutory provision and relevant effective date. Products can also be developed and analyzed in many stages. A programming manual might be labeled a "product" when created or a "service" when maintained on the Internet. Defendants would argue that publishing, not producing, is the proper label, and that publishing is not covered by the statute. Litigants will contest proper characterization of acts, items, and purposes, as well as counting of offenses.

251. Statutory damages for "each violation of section 1201" are "not less than $200 or more than $2,500 per act of circumvention, device, product, component, offer, or performance of service, as the court considers just." 17 U.S.C. § 1203(c)(3) (2000). Repeated violations, occurring "within 3 years after a final judgment . . . for another such violation," provide a basis for triple damages. 17 U.S.C. § 1203(c)(4) (2000). Cf. 18 AM. JUR. 2d Copyright and Literary Property § 237 (1985) ("Expert testimony may be useful to determine whether . . . infringing activity constituted a single or a multiple infringement, affecting the amount of damages" under 17 U.S.C. §504(c).)

252. 17 U.S.C. §§ 1204(a),(b) (2000) (A fine of not more than $500,000 or imprisonment not to exceed 5 years, or both, may be provided "for the first [criminal] offense," with increased penalties for subsequent offenses). Criminal statutes are strictly construed. See generally Singer v. United States, 323 U.S. 338, 341-42 (1945). Section 1201 violations are criminal if made "willfully and for purposes of commercial advantage or private financial gain." 17 U.S.C. § 1204(a). Because § 1201(a) lists but does not define illegal acts, and even experts may not share a "common" vocabulary, defendants could assert lack of adequate notice of the kind of conduct subject to criminal penalty. Cf. Dowling v. United States, 473 U.S. 207, 214 (1985) ("it is appropriate . . . to require that Congress should have spoken in language that is clear and definite.") Rather than focusing on lack of definitions alone, it may be useful to ask whether the § 1201(a) criteria provide sufficient notice of acts subject to criminal penalty. Dictionaries are only one source of information. Whether a consensus exists about a range of definitions or the nature of activities within a field might be relevant. Moreover, some defendants create their own code words or language to conceal what they are doing. Words serve many purposes and may camouflage as well as communicate, highlighting the need to consider conduct in context as well as language.

253. Cf. United States v. Pirello, 255 F.3d 728, 731-32 (9th Cir. 2001) ("by placing a classified ad on the Internet, Pirello was able to solicit funds instantaneously and continuously from over 200 million individuals worldwide").
Section 1201(a)(1) lists seven prohibited acts. Even if only one technological measure protects a work, several circumvention methods may be attempted. Section 1201(a)(2) lists eleven categories of items and acts, together with three improper purposes that cover at least five levels of inquiry (design, production, purpose, use and marketing). The statute casts a wide and intricate net. To aid analysis, counsel can design charts. Placing listed items on one axis and listed acts on another, relevant purposes may be considered where these intersect.

In Reimerdes, a teenage boy, and those who followed in his footsteps, compromised a system of copy protection and significantly threatened copyright owners' control over their works and revenues. The Furby hardware hack does not appear to have injured present revenues or future opportunities. Millions of toys were manufactured and sold. Only an estimated 100 or more upgrade kits were produced. Several legal and business factors probably discouraged action against the hackers and U.S. purchasers. But that will not always be the case.

XI. CONCLUSION

Intellectual property assets are flooding across the world in digital form. This revolutionary change in how creative expression is preserved, communicated and distributed has enormous implications for those who create and those who use original works of authorship. Section 1201(a) can serve as a powerful tool, partially governing individual and commercial conduct at gateways that control access to information streams. Technological protections alone are insufficient. The extent of legal protection under the statute is unclear. Section 1201(a) seeks to bring order out of chaos by regulating targeted conduct. Copyright owners and information users disagree about the propriety of the conduct that enables information users to seize control over creative works in digital and analog form. Copyright owners may not know of unauthorized conduct and often cannot act quickly enough to protect their interests. Information users seeking the boundaries for permissible conduct, for their part, will be troubled by the lack of definitions. Moreover, the statute regulates some conduct without regard to motive or purpose, presenting traps for the unwary. When the courts apply the statute to different technologies, additional ambiguities will probably become apparent. The statute's flexible language and ambiguities, however, offer opportunities to shape the evolution of the law in the coming years.