JOSEPH M. BURTON (SB No. 142105)
STEPHEN H. SUTRO (SB No. 172168)
DUANE MORRIS LLP
100 Spear Street, Suite 1500
San Francisco, CA 94105
Telephone: (415) 371-2200
Facsimile: (415)371-2201

Attorneys for Defendant
ELCOMSOFT COMPANY, LTD.

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

UNITED STATES OF AMERICA

Plaintiff,

v.

ELCOM LTD.,
a/k/a ELCOMSOFT CO., LTD.,

Defendant.

Case No.: CR 01-20138 RMW

MOTION TO DISMISS INDICTMENT FOR VIOLATION OF DUE PROCESS

Date: April 1, 2002
Time: 9:00 a.m.
Judge: The Honorable Ronald M. Whyte

MOTION

Defendant Elcomsoft Company, Ltd. moves this Court for an Order dismissing the indictment. As grounds therefore, Elcomsoft asserts that the statute upon which the charges against it are based violates the Due Process clause of the Fifth Amendment to the Constitution of the United States. Specifically, Elcomsoft asserts that 17 U.S.C. Section 1201(b)'s prohibitions are not clearly defined, and it is therefore unconstitutionally vague.

The prosecution in this case is based on the premise that the Digital Millennium Copyright Act prohibits, under any circumstance, the circumvention of technologies which are used to protect the rights of copyright holders in their works. This is fundamentally incorrect. The legislative history of the Digital Millennium Copyright Act makes clear that circumvention of these technologies is permitted for the purpose of enabling fair use copyrighted works by persons who have lawfully acquired them.

Section 1201(b) of the Digital Millennium Copyright Act prohibits the manufacture and sale of software tools which are intended to facilitate unlawful circumvention of protective technologies. Elcomsoft is a software company that manufactured and sold software tools which were intended to be used, and in fact were used to accomplish the lawful circumvention of protective technologies. However, because of Section 1201(b)'s failure to clearly define which software tools it prohibits, Elcomsoft could not know, with any reasonable certainty, if its lawful conduct was meant to be included within the statutory proscription.

The failure of a statute, particularly one which carries criminal consequences, to clearly define the conduct it proscribes and thereby ensnare innocent law-abiding individuals is the essence of constitutional vagueness, and the basis for Elcomsoft's motion.

MEMORANDUM OF LAW

I. BACKGROUND

A. THE INDICTMENT.

On August 28, 2001, Elcomsoft was indicted for alleged violations of Sections 1201(b)(1)(A) (a device "primarily designed or produced for the purpose of circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner") and 1201(b)(1)(C) (a

device "marketed . . . for use in circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner").

The Indictment charges that "the primary purpose of [AEBPR] was to remove any and all limitations on an ebook purchaser's ability to copy, distribute, print, have the text read audibly by the computer, or any other limitation imposed by the publisher or distributor of an ebook in the eBook Reader format, as well as certain other ebook formats." (Indictment, ¶ 2, at p. 2:22-25). The Indictment otherwise charges that Elcomsoft made this program available for sale on the Internet. (Indictment, ¶3, at pp. 2:26-3:4).

B. THE ADOBE SYSTEMS eBOOK READER.

Adobe Systems, Inc., ("Adobe") is a software company headquartered in San Jose, California, that produces publishing software for various media. (Indictment, pg. 1:27 - pg. 2:1). Adobe distributed a product titled "Adobe Acrobat eBook Reader" that provided technology for the reading of books in digital form ("ebooks") on personal computers. (Indictment, pg. 2:6-7).

"When an ebook purchased for viewing in the Adobe eBook Reader format was sold by a publisher or distributor, the publisher or distributor of the ebook could authorize or limit the purchaser's ability to copy, distribute, print, or have the text read audibly by the computer. Adobe designed the eBook Reader to permit the management of such digital rights so that in the ordinary course of its operation, the eBook Reader effectively permitted the publisher or distributor of the ebook to restrict or limit the exercise of certain copyrights of an owner of the copyright for an ebook distributed in the eBook Reader format." (Indictment, pg. 2:14-20).

According to Adobe promotional material, the Adobe eBook Reader was designed with encryption technology and digital rights management software to secure and manage eBooks. Adobe explained that the software "includes the highest level of encryption technology, licensed from RSA Laboratories." (Declaration of Joseph M. Burton, Ex. A, document titled "Adobe Solutions for the eBook Market," at 000041).

///

///

///

C. ELCOMSOFT CO. LTD.

1. The Company.

Elcomsoft Co. Ltd. ("Elcomsoft") is a privately owned software development company headquartered in Moscow, Russia. Established in 1990, Elcomsoft produces Windows productivity and utility applications for businesses and individuals. In particular, Elcomsoft provides state-of-the-art computer forensics tool development, computer forensics training, and computer evidence consulting. Since 1997, Elcomsoft has developed and provided forensic software tools to law enforcement, military and intelligence agencies worldwide, including to law enforcement in the United States.[1] These software tools are also used by some of Fortune 500 corporations, many branches of the military all over the world, foreign governments, and major accounting firms. Elcomsoft is a member of the Russian Cryptology Association (RCA) and a lifetime member of the Association of Shareware Professionals (ASP). Elcomsoft is also a Microsoft Independent Software Vendor (ISV) partner. Katalov Decl., ¶¶ 2-4.

One line of software in which Elcomsoft has specialized is password recovery software. This software allows a user to recover a password that has been lost, forgotten, or destroyed. For instance, a corporation may use the software when a former employee has left the corporation without un-protecting his or her files. Likewise, a government may use the software in the investigation of a crime. Elcomsoft's software allows recovery of passwords for files created in most popular applications, including Corel WordPerfect Office, Lotus SmartSuite, Intuit Quicken, and Microsoft Office and WinZIP. Elcomsoft also has a product that decrypts protected Adobe Acrobat PDF files[2] which have an "owner" password set, preventing the file from being edited and/or printed. Through

///

---

[1] For example, after Elcomsoft software helped local officials in Fort Bend, Texas, solve a crime they were investigating, the Sheriff's Office appointed an Elcomsoft employee "Honorary Deputy Sheriff." Declaration of Alexander Katalov, Ex. A.

[2] PDF (Portable Document Format) is a file format that has captured all the elements of a printed document as an electronic image such that a user can view, navigate, print, or forward the document to someone else. PDF files may be created using Adobe Acrobat, Acrobat Capture, or similar products. To view and use the files, a user needs Adobe Acrobat Reader. PDF files are especially useful for documents such as magazine articles, product brochures, or flyers in which a viewer wants to preserve the original graphic appearance online.

the use of Elcomsoft's product, the protected file may be opened in any PDF viewer without restrictions. Katalov Decl., ¶ 5.

2. The Advanced eBook Processor ("AEBPR").

On June 20, 2001, Elcomsoft released the Advanced eBook Processor ("AEBPR"), a Windows-based program that allowed a lawful user to remove usage restrictions from Adobe Acrobat PDF files and the Adobe eBook Reader. The AEBPR program permits a legitimate purchaser of an e-book formatted in the Adobe Acrobat e-book reader format to convert that e-book from the Adobe e-book reader format to a format readable in any PDF viewer without restrictions. Katalov Decl., ¶ 6. As such, the conversion accomplished by the AEBPR program enabled a legitimate purchaser of an e-book to exercise his or her rights of fair use under the copyright laws by allowing the lawful owner of an ebook to read it on another computer, make a back-up copy, print the ebook, etc.

Importantly, this product was not sold by Elcomsoft to allow *unlawful* distribution of copyrighted works. Rather, Elcomsoft sold the product to allow *a lawful* owner to have more freedom to read the book how and/or where the owner wanted. In its press release, Elcomsoft explained the AEBPR:

> The latest addition to Elcomsoft's family of password recovery software allows business managers to deal with lost and destroyed passwords, as well as with employees who, intentionally or unintentionally, are unable to edit and print password-protected PDF files.
>
> Advanced eBook Processor lets users make backup copies of eBooks that are protected with passwords, security plug-ins, various DRM (Digital Rights Management) schemes like EBX and WebBuy, enabling them to be readable with any PDF viewer, without additional plug-ins. *In addition, the program makes it easy to decrypt eBooks and load them onto Palm Pilot's and other small, portable devices. This gives users - especially users who read on airplanes or in hotels - a more convenient option than using larger notebooks with limited battery power to read their eBooks. . . .*
>
> Advanced eBook Processor protects businesses from losing control of their eBooks, technical articles, documentation manuals, presentations, and all PDF documents that could be rendered unusable by improperly managed passwords and licenses.

Katalov Decl., Ex. B (June 22, 2001 Press Release) (emphasis added). Elcomsoft further explained on its web site that the AEPBR only worked with eBooks that were *legally owned* and was priced in a manner that would protect "unauthorized distribution of eBooks on the piracy market:"

> This program *only* works with eBooks you legally own, *i.e.* purchased from one of online stores like Amazon or Barnes & Noble. So we are absolutely sure that the owner of the eBook has all rights to read the book he *purchased* where he wants and how he wants.
>
> The demo version of AEBPR allows to convert only first 10% of the book content. *To protect unauthorized distribution of eBooks on the piracy market, we have set the "border" price for this program – $99, which is much more than the eBook cost (most eBooks are being sold from $10 to $30, and there are a lot of free ones).*

Burton Decl., Ex. B. (emphasis added).

The AEBPR was offered for sale by Elcomsoft on the Internet for only a few weeks.[3] At no point was the software marketed for an *unlawful* purpose.[4] Indeed, following complaints from Adobe and allegations that the software violated the DMCA, Elcomsoft directed Register Now – the internet site that sold AEBPR – to remove the product from its internet site.[5] *See, e.g.,* Burton Decl., Ex. C, July 16, 2001 Statement of Elcomsoft Employee Dmitry Sklyarov to the FBI, at 000108 ("SKLYAROV stated that [the AEBPR] was sold commercially for a short period of time over the Internet by ELCOMSOFT for an amount of $99.95 but after Adobe Inc. complained, it was no longer sold").

3. The Lawful Uses of AEBPR.

Consistent with its advertising of the AEBPR, Elcomsoft is aware of no *unlawful* use of AEBPR. Nor has evidence of such unlawful use been revealed in the discovery provided by the

---

[3] The indictment charges that sales were made over the Internet through the use of an on-line payment service, "RegNow:"

> [D]efendant Elcomsoft and others made the AEBPR program available for purchase on the Elcomsoft.com website. Individuals wishing to purchase the AEBPR program were permitted to download a partially functional copy of the program from the Elcomsoft.com and then were directed to pay approximately $99 to an online payment service, RegNow, based in Issaquah, Washington. Upon making a payment via RegNow website, Elcomsoft and other persons provided purchasers a registration number permitting full use of AEBPR program. Indictment, para. 3.

[4] If Elcomsoft sought for others to use the AEBPR for unlawful purposes, it very well could have posted its product and the code on the Internet for free. Ironically, under those circumstances, no criminal charges could have been brought against Elcomsoft because it would not have published the code for financial gain. *See* Section 104 (criminal penalty for those who violate Section 1201 wilfully and for financial gain).

[5] Before that time, however, Register Now apparently had posted a notice on its web site that the software was only for use with eBooks which were owned by the user. Burton Decl., Ex. D, September 5, 2001 FBI Interview of Aaron Mathieson.

government to date. In contrast, although Elcomsoft does not have the resources of the United States government, Elcomsoft has been made aware of many lawful uses of the AEBPR, as follows:

- One purchaser of AEBPR worked in the insurance business. This individual purchased an eBook for use on his laptop that contains information that he uses and needs when he is out in "the field." The individual does not know anything about computers. Within a week or two of normal use, the eBook stopped working and was not reliable for him to use "in the field." Several attempts were made to contact the publisher's technical support, with no luck. The user was given the option of purchasing the eBook again, despite the publisher's prior statements that the individual was authorized to not only use the eBook, but to load it onto one other machine. Further attempts were made to contact the publisher, again with no luck. Not wanting to purchase the eBook again and risk the same problem, AEBPR was purchased and the problems with the eBook ceased; the eBook is now fully functional in "the field." Burton Decl., Ex. E, August 28, 2001 E-mail from Aaron Mathieson.[6]
- One purchaser of AEBPR was a Mortgage Loan Document Company. The company was working to convert their loan documents to the Adobe PDF format and needed to determine if the Adobe software encryption was secure. The company purchased the AEBPR to test PDF encryption. The company used AEBPR and determined that the PDF encryption was not secure. The company therefore did not post PDF documents on the Internet.[7] Burton Decl., Ex. F, August 31, 2001 FBI Interview of Stephen Richard Levine.
- One person sought a copy of AEBPR in order to gain access to malfunctioning eBooks that he had purchased from Barnes & Noble. The user explained that in May, 2001, he had downloaded and activated the Adobe Reader "from Barnes & Noble, along with about $150 in e-Books in both formats." The user then experienced problems with his computer and purchased a new computer. But the user no longer had "access to the e-Books that [he] paid for." The user explained that Adobe and Barnes & Noble failed to respond to his inquiries

---

[6] The FBI also has interviewed Mr. Mathieson. Burton Decl., Ex. D, September 5, 2001 FBI Interview of Aaron Mathieson.

[7] "Security Testing" is authorized by the DMCA. 17 U.S.C. § 1201(j).

and that he could not "afford to buy the same books all over again." Burton Decl., Ex. G, July 5, 2001 E-Mail.

- The State of Wisconsin sought a copy of AEBPR in order to resolve the problem of "content being restricted to the computer that was used to download the ebook." The State of Wisconsin explained that "[w]ithout a method of moving content to new computers as old computers are replaced [the Adobe e-Book] format would not be an option." Burton Decl., Ex. H, July 6, 2001 E-Mail from State of Wisconsin.
- One individual sought a copy of AEBPR on behalf of SunGard eSourcing. The employee wanted AEBPR to create a "one stop document with reference material" from eBooks for the employee's department. Burton Decl., Ex. I, July 5, 2001 E-Mail from SunGard eSourcing.
- One individual sought a copy of AEBPR on behalf of Time Warner Communications. The individual wrote content for www.pocketnow.com (a portable computer-related site) and recognized that AEBPR was "very relevant to mobile computing and portable electronic content." Burton Decl., Ex. J, July 5, 2001 E-Mail from Time Warner Communications.
- After purchasing a number of electrical engineering eBooks for use with Adobe eBook Reader, an e-Book owner's Adobe e-Book Reader "crashed." Adobe would not assist the e-Book owner in restoring the books that he had purchased. The individual sought a copy of AEBPR from Elcomsoft. Burton Decl., Ex. K, July 14, 2001 E-Mail from Daniel Bailey.

Of course, the *lawful* use of AEBPR was not limited to the private sector. Among the purchasers of AEBPR was the *United States government*. Records produced by the government in this case indicate that the celebrated Los Alamos Nuclear Laboratories purchased AEBPR. This purchase was made with the use of a government credit card issued to the government employee that was responsible for purchases for the Solid Waste Division at Los Alamos, New Mexico, e-mail: Ggg@lanl.gov. Burton Decl., Exs. L and M. Although it is unclear what the government intends to use AEBPR for, the DMCA specifically exempts "an employee of the United States" from liability for "any lawfully authorized investigative, protective, information security, or intelligence activity." 17 U.S.C. § 1201(e).

///

In sum, Elcomsoft is aware of no evidence of unlawful uses of AEBPR. Rather, the lawful uses for AEBPR are well documented.

II. CIRCUMVENTION OF USAGE CONTROLS IS LAWFUL UNDER THE DIGITAL MILLENNIUM COPYRIGHT ACT

A. STATUTORY STRUCTURE.

Critical to understanding the basis for Elcomsoft's due process claim is the fact that the Digital Millennium Copyright Act *does not* prohibit the circumvention of technological measures which protect the rights of a copyright owner under the copyright act. These particular rights which are referred to as "usage control rights" in this brief. Congress treated usage control rights, for reasons fully explained below, differently than it did a copyright owner's right to control *access* to his works.

On October 28, 1998, the United States enacted the Digital Millennium Copyright Act (the "DMCA"), Pub. L. 105-304 (1998). The DMCA represents an expansion of traditional copyright law by Congress in recognition of the fact that in the digital age authors are compelled to employ protective technologies in order to secure their works from unauthorized actions. Congress therefore developed a structure designed to prohibit efforts to unlawfully circumvent these protective technologies. Title I of the Digital Millennium Copyright Act added a new Chapter 12 to Title 17 U.S.C. (the Copyright Act). The new anti-circumvention prohibitions are contained in the three distinct provisions of Section 1201 of Chapter 12 of 17 U.S.C.

The principal anti-circumvention prohibition is contained in Section 1201(a)(1)(A) which provides that: "No person shall circumvent a technological measure that effectively controls access to a work protected under this title." *Id.* Under this provision, the mere *act* of circumventing access controls is unlawful. As such it represents an entirely new form of copyright law violation. One that is separate and distinct from copyright infringement.

The second prohibition is found in Section 1201(a)(2) which states:

> (2) No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that -
>
> > (A) is primarily designed or produced for the purpose of circumventing a technological measure that *effectively controls access* to a work protected under this title;

> (B) has only limited commercially significant purpose or use other than to circumvent a technological measure that *effectively controls access* to a work protected under this title [17 U.S.C.A. § 1 et seq.]; or
>
> (C) is marketed by that person or another acting in convert with that person with that person's knowledge for use in circumventing a technological measure that *effectively controls access* to a work protected under this title.

Id. (emphasis added).

The final prohibition is the legal foundation upon which the indictment in this case rests. Section 1201(b) provides :

> (1) No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that -
>
> (A) is primarily designed or produced for the purpose of circumventing protection afforded by a technological measure that effectively *protects a right* of a copyright owner under this title in a work or a portion thereof;
>
> (B) has only limited commercially significant purpose or use other than to circumvent protection afforded by a technological measure that effectively *protects a right* of a copyright owner under this title in a work or a portion thereof; or
>
> (C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing protection afforded by a technological measure that effectively *protects a right* of a copyright owner under this title in a work or a portion thereof.

Id. (emphasis added).

This provision is similar to Section 1201(a)(2) in that it uses very similar language to focus on prohibited tools. Unlike Section 1201(a)(2), however, it applies to technologies that protect the rights of a copyright owner in her copyrighted works rather than to technologies that control access to her copyrighted works.

B. UNAUTHORIZED ACCESS.

It is clear from both the language and legislative history of the DMCA that Congress sought to protect copyright owners from the *unauthorized* actions of others. However, the nature of the unauthorized actions prohibited under the DMCA are different and therefore required different means of control.

Sections 1201(a)(1) and 1201(a)(2) are expressly directed toward preventing unauthorized *access* of copyrighted works. Congress found that the "act of circumventing a technological protection measure put in place by a copyright owner to control access to a copyrighted work is the

electronic equivalent of breaking into a locked room in order to obtain a copy of a book." Burton Decl., Ex. N, H.R. Rep. No.105-551, Pt. 1, at 17 (1998).

Section 1201(a) achieves the goal of preventing unauthorized access in two distinct ways. First, Section 1201(a)(1) prohibits the act of circumventing protective technologies which control access to works. It is, by its terms, absolute. Any and all acts of that form of circumvention are prohibited. The issue of controlling access to copyrighted works in digital form was the subject of long and extremely vigorous discussion and debate in Congress because of its potential to cripple the doctrine of fair use, and give authors the ability to severely restrict or eliminate public access to copyrighted materials. Despite these significant concerns Congress however, chose to completely ban this form of circumvention subject only to limited and carefully crafted exemptions.[8] These exemptions were developed because Congress felt it "appropriate to modify the flat prohibition against the circumvention of effective technological measures that control access to copyrighted materials, in order to insure that access for lawful purposes is not unjustifiably diminished." Burton Decl., Ex. O, H.R. Rep. No. 105-551, pt. 2, at 36 (1998).

The second means by which unauthorized access to copyrighted works are protected is through a ban on the manufacture or trafficking in technologies, devices, etc. (hereinafter referred to as "tools") which could enable the unauthorized circumventions barred in Section 1201(a)(1).

Section 1201(a)(2) is a companion provision to Section 1201(a)(1) which is aimed at tools which could be used to facilitate an act of unlawful circumvention under Section 1201(a)(1). Congress intended that Section 1201(a)(2) prohibition against such tools to be a "meaningful protection and enforcement of the copyright owner's right to *control access* to his or her copyrighted work." Burton Decl., Ex. N, H.R. Rep. No. 105-551, Pt. 1, at 18. (emphasis added)

C. UNAUTHORIZED USE.

In stark contrast to the Sections 1201(a)(1) and (2), Section 1201(b) is not directed at unauthorized access, but at more traditional unlawful behavior. It prohibits tools which could be used to facilitate a different kind of circumvention. By its own terms it is concerned with

[8] Whether Congress' handling of these fair use concerns passes constitutional muster is the subject of a companion Motion to Dismiss based upon First Amendment objections.

circumventions of those technological measures that protect "*a right of a copyright owner*." The legislative history makes clear that Section 1201(b) does not concern itself with unauthorized access to copyrighted works, but rather the unauthorized *use* of copyrighted material once authorized access is obtained. Congress noted that the "subsequent actions of a person once he or she has obtained authorized access to a copy of a work protected under Title 17, even if such actions involve circumvention of additional forms of technological protection measures" are not covered under Section 1201(a). Burton Decl., Ex. N, H. Rep. No. 105-551, pt. 1, at 18; *see also* Burton Decl., Ex. P, S. Rep. No. 105-190, at 28 (1998).

If the circumvention addressed under 1201(a) is the electronic equivalent of breaking into a locked room in order to obtain a copy of a book, then the circumvention addressed under 1201(b) is the electronic equivalent of reproducing and distributing multiple copies of a book purchased from Barnes & Nobles. Once lawful access is obtained copyright holders lose control over the work in several respects. The fair use doctrine, for example, prevents copyright owners from barring or demanding a royalty for the use of a quotations in a critique of the work. *See* 17 U.S.C. § 107 (laying out the factors of fair use).[9] The right to fair use is deeply rooted in the law of copyright.[10] Congress recognized that once an individual has gained lawful *access* to a copyrighted work, there are authorized uses which can be made of a work, irrespective of the wishes of a copyright owner. Because of the significant differences between the range of activities permitted once lawful access is obtained, Congress used a different scheme to address unauthorized use.

---

[9] Likewise, the first sale doctrine prevents copyright owners from barring or demanding a royalty upon subsequent disposition of published copies. *See* 17 U.S.C. § 109 (exempting transfer of a particular copy from the copyright owner's exclusive rights).

[10] The Supreme Court has explained that fair use has constitutional underpinnings:

> From the infancy of copyright protection, some opportunity for fair use of copyrighted materials has been thought necessary to fulfill copyright's very purpose, 'to promote the Progress of Science and useful Arts . . . .' U.S. Const., Art. I, Sec. 8. For as Justice Story explained, 'in truth, in literature, in science and in art, there are and can be few, if any, things, which in the abstract sense, are strictly new and original throughout. Every book in literature, science and art, borrows and must necessarily borrow, and use much which was well known and used before.' Similarly, Lord Ellenborough expressed the inherent tension in the need simultaneously to protect copyrighted material and to allow others to build upon it when he wrote, 'while I shall think myself bound to secure every man in the enjoyment of his copy-right, one must not put manacles on science.' *Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569, 575 (1994) (citations omitted).

While Section 1201(b) is clearly aimed at unauthorized uses of lawfully obtained (accessed) materials, it only prohibits the tools which could be used to achieve such unauthorized uses. There is no underlying substantive prohibition. Unlike its close cousin, Section 1201(a)(2), Section 1201(b) does not have a complimentary provision prohibiting the act of circumventing usage control measures. Circumvention of usage restrictions is not prohibited under the DMCA. While the DMCA does not contain a general ban on the circumvention of usage control technologies, Section 1201(b) does ban the narrow range of tools which could allow circumvention of those usage control technologies which protect the rights of a copyright holder. That is, those technologies which a copyright holder may employ to prevent *unauthorized* use of his works. Such unauthorized uses constitute copyright infringement.

Congress' determination not to include a prohibition against the circumvention of usage control technologies was a deliberate decision made in recognition of the right to exercise fair use once copyrighted material had been lawfully obtained.

As the Copyright Office has noted, there is no prohibition of the act of circumvention of copy controls in recognition of the rights of an owner of a copyrighted work to enable fair use:

> The type of technological measure addressed in section 1201(b) includes copy-control measures and other measures that control uses of works that would infringe the exclusive rights of the copyright owner. . . . unlike section 1201(a), which prohibits both the conduct of circumvention and devices that circumvent, section 1201(b) does not prohibit the conduct of circumventing copy control measures. The prohibition in section 1201(b) extends only to devices that circumvent copy control measures. *The decision not to prohibit the conduct of circumventing copy controls was made, in part, because it would penalize some noninfringing conduct such as fair use.*

Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 65 Fed. Reg. 64,557 (2000) (codified at 37 C.F.R. § 201) (emphasis added).

The copyright office's conclusions are borne out by the legislative history:

> . . . *where access is authorized*, the traditional defenses to copyright infringement, including fair use, would be fully applicable. So, an individual would not be able to circumvent in order to gain unauthorized access to a work, but would be able to do so in order to make fair use of a work which he or she has lawfully acquired. Burton Decl., Ex. N, H.R. Rep. 105-551, pt. 1, at 18 (1998)(emphasis added).

Once lawful access to a protected work is obtained, circumvention for purposes of enabling fair use is not prohibited. Congress in fact anticipated that this would occur. Circumvention of copy

controls for purposes of fair use is legal and sanctioned conduct. By its refusal to prohibit the act of circumventing usage controls, Congress expressed its intent that society have the ability to continue to make non-infringing unauthorized uses of works. The wording in Section 1201(b), protecting "the rights of a copyright holder," reflects this intention.[11]

The tools prohibited by Section 1201(b) are those tools which could be used to accomplish the unlawful circumvention recognized by that section. That is, tools which can be used for purposes of copyright infringement

> [T]he reason there is no prohibition on conduct [under Section 1201(b)] akin to the prohibition on circumvention conduct in [Section 1201(a)(1)] is that the basic provision itself is necessary because prior to this act, the conduct of circumvention was never before made unlawful. The device limitation in [Section 1201(a)(2)] enforces this new prohibition on conduct. The copyright law has long forbidden copyright infringements so no new prohibition was necessary. *The device limitation in [Section 1201(b)] enforces the longstanding prohibitions on infringements.*

Burton Decl., Ex. P, S. Rep. No. 105-190, at 12 (1998) (emphasis added).

Thus, *only* those tools which are "primarily designed" to circumvent usage control technologies for the unlawful purpose of infringement are prohibited.

III. SECTION 1201(b) IS UNCONSTITUTIONALLY VAGUE AS APPLIED TO ELCOMSOFT

A. THE VAGUENESS STANDARD.

The due process clause of the Fifth Amendment to the United States Constitution requires that a statute clearly delineate the conduct which it intends to prohibit. A statute violates due process if its prohibitions are not clearly defined. *Grayned v. City of Rockford*, 408 U.S. 104, 108 (1972). "Vagueness may invalidate a criminal law for either of two independent reasons. First, it may fail to

---

[11] In December 1996, the World Intellectual Property Organization ("WIPO"), held a diplomatic conference in Geneva that led to the adoption of the WIPO Copyright Treaty. Article 11 of treaty provides in relevant part that contracting states "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*." WIPO Copyright Treaty, Apr. 12, 1997, Art. 11, S. Treaty Doc. No. 105-17 (1997), available at 1997 WL 447232 (emphasis added).

As such, the Treaty called for the establishment of remedies to protect against the circumvention of technology that protected copyrighted works. The Treaty also recognized by its plain terms, however, that under certain circumstances circumvention of the technology was "permitted by law."

provide the kind of notice that will enable ordinary people to understand what conduct it prohibits; second, it may authorize and even encourage arbitrary and discriminatory enforcement." *City of Chicago v. Morales*, 527 U.S. 41, 56 (1999).

"The degree of vagueness that the Constitution tolerates – as well as the relative importance of fair notice and fair enforcement -- depends in part on the nature of the enactment." *Village of Hoffman Estates v. The Flipside, Hoffman Estates, Inc.*, 455 U.S. 489, 498 (1982). A statute that imposes criminal penalties will be subject to more critical scrutiny than will other statutes challenged on vagueness grounds. See, e.g., *IDK, Inc. v. Clark County*, 836 F.2d 1185, 1198 (9th Cir. 1988); *Flipside*, *supra*, 455 U.S. at 498-499. Furthermore, just as "a scienter requirement may mitigate a law's vagueness, especially with respect to the adequacy of notice to the complainant that his conduct is proscribed," *Flipside, supra*, 455 U.S. at 499, where so-called "multi-purpose" devices are at issue (*e.g.*, drug paraphernalia, burglary tools), a law without a scienter requirement warrants a heightened scrutiny because an individual must be able to know when his or her conduct is unlawful.

The legislative history and the language of the DMCA establish that Congress did not prohibit the act of circumventing usage control technologies. For reasons directly related to that decision, it also did not ban *all* tools which might be used to circumvent usage control technologies. Congress sought to prohibit only those tools which are intended to be used to circumvent usage control technologies for the purpose of copyright infringement. Section 1201(b) does not provide a constitutionally adequate notice of this prohibition.

"It is established that a law fails to meet the requirements of the Due Process Clause if it is so vague and standardless that it leaves the public uncertain as to the conduct it prohibits. . . ." *City of Chicago v. Morales*, 527 U.S. at 56 (1999), *citing Giaccio v. Pennsylvania*, 382 U.S. 399, 402-403 (1966).

The general rule is that "[a] criminal statute is not vague if it provides adequate notice in terms that a reasonable person of ordinary intelligence would understand that [his] conduct is prohibited." *United States v. Martinez*, 49 F.3d 1398, 1403 (9th Cir.1995), cert. denied 516 U.S. 1065 (superseded by statute on other grounds). "The requirement involves an understanding by a putative actor about what conduct is prohibited. . . . Notice that does not provide a meaningful

understanding of what conduct is prohibited is vague and unenforceable." *Free Speech Coalition v. Reno*, 198 F.3d 1083, 1095 (9th Cir. 1999).

"The purpose of the fair notice requirement is to enable the ordinary citizen to conform his or her conduct to the law. 'No one may be required at peril of life, liberty or property to speculate as to the meaning of penal statutes.'" *City of Chicago v. Morales*, 527 U.S. at 58 (1999), *citing Lanzetta v. New Jersey*, 306 U.S. 451, 453, 59 S.Ct. 618, 83 L.Ed. 888 (1939).

B. SECTION 1201(b) FAILS TO SPECIFY AN UNLAWFUL PURPOSE.

Section 1201(b) does not directly prohibit the primary unlawful conduct, but is instead aimed at prohibiting other conduct intended to facilitate it. It parallels Section 1201(a)(2), which prohibits technologies used to facilitate the unlawful circumvention of access control technologies. In drafting Section 1201(b) Congress borrowed almost verbatim from the language of Section 1201(a)(2). Unfortunately, this has created difficulties because of the differences in the underlying conduct which is prohibited. Section 1201(a)(2) makes explicit reference to the unlawful purpose which the prohibited tools facilitate (*i.e.*, circumvention of access control technology). Because the circumvention of access controls is completely banned, *all* tools which are intended to facilitate this purpose are also completely banned. There is no ambiguity about which tools are banned under Section 1201(a)(2).

Section 1201(b) constitutional shortcomings arise from a simple but significant omission. It does not itself identify the unlawful conduct which would be facilitated by the tools it bans. Absent identification of the unlawful purpose which the tools facilitate, Section 1201(b) is doomed to inherent vagueness because not *all* tools are banned, and the language of the statute renders it impossible to determine which tools it in fact bans.

Unlike Section 1201(a)(2), under Section 1201(b) *all* circumventions of usage control technologies are *not* banned. Thus, unlike Section 1201(a)(2), the unlawful conduct which may be facilitated by the prohibited tools must be determined, not by explicit reference as in Section 1201(a)(2), but by inference from the phrase ". . . protects a right of a copyright owner under this title. . ." However, because of the nature of the relationship between copyright owner rights and fair use, reference to this phrase provides little help in determining what tools are prohibited by Section

1201(b). Any circumvention of a usage control technology for an authorized purpose must almost invariably involve circumvention of a technology which "protects a right of a copyright owner."

As set forth fully in the preceding sections of this brief, Congress intended to permit the circumvention of usage control technologies for the purpose of fair use once a copyrighted work had been lawfully obtained and accessed. Under copyright law, the rights of a copyright owner and the "right" of fair use are inexorably intertwined. Fair use is in fact a statutory limitation on the rights of a copyright owner. *See* 17 U.S.C. Section 107. Fair use does not exist in a vacuum but always coincides with complementary copyright owner rights. For this reason, circumvention of a usage control technology for the purpose of enabling fair use must almost by definition involve the circumvention of a technology which protects a right of a copyright owner. Yet, one such circumvention is prohibited (as are the tools to facilitate it) and the other is not. Reference to the statute's language does not enable an individual to determine which circumvention (and therefore which tool) is prohibited. This conundrum could only be resolved through inclusion of an explicit reference to the prohibited conduct.[12] That is, if Section 1201(b) were to specifically refer to the underlying unlawful conduct - - circumvention for an unlawful purpose.

The use of the phrase "primarily designed or produced for the purpose of circumventing protections. . ." in Section 1201(b)(1)(A) (one of the subsections directly at issue in this case) only compounds this intrinsic ambiguity. It is unclear if the "primarily designed" language is intended to only modify the phrase "for the purpose of circumventing protections afforded by a technological measure. . ." or whether this language also modifies the remainder of the phrase: "that effectively protects a right of a copyright owner. . ." In other words, must the prohibited tool be designed merely to circumvent any protective technological measure or must it be specifically designed to accomplish an unlawful circumvention? This is a distinction not without significant consequence. A tool designer, like Elcomsoft, who designs a tool for a lawful purpose - - circumventing a usage

///

---

[12] For example Section 1201(b)(1)(A) could simply have stated:
(A) is primarily designed or produced for the purpose of [*unlawfully*] circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title [17 U.S.C.A. Section 1, et seq.] in a work or a portion thereof;

control technology in order to enable fair use rights - - cannot determine the circumstances under which his conduct will violate the statute.

Under the first interpretation there is no scienter required to violate this section; the designer of *any* circumvention tool is guilty irrespective of whether the circumvention tool is designed for lawful or unlawful purposes. By definition, any circumvention tool is "primarily designed" to "circumvent[] . . . a technological measure."

Under the second interpretation of 1201(b)(1)(A), a tool designer will not violate the statute as long as the technological measure which the tool is designed to circumvent does not also protect a right of a copyright owner. However, this interpretation presents insurmountable difficulties in application because of the virtual impossibility of finding a situation in which the right of fair use is not also encompassed within the same technology which protects a "right of the copyright owner." If in making a tool which is primarily designed for the purpose of enabling the right of fair use the tool must necessarily circumvent a technological protection - - which is the fact in virtually every case - - then the designer will have violated Section 1201(b)(1)(A) despite a contrary intent.[13] Recognition of this fact is the reason that Congress specifically permitted acts of circumvention for the *purpose* of fair use.

Thus, application of this second interpretation produces a result identical to the first interpretation. That is, an ostensible ban on tools designed for a lawful purpose. While it is arguable that Congress could have banned all such tools, thus severely restricting or eliminating the fair use of digital media, they could have done so more directly and easily. More importantly, the legislative history as discussed *infra* in Part II of this brief makes clear that this is the exact opposite of what they intended to do.

---

[13] Elcomsoft is also charged with two counts of violation Section 1201(b)(1)(C), which provides that "[n]o person shall manufacture . . . in any . . . device . . . that . . . is marketed by that person . . . for use in circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof."

Like the problems presented with respect to the "primarily designed" language of Section 1201(b)(1)(A), this section does not specify whether the marketing of a device that is designed simply to accomplish circumvention is prohibited, or whether the device *also* must be marketed to infringe a copyright. Again, the government's view appears to be that the mere marketing of a device that circumvents a copy control is all that is required to violate Section 1201(b)(1)(C). There is no practical way of defining when one has marketed an authorized or unauthorized device.

C. SPECIFICATION OF AN UNLAWFUL PURPOSE IS ESSENTIAL.

These problems of vagueness and ambiguity arise because Section 1201(b) fails to refer to any unlawful purpose. When not all circumventions of usage control technologies are prohibited, the mere circumvention of a usage control technology without reference to the purpose for that circumvention cannot be a violation. However, without the appropriate language, ascertaining when a violation occurs is impossible. In order to eliminate this problem, statutes of this type have as an essential component of their structure, a scienter provision which connects the putative violator's actions and intent to a specified unlawful purpose..

The lack of such a scienter provision here is startling when contrasted with its presence in Section 1201(a)(2), and other similar statutes.

1. Drug Paraphernalia Statutes.

The cases discussing the need for a scienter provision in "drug paraphernalia" statutes are instructive here. In that context, the Supreme Court has recognized that "a scienter requirement may mitigate a law's vagueness, especially with respect to the adequacy of notice to the complainant that his conduct is proscribed." *Flipside*, *supra*, 455 U.S. at 499. Notwithstanding, Courts reviewing such statutes – which often concern products such as pipes that could be used for lawful and unlawful purposes – were wary of so-called "scienter" requirements that did not tie the requisite intent to unlawfulness:

> it is evident that . . . the "scienter" meant must be some other kind of scienter than that traditionally known to the common law – the knowing performance of an act with intent to bring about that thing, whatever it is, which the statute proscribes, knowledge of the fact that it is so proscribed being immaterial. . . . Such scienter would clarify nothing; *a clarificatory "scienter" must envisage not only a knowing what is done but a knowing that what is done is unlawful or, at least, so "wrong" that it is probably unlawful.*

Murphy v. Matheson, 742 F.2d 564, 573 (10th Cir. 1984) (emphasis added), *citing*, Note, *The Void-for-Vagueness Doctrine in the Supreme Court*, 109 U.Pa.L.Rev. 67, 87 n. 98 (1960) (cited in *Flipside*, 455 U.S. at 499 n. 14). As pointed out in *Levas & Levas v. Village of Antioch, Illinois*, 684 F.2d 446, 453 (7th Cir.1982), a scienter requirement is the only practical way to provide notice that a multi-purpose device is unlawful:

> Here the scienter requirement is not simply a circular reiteration of the offense – an intent to sell, offer for sale, display, furnish, supply or give away something that may

> be classifiable as drug paraphernalia. Rather the scienter requirement determines what is classifiable as drug paraphernalia: the violator must design the item for drug use, intend it for drug use, or actually employ it for drug use. Since very few of the items a paraphernalia ordinance seeks to reach are single-purpose items, *scienter is the only practical way of defining when a multi-purpose object becomes paraphernalia.* So long as a violation of the ordinance cannot be made out on the basis of someone other than the violator's knowledge, or on the basis of knowledge the violator ought to have had but did not, this sort of intent will suffice to distinguish "the paper clip which holds the pages of this memorandum of opinion from an identical clip which is used to hold a marijuana cigarette."

Id.

To this end, the government should not be heard to argue that Section 1201 is akin to the drug paraphernalia statute like the one scrutinized in *Flipside*, 455 U.S. 489 (1982). In *Flipside*, the Supreme Court reviewed a void-for-vagueness constitutional challenge to a local ordinance. "The ordinance [made] it unlawful for any person 'to sell any items, effect, paraphernalia, accessory or thing which is designed or marketed for use with illegal cannabis or drugs, as defined by Illinois Revised Statutes, without obtaining a license therefor.'" *Flipside*, 455 U.S. at 492. The *Flipside* Court concluded that "the standard [designed for use] encompasses at least an item that is principally used with illegal drugs by virtue of its objective features, *i.e.*, features designed by the manufacturer." *Id.* at 490. Based on this finding, the Court determined that it was "sufficiently clear that items which are principally used for nondrug purposes, such as ordinary pipes, are not 'designed for use' with illegal drugs." *Id*. at 501. The Court held that the ordinance was "reasonably clear in its application to the complainant." *Id.* at 505.

Section 1201 as applied in this case is unlike the statute in *Flipside*. Elcomsoft is being charged with a crime where its tool was designed for lawful purposes. Indeed, under the government's reading of Section 1201, *any* person who makes a circumvention tool will be subject to criminal prosecution because it is irrelevant whether a person intends to make a device for an authorized purpose. Accordingly, just as Elcomsoft is being prosecuted in this case for manufacturing the AEBPR program, under the government's view a person could be charged for manufacturing drug paraphernalia if that person made an ordinary pipe.

///

///

2. Burglary Tools Statutes.

The analogous state statutes prohibiting the possession or use of burglarer tools provide a basis for analogous comparison. Like Section 1201(b) "the purpose of all such statutes is to deter or prevent the commission a prohibited act by enabling law enforcement authorities to act before the prospective violator has had the opportunity to gather his tools, weapons, and plans and strike." *See Validity, Construction, and Application of Statutes Relating to Burglars' Tools*, 33 A.L.R. 3d 798, 805.

In achieving this purpose, however, virtually all of the statutes contain a scienter provision which ties the use or possession of burglarious tool to an unlawful purpose, burglary. The relevant California penal code provision provides:

> Every person having upon him or her in his or her possession a picklock, crow, keybit, crowbar, screwdriver, vice grip pliers, water-pump pliers, slide-hammer, slim jim, tension bar, lock pick gun, tubular lock pick, floor-safe door puller, master key, or other instrument or tool *with intent feloniously* to break or enter into any building, railroad car, aircraft, or vessel, trailer coach, or vehicle as defined in the Vehicle Code, or who shall knowingly make or alter, or shall attempt to make or alter, any key or other instrument above named so that the same will fit or open the lock of a building, railroad car, aircraft, or vessel, trailer coach, or vehicle as defined in the Vehicle Code, without being requested so to do by some person having the right to open the same. . .

California Penal Code, Section 466 (emphasis added).

It is the presence of similar language which allows these statutes to avoid being struck because of vagueness. In *State v. Palmer*, 2 Wash. App. 863, 471 P. 2d 118 (1970), the Supreme Court was called upon to consider whether the Washington state burglary statute was void for vagueness. That statute provided:

> Every person who shall make or mend or cause to be made or mended, or have in his possession in the day or nighttime any engine, machine, tool, false key, pick lock, bit, nippers or implement adapted, designed or commonly used for the permission of burglary, larceny, or other crime, under circumstances evincing an intent to use or employ or allow the same to be used or employed in the commission of a crime or knowing that the same is intended to be so used, shall be guilty of a gross misdemeanor.

R.C.W.A. 9.19.050.

The Washington Supreme Court found that:

> The conduct forbidden by the statute is the possession of tools or devices suitable for and commonly used in unlawful breaking and entering, *with intent to use those tools*

> *for that unlawful purpose*. As noted by the court and the *State v. McDonald*, 74 Wash. 2d 474, 445 p.345 (1968), 'we think even the most stupid member of the house breaking cult would understand that such undesirable conduct falls within the prohibition of this statute.' We agree and do not believe that the statute is void for vagueness.

Id. at 471 P.2d 120.

The exact opposite is the case under Section 1201(b). Here, even the most intelligent and honest software tool maker can not determine how to make a tool that would enable the lawful exercise fair use.

3. Other Federal Statutes.

A review of analogous federal statutes also revealed the presence of the requisite scienter component. 18 U.S.C. Section 2512 provides a relevant part:

> (1) except as otherwise specifically provided in this chapter, any person who intentionally -
> (b) manufactures, assembles, possesses, or sells any electronic, mechanical or other device knowing or having reason to know that the design of such device renders it primarily useful for the *purpose of the surreptitious interception* of wire, oral, or electronic communications, and that such device or any component thereof has been or will be sent through the mail or transported in interstate or foreign commerce. . .

Numerous cases construing the statute have determined that the use of the term "surreptitious" indicates that the prohibited devices be used in an illegal or unauthorized manner. *See e.g.*, *United States v. Lande*, 986 F.2d 907 (9th Cir. 1992); *United States v. Biro*, 143 F.3d 1421, 1428 (11th Cir. 1998). Finally, 47 U.S.C. Section 553 prohibits the manufacture or distribution of devices which can be used to receive cable telecommunications services.

> (1) no person shall intercept or receive or assist in intercepting or receiving any communications service offered over a cable system, unless *specifically authorized* to do so by a cable operator or as may be *specifically authorized* by law.
>
> (2) For the purpose of this section, the term "assist and intercepting or receiving" shall include the manufacture or distribution or equipment intended by the manufacturer or distributor (as the case may be) for *unauthorized reception* of any communication service offered over a cable system in violation of subparagraph (1).

Unlike the DMCA, this statute specifically connects the manufacturer's actions and intent with the relevant unlawful purpose.

///

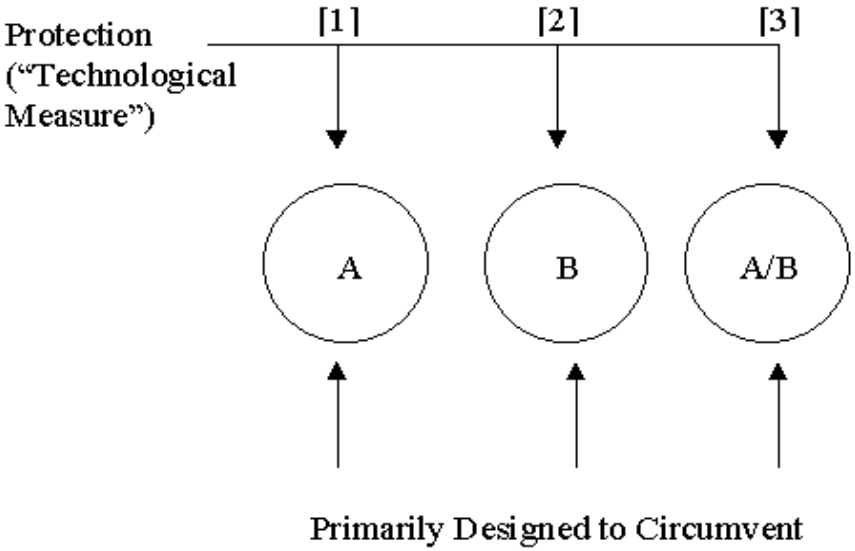
///

D. DETERMINING WHICH TOOLS ARE PROHIBITED IS IMPOSSIBLE.

In order to be enforceable, at the very least, a law must allow a person to conform his or her conduct to a "comprehensible standard." *Coates v. City of Cincinnati*, 402 U.S. 611, 614 (1971). Unfortunately, under 1201(b), there are *no* standards at all governing when a device is lawful or unlawful. No guidelines are provided regarding the manufacture and/or marketing of a device which allows authorized circumvention of copy controls. No objective criteria are provided for those seeking to create tools that will allow lawful owners of copyrighted material to exercise their rights to fair use. It cannot now be that Elcomsoft is guilty of a crime when it was acting in a manner contemplated – indeed encouraged – by Congress.

The following diagram is helpful in demonstrating the tremendous uncertainties Elcomsoft and other similarly situated companies face in determining if the actions they undertake are permissible under Section 1201(b).

A=Copyright Owner Rights
B=User Rights (Primarily "Fair Use")



In the first example [1] the usage control technology only encompasses a copyright owner rights and no fair use rights are involved (for the reasons discussed earlier, an impossible situation). Circumvention of the usage control technologies constitutes a violation of the statute under any interpretation of the "primarily designed" language. More importantly, because the usage control technologies *only* encompass copyright owner rights the circumvention of the protection can *only* be for an unlawful purpose.

In the second example [2] the usage control technologies only encompass fair use rights (no copyright owner rights are involved - - another impossible situation). Here the statute would still be violated under the first interpretation of the primarily designed language. That interpretation only requires that the tool be primarily designed to circumvent any protective technology, without regard to whether or not that technology protects a copyright owner's right, or what the tool maker's purpose may be. Though the purpose of the circumvention can here *only* be lawful (because no copyright owner rights are implicated), a tool maker could be liable.

In the third (real world) example, the usage control technology protects a bundle of rights, both copyright owner rights and user rights. If the tool maker's purpose in circumventing the protective technology is not considered then again *any* tool would violate the statute. In this example either interpretation of the primarily designed language would result in a violation (for the same reason as example No. 1). Most significantly, even if the tool maker's sole purpose in designing the tool were to enable fair use rights, he would still be in violation of the statute because those rights are within a usage control technology which "protects a right of a copyright owner."

The right to lawfully circumvent usage controls would be meaningless, of course, if tools that facilitate such lawful circumvention were not allowed. Indeed, for lawful owners of ebooks who lack the expertise to circumvent password encryption and other usage restrictions in the Adobe eBook Reader (like the users identified above), the AEBPR software is the only way to effectuate the uses to which the owner is legally entitled. Congress certainly contemplated tools like AEBPR.

It would seem, therefore, that Elcomsoft's product is not only lawful under the statute, but that the product deserves praise – for AEBPR is necessary to further the policies surrounding copyright law. Indeed, if the lawful owner of an ebook does not have the ability to exercise his or

her rights, then that owner has no rights at all, and the framework of Section 1201 would be eviscerated. For the reasons discussed earlier in this brief at length, it is clear that Congress did not intend to ban *all* circumvention tools and thereby render its express authorization of lawful circumvention a cruel joke. Despite Congress' clear intention, Section 1201(b) does not clearly define how the designer of a tool intended for a lawful purpose can achieve this purpose without violating its provisions.

E. APPLICATION OF SECTION 1201(b) TO ELCOMSOFT.

Whatever its status as a general matter, it is clear that Section 1201(b) is unconstitutionally vague as applied to this case. *See Posters 'N' Things, Ltd. v. United States*, 511 U.S. 513, 525, 114 S. Ct. 1747, 1754 (1994). No better case demonstrates the ambiguities inherent in Section 1201(b). Elcomsoft manufactured and marketed a tool that allows the lawful owner of an eBook to circumvent usage control technologies for the lawful purpose of permitting fair use of that eBook. Yet, Elcomsoft could not have known from reading the statute that its conduct in this regard would subject it to criminal consequences.[14]

In addition, the vagueness of Section 1201(b) permits precisely the sort of arbitrary enforcement that the void for vagueness doctrine is designed to guard against. Notwithstanding that Congress contemplated the kind of tool that Elcomsoft advertised and sold on the Internet, the government is using the imprecision of Section 1201(b)'s language to support a criminal case against a Russian defendant, on behalf of a "victim" which is a very powerful local software company. Adobe, a well-known company with a strong presence in the Silicon Valley, felt threatened by Elcomsoft's tool because it exposed weaknesses in the security features of its eBook products. Rather than fixing the flawed security of its eBook software, Adobe went to the federal authorities claiming that a Russian company was violating Section 1201. The federal authorities, with Adobe's assistance and reliance upon a vague, untested, but controversial statute, quickly arrested a visiting Elcomsoft employee. This conduct illustrates precisely the evils attending delegation of basic policy

///

---

[14] The lack of adequate warning inherent in Section 1201(b) is exacerbated in this case because Elcomsoft is a foreign corporation. It had no warning or reason to expect that Section 1201(b) would be applicable to its conduct. *See*, Burton Decl., Ex. C.

matters "for resolution on an *ad hoc* and subjective basis" by those who wield prosecutorial power. *Grayned v. City of Rockford*, 408 U.S. 104, 108-09 (1972).

"Under the rule of lenity, an ambiguous criminal statute is to be strictly construed against the government." *United States v. Bin Laden*, 92 F.Supp. 2d 189, 216 (S.D.N.Y. 2000); *People v. Materne*, 72 F.3d 103, 106 (9th Cir. 1995). Elcomsoft cannot be subjected to criminal prosecution because it would have to guess at the meaning of Section 1201(b) or because it may differ with the government as to the statute's application. *See*, *Connolly v. General Construction Company*, 269 U.S. 385, 391, 46 S.Ct. 126, 127 (1926). It is clear that under the well recognized principles of statutory construction, application of Section 1201(b) to Elcomsoft violates its due process rights.

IV. CONCLUSION

For all of the foregoing reasons, defendant Elcomsoft requests that the indictment be dismissed with prejudice in its entirety.

Dated: January ____, 2002

DUANE MORRIS LLP

By:_____
JOSEPH M. BURTON
Attorneys for Defendant
ELCOMSOFT COMPANY, LTD.

SF\28404.1

United States of America v. Elcom Ltd., a/k/a Elcomsoft Co., Ltd.
Case No.: CR 01-20138 RMW

PROOF OF SERVICE

I am a resident of the state of California, I am over the age of 18 years, and I am not a party to this lawsuit. My business address is Duane Morris LLP, 100 Spear Street, Suite 1500, San Francisco, California 94105. On the date listed below, I served the following document(s):

MOTION TO DISMISS INDICTMENT FOR VIOLATION OF DUE PROCESS

☐ by transmitting via facsimile the document(s) listed above to the fax number(s) set forth below on this date during normal business hours. Our facsimile machine reported the "send" as successful.

☐ by placing the document(s) listed above in a sealed envelope with postage thereon fully prepaid, in the United States mail at San Francisco, California, addressed as set forth below.

I am readily familiar with the firm's practice of collecting and processing correspondence for mailing. According to that practice, items are deposited with the United States mail on that same day with postage thereon fully prepaid. I am aware that, on motion of the party served, service is presumed invalid if postal cancellation date or postage meter date is more than one day after the date of deposit for mailing stated in the affidavit.

John Keker
Keker & Van Nest
710 Sansome Street
San Francisco, CA 94111

☐ by placing the document(s) listed above in a sealed envelope with postage thereon fully prepaid, deposited with Federal Express Corporation on the same date set out below in the ordinary course of business; to the person at the address set forth below, I caused to be served a true copy of the attached document(s).

Scott H. Frewing
Assistant United States Attorney
United States District Court
Northern District of California
280 South First Street
San Jose, CA 95113

☐ by causing personal delivery of the document(s) listed above to the person at the address set forth below.

☐ by personally delivering the document(s) listed above to the person at the address set forth below.

I declare under penalty of perjury under the laws of the State of California that the above is true and correct.

Dated: January ___, 2002

_____
Lea A. Chase

SF-28404

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

MISCELLANEOUS