MPAA Model state "super-DMCA" Bill (April 4, 2003 draft)

Bolded sections are those recently added by the MPAA in response to criticism of its earlier model bill, on which most of the pending state bills were based. Additions and deletions in red are commentary and modifications proposed by EFF.

Unlawful Communication and Access Devices

(a) Offense defined.--Any person commits an offense if he knowingly **and with the intent to defraud**[1] **a communication service provider:**

(1) possesses, uses, manufactures, develops, assembles, distributes, transfers, imports into this state, licenses, leases**,** sells or offers, promotes or advertises for sale**,** use or distribution any communication device:

(i) for the commission of a theft of a communication service or to ~~receive,~~ [2]intercept, ~~disrupt,~~[3] ~~transmit, re-transmits,~~ decrypt, acquire ~~or facilitate the receipt, interception, disruption, transmission, re-transmission,~~[4] ~~decryption or acquisition of~~ [5]any communication service in violation of otherwise applicable law[6] ~~without the express consent or express authorization of the communication service provider~~; or

---

[1] This "intent to defraud" language was added by MPAA lobbyists in response to mounting criticism. This revision, however, creates as many problems as it purports to solve. Generally, "intent to defraud" requirements are applied to deception-related offenses, such as check kiting. When bolted onto a provision aimed at banning mere possession of devices, the "intent to defraud" requirement makes the scope of the bill unclear. For example, what if a satellite TV provider decides to prohibit subscribers from using TiVo, and a subscriber fails to disconnect her TiVo? Has she acted with an "intent to defraud" by failing to heed the TiVo ban? What about a researcher who possesses "plans or instructions" that are otherwise banned under (a)(4)?

[2] Virtually anything you might connect to any wire that you pay for would be swept up by "receive". For example, every TV, VCR, TiVo or media PC is capable of "receiving" signals from cable television. This would regulate what people who legitimately pay for service are allowed to connect to the home entertainment centers in their own living rooms. For example, "receipt" would appear to reach a TiVo that you attach to your unencrypted basic tier cable service (did your cable company "expressly authorize" you to attach a TiVo?).

[3] "Disrupt" would appear to move into areas more properly within the jurisdiction of the Federal Communications Commission (FCC). For example, this would appear to reach your portable 2.4ghz phone if it interferes with the WiFi access point installed by a neighboring Starbucks (Starbucks would be a communication service provider). If you continued to use your phone after being told by Starbucks to stop, would you be acting with an "intent to defraud"?

[4] "Transmit" and "retransmit" would appear to reach any home networking equipment, which retransmits communications that arrive from the Internet. Under the language here, all home networking equipment that has not been "expressly authorized" by your ISP would potentially be suspect, subject to the vague "intent to defraud" provision.

[5] This appears to be redundant with (a)(5), which already makes it a unlawful to "assist others".

[6] The original language would effectively make it unlawful to connect anything to any wire in your house that you pay for, absent the "express consent or express authorization" of your service provider(s). This reverses the traditional rule, which has always been that you remain free to connect anything you like in your living room

(ii) to conceal or to assist another to conceal from any communication service provider, or from any lawful authority, the existence or place of origin or destination of any communication, **provided that such concealment is for the purpose of committing a violation of subparagraph (i) above;** or

(2) ~~modifies, alters, programs or reprograms a communication device for the purposes described in subparagraphs (a)(1)(i) and (ii) above~~[7]; or

(3) possesses, uses, manufactures, develops, assembles, distributes, imports into this state, licenses, transfers, leases, sells, offers, promotes or advertises for sale, use or distribution any unlawful access device or

(4) possesses, uses, prepares, distributes, sells, gives, transfers or offers, promotes or advertises for sale, use or distribution any:

~~(i) plans or instructions for making, or assembling or developing any communication or unlawful access device, under circumstances evidencing an intent to use or employ such communication or unlawful access device, or to allow the same to be used or employed, for a purpose prohibited by this section, or knowing or having reason to believe that the same is intended to be so used, or that the aforesaid plans or instructions are intended to be used for manufacturing or assembling such communication or unlawful access device for a purpose prohibited by this section; or~~[8]

(ii) material, including hardware, cables, tools, data, computer software or other information or equipment, knowing that the purchaser or a third person intends to use the material in the manufacture**,** assembly or development of a communication device for a purpose prohibited by this section, or for use in the manufacture, assembly or development of an unlawful access device; and

(5) Assist others in committing any of the acts prohibited by this section.

(b) Criminal Penalties.--

(1) Except for violations of this section as provided for in paragraph (2) or (3), an offense under this section is a misdemeanor.

(2) An offense under this section is a _____ felony if:

---

absent some legal obligation to the contrary. At a minimum, this should be modified to reach only activities that are otherwise forbidden by existing laws.

[7] This appears redundant with (a)(1). The "programming" or "modification" of a communications device would appear to be included by the "possesses … manufactures, develops" language in (a)(1).

[8] This language pushes the boundaries of the First Amendment by attacking the mere publication of "instructions and plans." Although there is "intent" language here that makes at least some effort to rescue the provision from its obvious constitutional difficulties, the MPAA has made no showing that curtailing the right to publish truthful information is necessary here.

(i) the defendant has been convicted previously under this section or convicted of any similar crime in this or any Federal or other state jurisdiction; or

~~(ii) the violation of this section involves at least 10, but not more than 50, communication or access devices.~~

(3) An offense under this section is a _____ felony if:

(i) the defendant has been convicted previously on two or more occasions for offenses under this section or for any similar crime in this or any Federal or other state jurisdiction; or

~~(ii) the violation of this section involves more than 50 communication or unlawful access devices.~~

(4) For purposes of grading an offense based upon a prior conviction under this section or for any similar crime pursuant to subparagraphs (b)(2)(i) and (b)(3)(i), a prior conviction shall consist of convictions upon separate indictments or criminal complaints for offenses under this section or any similar crime in this or any Federal or other state jurisdiction.

(5) As provided for in subparagraphs (b)(2)(i) and (b)(3)(i), in grading an offense under this section based upon a prior conviction, the term "any similar crime" shall include, but not be limited to, offenses involving theft of service or fraud, including violations of the Cable Communications Policy Act of 1984 (Public Law 98-549, 98 Stat. 2779).

~~(6) **Separate offenses.** For purposes of all criminal penalties or fines established for violations of this section, the prohibited activity established herein as it applies to each communication or unlawful access device shall be deemed a separate offense. Each day a person is in violation of this section also constitutes a separate offense.~~

~~(7) **Fines**. For purposes of imposing fines upon conviction of a defendant for an offense under this section, all fines shall be imposed as authorized by law for each day a person is in violation of this section and for each communication or unlawful access device involved in the violation.~~[9]

(8) **Restitution.** --The court shall, in addition to any other sentence authorized by law, sentence a person convicted of violating this section to make restitution as authorized by law.

(9) **Forfeiture of communication or unlawful access devices.--**Upon conviction of a defendant under this section, the court may, in addition to any other sentence authorized by law, direct that the defendant

[9] Where software is concerned, as well as instructions and plans, enhancements based on the number of devices or number of days they are possessed will function as an arbitrary enhancement against some defendants without any connection to the magnitude of underlying harm. Where software is concerned, the number of copies has no necessary relationship to the harm suffered by a service provider. For example, if a defendant had numerous copies of a piece of software on several computers in his house, even if the software was not intended for any further distribution, he would face enhanced criminal penalties. The number of devices simply has no necessary relationship to the harm involved, and thus should not be the basis for a penalty enhancement.

forfeit any communication or unlawful access devices in the defendant's possession or control which were involved in the violation for which the defendant was convicted.

(c) Venue.--An offense or violation under subsection (a) may be deemed to have been committed at either place where the defendant manufactures**,** develops or assembles an communication or unlawful access device or assists others in doing so**,** or the places where the communication or unlawful access device is sold or delivered to a purchaser or recipient. It shall be no defense to a violation of subsection (a) that some of the acts constituting the violation occurred outside of this [State or Commonwealth].

(d) Civil actions. --

(1) Any person aggrieved by a violation of this section may bring a civil action in any court of competent jurisdiction. "Any person aggrieved" shall include any communication service provider.

(2) The court may:

(i) award declaratory relief and other equitable remedies, including preliminary and final injunctions to prevent or restrain violations of this section, ~~without requiring proof that the plaintiff has suffered, or will suffer, actual damages, irreparable harm or lacks an adequate remedy at law~~[10];

(ii) at any time while an action is pending, order the impounding, on such terms as it deems reasonable, of any communication or unlawful access device that is in the custody or control of the violator and that the court has reasonable cause to believe was involved in the alleged violation of this section;

(iii) award damages as described in subsection (3) below;

(iv) in its discretion, award reasonable attorney fees and costs, including, but not limited to, costs for investigation, testing and expert witness fees, to an aggrieved party who prevails; and

(v) as part of a final judgment or decree finding a violation of this section, order the remedial modification or destruction of any communication or unlawful access device, or any other devices or equipment involved in the violation, that is in the custody ~~or control~~ [11]of the violator, or has been impounded under subparagraph (ii) above.

---

[10] There is no justification for these changes, which will entitle plaintiffs to preliminary injunctions as a matter of course. This outcome is particularly troubling where it reaches software and instructions, both of which have been recognized as expression protected by the First Amendment. Plaintiffs here should be required to play by the same rules that apply to everyone else—they should have to satisfy the traditional requirements for injunctive relief.

[11] This sets an extremely dangerous precedent, potentially authorizing a judge to force a software vendor to forcibly "downgrade" existing devices in the hands of legitimate customers by means of an "auto-update" or other remote control. The concept of "control" here is very slippery. Does TiVo "control" every device in the

(3) Types of damages recoverable**.** --Damages awarded by a court under this section shall be computed as either of the following:

(i) Upon his election of such damages at any time before final judgment is entered, the complaining party may recover the actual damages suffered by him as a result of the violation of this section and any profits of the violator that are attributable to the violation and are not taken into account in computing the actual damages. Actual damages include the retail value of any communication services illegally available to those persons to whom the violator directly or indirectly provided or distributed any communication or unlawful access devices. In proving actual damages, the complaining party shall be required to prove only that the violator manufactured, distributed or sold any communication or unlawful access devices, but shall not be required to prove that those devices were actually used in violation of this section. In determining the violator's profits, the complaining party shall be required to prove only the violator's gross revenue, and the violator shall be required to prove his deductible expenses and the elements of profit attributable to factors other than the violation**;** or

(ii) Upon election by the complaining party at any time before final judgment is entered, that party may recover in lieu of actual damages an award of statutory damages of between $1,50~~0~~ to $10,000~~ for each communication or unlawful access device involved in the action~~, with the amount of statutory damages to be determined by the court as the court considers just.

(4) In any case where the court finds that any of the violations of this section were committed willfully and for purposes of commercial advantage or private financial gain, the court in its discretion may increase the total award of any damages amended under subparagraphs (i) and (ii) above, by an amount of not more than $50,000~~ for each communication or unlawful access device involved in the action and for each day the defendant was in violation of this section~~[12].

(e) Definitions.—As used in this section, the following words and phrases shall have the following meanings:

(1) **"Manufacture, assembly or development of a communication device."** To make, produce**,** develop or assemble a communication device, or to knowingly assist others in those activities.

---

field just because they are able to automatically update the software remotely? Does Apple or Microsoft "control" every Internet-connected PC simply because they offer online upgrades to their customers?

[12] Statutory damages should not be automatically multiplied solely on the basis of the number of devices involved, as the number of devices is a poor proxy for the harm inflicted in any particular case. For example, if a security researcher were to publish a paper that included software held to be an "unlawful access device," and that paper were downloaded by only 100 academic colleagues, the court would be forced to impose damages of *at least* $1,500,000. Similarly, because the proposed statutes criminalize mere *possession* of an "unlawful access device," a researcher could face serious penalties simply for installing a tool on several computers in his own research lab.

Statutory damages should be a fall-back for plaintiffs who are unable to demonstrate any actual damages. An automatic multiplier, however, raises the specter that statutory damages will become the default election for plaintiffs interested in obtaining enormous awards that vastly exceed the actual harm that they suffer.

(2) **"Communication device."**

(i) Any type of electronic mechanism, transmission lines or connections and appurtenances thereto, instrument, device, machine**,** equipment, technology or software which is capable of intercepting, transmitting, re-transmitting, acquiring, decrypting or receiving any communication service; and

(ii) **A**ny component thereof, including any electronic serial number, mobile identification number, personal identification number, computer circuit, splitter, connectors, switches, transmission hardware, security module, smart card, software, computer chip, electronic mechanism or any component, accessory or part of any communication device which is capable of facilitating the interception, transmission, re-transmission, decryption, acquisition or reception of any communication service**;**

(3) **"Communication service."** Any service lawfully provided for a charge or compensation to facilitate the lawful origination, transmission, emission or reception of signs, signals, data, writings, images and sounds or intelligence of any nature by telephone, including cellular or other wireless telephones, wire, wireless, radio, electromagnetic, photoelectronic or photo-optical systems, networks or facilities; and any service lawfully provided **for a charge or compensation** by any radio, telephone, fiber optic, photo-optical, electromagnetic, photoelectric, cable television, satellite, microwave, data transmission, wireless or Internet-based distribution system, network or facility, including, but not limited to, any and all electronic, data, video, audio, Internet access, telephonic, microwave and radio communications, transmissions, signals and services, and any such communications, transmissions, signals and services lawfully provided directly or indirectly by or through any of the aforementioned systems, networks or facilities.

(4) **"Communication service provider."** (i) Any person or entity providing a communication service, whether directly or indirectly as a reseller, including, but not limited to, a cellular, paging or other wireless communications company or other person or entity which, for a fee, supplies the facility , cell site, mobile telephone switching office or other equipment or communication service; (ii) any person or entity owning or operating any fiber optic, photo-optical, electromagnetic, photoelectronic, cable television, satellite, Internet-based, telephone, wireless, microwave, data transmission or radio distribution system, network or facility; and (iii) any person or entity providing any communication service directly or indirectly by or through any such distribution systems, networks or facilities.

(**5**) **"Unlawful access device."** Any type of instrument, device, machine**,** equipment, technology or software that has no substantial use other than ~~which is primarily designed, developed, assembled, manufactured, sold, distributed, possessed, used or offered, promoted or advertised, for the purpose of~~[13]

[13] This change would restore the existing copyright law principles governing devices that can be used for infringement. The original MPAA language would replace the well-established legal standard announced by the U.S. Supreme Court in the 1984 *Betamax* case with a "primarily designed, … sold, ... or promoted" test. Notice that this definition, when combined with the (a)(3) prohibition, makes it unlawful for a defendant to possess a piece of software based on what third parties, over which he has no control, are doing. For example, imagine that a computer science graduate student wants to purchase Xbox mod chips in order to discover how they work. He could be in violation of (a)(3) because the chips are "primarily … sold" for circumvention. Moreover,

defeating or circumventing, in violation of otherwise applicable law,[14] an **effective** technology, device or software**,** or any component or part thereof**,** used by the provider, owner or licensee of any communication service or of any data, audio or video programs or transmissions, to protect any such communication, data, audio or video services, programs or transmissions from unauthorized receipt, acquisition, interception, access, decryption, disclosure, communication, transmission or re-transmission.

~~(6) **"Manufacture, assembly or development of an unlawful access device."** To make, develop, produce or assemble an unlawful access device or modify, alter, program or reprogram any instrument, device, machine, equipment, technology or software **for the purpose of** defeating or circumventing any effective technology, device or software used by the provider, owner or licensee of a communication service, or of any data, audio or video programs or transmissions, to protect any such communication, data, audio or video services, programs or transmissions from unauthorized receipt, interception, acquisition, access, decryption, disclosure, communication, transmission or re-transmission, or to knowingly assist others in those activities.~~[15]

~~**(7) "Multipurpose Device" means any communication device that is capable of more than one function, and includes any component thereof.**~~[16]

(f) Notwithstanding anything to the contrary in this section, the manufacture, production, assembly, design, sale, distribution, license or development of a ~~multipurpose~~ communication or unlawful access device shall not constitute a violation ~~of subsection (a)(3)~~ unless the ~~multipurpose~~ device is manufactured, developed, assembled, produced, designed, distributed, sold or licensed for the primary purpose of committing a violation of subsection (a)(~~3~~5);~~ or has only a limited commercially significant purpose or use other than as a unlawful access device; or is marketed by a person or another acting in concert with that person with that person's knowledge for use as an unlawful access device~~.[17]

---

the "intent to defraud" limitation may not rescue him, depending on whether his research in the face notice that mod chips are expressly forbidden by Microsoft constitutes an "intent to defraud".

[14] Without this modification, the provision appears to make it unlawful to make or possess a tool that is designed to circumvent, even where the circumvention might otherwise be permitted under the DMCA (e.g., under 17 U.S.C. 1201(f) or (g)). The MPAA has long argued that exceptions in the Copyright Act are merely defenses, and that the defenses can therefore be overridden by other laws. This change makes it clear that devices and conduct that is expressly permitted by the DMCA and other laws should not be banned here.

[15] This provision makes no sense at all within the structure of the bill. While this provision appears to be an effort to limit the bill's scope, it limits only three of thirteen prescribed verbs. "Manufacture, assemble, or develop" is only a subset of the activities banned by (a)(3), so this limitation does not reach the "possess, use,… distribute, import, licenses, leases, sells, offers, promotes or advertises for sale, use or distribution" provisions of (a)(3). The limitation, even as to the three verbs, is meaningless, as the remaining ten verbs reach just about anything that "manufacture, assemble, or develop" might reach.

[16] This additional definition is entirely superfluous. The bill regulates "communications devices" and "unlawful access devices." There is no need for an additional definition, except to save the MPAA from the embarrassment of permitting the manufacture and distribution of "unlawful access devices" in section (f).

[17] This provision was added by the MPAA as a "savings clause" intended to exempt makers of general purpose tools from liability. Unfortunately, while purporting to limit the reach of this measure, it actually makes things worse for technology companies.

(g) Nothing in this section shall require that the design of, or design and selection of parts, software code, and/or components for, a communication device provide for a response to any particular technology, device or software, or any component or part thereof, used by the provider, owner or licensee of any communication service or of any data, audio or video programs or transmissions, to protect any such communication, data, audio or video service, programs or transmissions from unauthorized receipt, acquisition, interception, access, decryption, disclosure, communication, transmission or re-transmission.[18]

First, as currently drafted, this limitation only reaches (a)(3) violations. The definition of "unlawful access devices" regulated under (a)(3), however, already limits the scope of the section to devices "primarily designed" for circumvention. By adding in the "limited commercially significant purpose" and "marketed for" language (borrowed from the DMCA), the amendment seems to *expand* the reach of the "unlawful access device" definition.

Second, this becomes totally incoherent when combined with the "intend to defraud" language. How is it possible to design a product for the "primary purpose" of "intending to defraud a communications service provider" by "distributing … an unlawful access device"? When you try to apply this "savings clause" by feeding it back through the language of (a)(3) and the definition of "unlawful access device", the whole effort collapses under its own weight amid a clutter of "intent" and "purpose" requirements.

This "savings clause" only makes sense in conjunction with (a)(5). It should rescue *any* multiple purpose device, so long as it was not purposefully designed to knowingly assist others under (a)(5), assuming that all of the (a) prohibitions are properly narrowed in scope. Even with these changes, it remains unclear how "intent to defraud" applies to a technology vendor's "primary purpose" in designing a device for third parties he has never met.

[18] This language represents an effort to include a "no mandate" provision similar to the one that was included in the DMCA (see 17 U.S.C. 1201(c)(3)). Unfortunately, even with this addition, the proposed bill fails to include any of the other hard-fought exceptions that Congress included in the DMCA. As noted above, this may well interfere with the balance struck by Congress when enacting the DMCA in 1998.