SDMCA Laws: Preemption and Constitutional Issues

By Kevin McReynolds*

TABLE OF CONTENTS

I. INTRODUCTION

Since 2001, the Motion Picture Association of America ("MPAA") has been lobbying state governments to enact new legislation to update existing telecommunications and cable security laws. This new legislation is designed to prevent theft of telephone and cable service.[1] The MPAA drafted model legislation that has been enacted in seven states and is pending in several more.[2] The stated purpose of the model legis-

* J.D. Candidate, UCLA School of Law, 2005. I would like to thank Professors David Nimmer, Eugene Volokh, and Neil Netanel, Judge George Schiavelli, and my wife Anjuli.

[1] William Sloan Coats & Timothy B. Choe, *Super-DMCA: Has It Landed in Your State?*, 754 PRACTICING L. INST.: PAT., COPYRIGHTS, TRADEMARKS, AND LITERARY PROP. CTS. HANDBOOK SERIES, 367, 369 (2003).

[2] Jeffrey P. Cunard & Jennifer B. Coplan, *Cyberliability 2003: Selected Developments*, 769 PRACTICING L. INST.: PAT., COPYRIGHTS, TRADEMARKS, AND LITERARY PROP. CTS. HANDBOOK SERIES, 481, 500-1 (2003) (Pennsylvania in 2000, Delaware and Maryland in 2001, Illinois, Michigan and Virginia in 2002, Arkansas and Florida in 2003); ELECTRONIC FRONTIER FOUNDATION, STATE-LEVEL "SUPER-DMCA" INITIATIVES ARCHIVE, *at* http://

lation is meant to update traditional cable and telephone theft laws to include a broader range of telecommunications services, including Internet-based systems, and outlaw a more extensive array of circumvention devices.[3] However, these laws have become a source of debate as critics have attempted to stop their passage. Critics have dubbed these laws "Super" Digital Millennium Copyright Act laws ("SDMCA") because they functionally expand the powers of telecommunications service providers and entertainment companies along the same lines as the federal Digital Millennium Copyright Act.[4]

Part II of this article will briefly review the two sides of the debate about SDMCA laws. Part III will analyze the express language of the Delaware SDMCA law and consider the plain meaning of the statute as enacted.[5] In Part IV this article will again look to the Delaware version

---

www.eff.org/IP/DMCA/states/ (last visited October 1, 2004) [hereinafter EFF STATES] (giving same information, though it marks Michigan as 'date unknown'). *See also* PUBLIC KNOWLEDGE, 2004 STATUS OF SDMCA BY STATE, *at* http://www.publicknowledge.org/content/policy-papers/SDMCA-status-table (last visited October 1, 2004) (listing six of the seven same states as having SDMCA legislation on the books. Does not list Pennslyvania. Also lists pending legislation more recent than the EFF STATES list).

[3] Coats & Choe, *supra* note 1, at 369. Note, the MPAA calls the Model version the "Draft Model Communications Security Legislation." *See* DRAFT MODEL COMMUNICATIONS SECURITY LEGISLATION (Geoffrey L. Beauchamp), *at* http://www.eff.org/IP/DMCA/states/mpaa_3apr.pdf (last visited October 1, 2004) [hereinafter MPAA REVISED MODEL ACT]. Although the MPAA's name does not appear on the cover sheet, this is their Model Act.

[4] *See* George V. Hulme, *Proposed Telecom Laws Draw Fire*, INFORMATION WEEK, Apr. 7, 2003, *available at*: http://www.informationweek.com/story/showArticle.jhtml?articleID=8700378 (last visited October 1, 2004).

[5] Note that this article will focus exclusively on the substantive characteristics of the Delaware SDMCA law and will thus not be discussing the procedural aspects of the law. However, it is worth noting that the Delaware version of the law incorporates many of the procedural aspects of the MPAA Model Act, which the Electronic Frontier Foundation believes to be arbitrary and oppressive.

For example the Electronic Frontier Foundation believes that Section (b)(9) of the MPAA's Model Act is an arbitrary enhancement where software or plans are concerned. ELECTRONIC FRONTIER FOUNDATION, EFF LINE-BY-LINE ANALYSIS OF THE MPAA MODEL BILL, *at* http://www.eff.org/IP/DMCA/states/20030408_eff_redline_of_mpaa_model.php (last visited October 1, 2004) [hereinafter EFF LINE-BY-LINE]. Section (b)(9) states, "[f]ines: 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." *Id.* This increases the penalty without any connection to the magnitude of the underlying harm. *Id.* The Delaware law includes this section virtually verbatim, and thus raises the same concerns. *See* DEL.CODE.ANN. tit. 11, §850(b)(7) (2001).

However, not all of the procedural problems with the Model Act seem to have been taken directly into the Delaware law. The Model Act specifically allows for preliminary injunctions without any of the normal requirements like proof of damages, irreparable harm or a lack of adequate remedies at law. *See* EFF LINE-BY-LINE, *supra*. The Delaware version does not include this express language authorizing injunctions without any of these standard showings. *See* DEL.CODE.ANN. tit. 11, §850(d)(2)(a) (2001).

of the law to suggest how federal preemption may apply to state SDMCA laws. In Part V the author will suggest other potential constitutional problems SDMCA laws may face. Finally, Part VI concludes that not only do the critics have the better argument, but also that SDMCA laws, like Delaware's, may violate the federal constitution for several reasons.

II. SDMCA Laws: Origins, Critics and Proponents

As noted before, these state "Super" DMCA laws have been hotly debated since the first few laws were introduced in 2000. The laws' proponents argue that these measures are necessary in the Internet era to protect against the theft of cable and movie privileges since digital technology increases the potential harm of these thefts to service providers and copyright owners.[6] Critics, however, contend the laws are too restrictive and thus jeopardize privacy, threaten innovation, and provide unprecedented control over how media content is used to communication service providers in homes and the technology marketplace.[7]

The laws' chief proponent is, of course the, MPAA, which created the first versions of the laws and began lobbying state legislatures to enact them. The MPAA says these laws are necessary to accomplish four objectives:

> [(1) To p]rovide comprehensive protection for all broadband and Internet based communication services from unauthorized access, receipt, transmission, decryption and disruption, thereby addressing not only outright theft, but also intentional disruption or sabotage of communication services; [(2) To p]rotect e-commerce networks against intentional disruption or unauthorized access, thereby making them more legally secure for businesses and consumers; [(3) To p]rohibit 'unlawful access devices' so that the laws better protect consumer interface devices such as 'smart cards' from circumvention by pirate technologies; and [(4) To d]efine 'unlawful access devices' so that technological protection measures used to protect programming content are legally protected from circumvention.[8]

The MPAA suggests these objectives can be accomplished simply by upgrading the existing state telecommunication theft laws.[9]

The MPAA denounces critics' characterizations of the new laws as an expansion of federal DMCA powers.[10] The MPAA's senior vice

---

[6] Coats & Choe, *supra* note 1, at 370.

[7] *Id.*

[8] Press Release, Motion Picture Association of America, Key Features of the Model Communications Security legislation, 1 *available at* http://www.eff.org/IP/DMCA/states/mpaa2_1apr.pdf (last visited October 1, 2004) [hereinafter MPAA Self-Justification].

[9] *See* Hulme, *supra* note 4.

[10] *Id.*

president of state legislative affairs, Vans Stevenson, addressed this issue directly saying "[t]hese are amendments to existing communications and cable theft laws . . . [and] have nothing to do with the DMCA."[11]

Opponents of SDMCA laws, including the Electronic Frontier Foundation ("EFF"),[12] the Consumer Electronics Association,[13] and Public Knowledge,[14] attack the MPAA's Model Act, claiming that it would ban the possession, development, or distribution of a broad array of 'communications' and 'unlawful access' devices, as well as ban devices that enable anonymous communication.[15] These effects, if not intended, are the direct result of what critics consider "absurdly broad" language.[16] A 'communications device' is virtually any electronic device you might connect to any communications service.[17] This would dramatically expand the power of entertainment companies, ISPs, cable companies and others to control what you can and cannot connect to the services you pay for.[18]

Prominent legal scholars have joined in the fight against this legislation. John Palfrey, the Executive Director of the Berkman Center for Internet and Society at Harvard Law School, testified before the Massachusetts Joint Committee on Criminal Justice in April of 2003 in opposition to the SDMCA law that was being considered there.[19] The Massachusetts version under consideration was virtually identical to the

---

[11] Coats & Choe, *supra* note 1, at 370.

[12] A digital rights advocacy group based in San Francisco. *See id.*

[13] A trade association whose mission is to promote growth in the consumer technology industry. They represent more than a thousand corporate members in the consumer technology industry. *See* Press Release, Consumer Electronics Association, CEA Remains Opposed to Overly Broad, Ambiguous "Theft of Service" Bills, *available at* http://www.ce.org/press_room/press_release_detail.asp?id=10205 (last visited October 1, 2004) [hereinafter CEA Opposed].

[14] A public-interest advocacy group based in Washington, D.C. Coats & Choe, *supra* note 1, at 370.

[15] FRED VON LOHMANN, STATE LEGISLATION: MPAA'S STEALTH ATTACK ON YOUR LIVING ROOM, *at* http://www.eff.org/IP/DMCA/states/200304_sdmca_eff_analysis.php (last visited May 6, 2004) [hereinafter EFF STEALTH]. *See also* MIKE GODWIN, A BRIEF ANALYSIS OF THE SUPER DMCA (THE DRAFT MODEL COMMUNICATIONS SECURITY ACT), *at* http://www.publicknowledge.org/content/policy-papers/pp-analysis-super-dmca/ (last visited October 1, 2004); CEA Opposed, *supra* note 13. These same effects could be found in enacted SDMCA laws that closley mirror the Model Act's language.

[16] EFF STEALTH, *supra* note 15.

[17] *Id.*

[18] *Id.*

[19] *Internet Security: Hearing on H.B. 2743 Before the Comm. of Great and General Court*, 2003 (Mass. 2003) [hereinafter *Hearing*] (Testimony of Prof. John Palfey), *available at* http://blogs.law.harvard.edu/palfrey/stories/storyReader$86 (last visited October 1, 2004). *See also* Hulme, *supra* note 4.

original MPAA Model Act.[20] Professor Palfrey called the proposed legislation "a bad idea . . . [u]necessary to achieve its stated purposes."[21] He noted that, as a result of a series of unintended consequences, the SDMCA law would cause results contrary to its stated goals.[22] He argued the bill would actually be bad for computer security and terrible for software development[23] for several reasons: (1) to the extent the goal of the law is simply to keep people from stealing or hacking a computer system, there are already laws that achieve this end;[24] (2) the Internet law of the United States is already too complex, and this legislation would only make things worse;[25] and (3) the law will go much further than banning hacking and stealing—it will stifle research, chill speech, and criminalize legitimate scholarship.[26] Finally the Professor noted the improper motives actually behind this bill: "This bill is part of a concerted national special interest campaign . . . that would undercut [American] freedoms for one reason only: greed . . . [and] not even the good kind of greed, that will help lots of people by creating lots of jobs . . . [this legislation] is not going to help the

---

[20] DAVID "NOVALIS" TURNER, THE STATE SUPER-DMCA FIGHT, *at* http://www.gnu.org/bulletins/bulletin-002.html (last visited October 1, 2004). Thus it was lacking the "intent to defraud" language discussed *infra* at note 32.

[21] *Hearing, supra* note 19.

[22] *Id.*

[23] *Id.* The American Library Association had similar thoughts:

> [T]his copyright protection legislation largely duplicates the intention and the protective mechanisms inherent in the Digital Millennium Copyright Act (DMCA) passed by Congress in 1998 with the stated purpose of preventing digital piracy. However, unlike the DMCA that builds in certain exception and limitations to permit legitimate activities, the state versions do not. Furthermore, the sweeping language of the proposed legislation would inadvertently outlaw the use of security technologies such as encrypted e-mail and firewalls. The legislation would increase the vulnerability of communications and the Internet at a time when cybersecurity is a national priority.

AMERICAN LIBRARY ASSOCIATION, COPYRIGHT-RELATED STATE LEGISLATION, *at* http://www.ala.org/ala/washoff/WOissues/copyrightb/stateleg/slmain.htm#sdmca (last visited October 1, 2004).

[24] *Hearing, supra* note 19. Professor Palfey testified:

> We already have an alphabet soup of laws that achieve this end. Starting with the state's criminal statutes and common law; our law enforcement agencies that do good work in this front have many tools at their disposal. Consider, for instance, just the [DMCA], the Computer Fraud and Abuse Act, the Patriot Act, and other prohibitions against theft, copyright violation, fraud, and trespass to chattels. If all you want to do is criminalize hacking or stealing, then we need to be honest: these acts are already crimes here and elsewhere . . . ;[Further] it's worth noting that the state Attorney General's office is not here testifying that it needs this law.

Id.

[25] *Id.* Indeed, Professor Palfrey candidly admitted "I study this topic for a living, and I don't pretend to understand my rights and responsibilities in this area; it's already too complex . . . [and this SDMCA] law will make a bad situation worse." *Id.*

[26] *Id.*

economy . . . it will just make a few rich people richer."[27] The MPAA's representative was unable to counter these arguments and the Massachusetts bill was defeated.[28]

The MPAA contends that critics are reading the language of the laws far too broadly.[29] Responding to criticism by the Consumer Electronics Association,[30] Vans Stevenson circulated a letter in calling the group's reading of the model law "patently false" and a "disservice to honest consumers" who will be mislead into believing these laws are a bad idea.[31] Mr. Stevenson explained that these laws only apply "if an individual steals a service offered for a fee . . . [and thus, to] an honest consumer, this legislation will pave the way for future generations of digital services [rather than do them any harm]."[32] Mr. Stevenson attacked the CEA for "resorting to scare tactics" and "misinformation after failing to object to this legislation when it [was] enacted in six states over the past three years."[33] Critics charge this last attack is far off the mark, and accuse the MPAA of pushing the legislation through smaller states first to avoid a fight like the one in Massachusetts.[34]

In order to better understand which interpretation of SDMCA laws is more accurate, Part III will now analyze the Delaware law that was enacted in 2001.

---

[27] *Id.*

[28] In May 2003 a nearly identical version of the bill was defeated in Texas after advocacy groups and legal scholars testified at a public hearing. *See* EFF STATES, *supra* note 2. *See also* Letter from George E. Nix, Professor of Law, University of Texas, to Senate Criminal Justice Committee, Texas Legislature (Apr. 29, 2003) *available at* http://www.eff.org/IP/DMCA/states/dix_letter_intent_defraud.pdf (last visited October 1, 2004) (suggesting the then pending Texas SDMCA law was a bad idea).

[29] Press Release, Motion Picture Association of America, Statement by Vans Stevenson (Apr. 29, 2003) *available at* http://www.eff.org/IP/DMCA/states/MPAA-statement-4-29-03.pdf (last visited October 1, 2004)[hereinafter MPAA response to CEA]. Note this letter went out April 29, 2003 shortly after the Massachusetts public hearing that defeated the SDMCA law there, but after the MPAA revised the Model law to include the "intent to defraud language." *See infra* note 32.

[30] *Id.*

[31] *Id.*

[32] *Id. See* Hulme, *supra* note 4. Note the MPAA altered the language of the Model law to include "intent to defraud" hoping to appease the critics. *See* MPAA REVISED MODEL ACT, *supra* note 3. *But see* EFF LINE-BY-LINE, *supra* note 5 (suggesting the "intent to defraud" language creates as many problems as it solves since the scope of the bill is still unclear).

[33] MPAA response to CEA. It is worth noting that these organizations did fight and successfully defeat or get the language dramatically changed in new SDMCA legislation once they noticed what the MPAA was enacting.

[34] Declan McCullagh, *DMCA Critics Decry State-level Proposal*, NEWS.COM, Mar. 28, 2003, *available at*: http://news.com.com/2100-1028-994667.html?tag=CD_mh (last visited October 3, 2004) (quoting David McClure, the president of the U.S. Internet Industry Association, "[The MPAA was enacting SDMCA laws] in four states before we even saw them doing this").

III. Analysis of the Delaware SDMCA Law

The Delaware SDMCA law was one of the first passed in the United States. It's passage predates the critics' efforts to lobby against this type of legislation.[35] The language of the Delaware law is not significantly different than that of the original Model Act the MPAA was advocating to state governments at the time.[36] Thus the Delaware law is an appropriate model to help understand the potential effects of the SDMCA laws.

An analysis of the language of the four main substantive subsections of the Delaware SDMCA law illustrates the potential breadth of the law and suggests that the critics have the stronger side of the SDMCA debate discussed in Part II.

The differences between the Delaware law and MPAA's Model Act will be mentioned throughout the analysis below. Generally these differences show the Delaware law to be narrower and thus more reasonable than the Model Act, though still overly broad. The fact that the Delaware law, which was enacted, is overbroad and intrusive suggests that the Model Act is that much more problematic.

The four substantive subsections of the Delaware law considered here are subsections (a)(1)(a), (a)(1)(b), (a)(2), and (a)(3)(a). Subsection (a)(1)(a) generally prohibits the use of telecommunication devices to disrupt, receive, or transmit any telecommunication service without the express consent of the telecommunication provider.[37] Subsection (a)(1)(b) outlaws the concealment of the origin or destination of a telecommunication under circumstances suggesting an intent to commit any offense.[38] Subsection (a)(2) prohibits the manufacture, development, and distribution of 'unlawful access devices.'[39] Finally subsection (a)(3)(a) forbids the preparation or distribution of plans or instructions for the manufacture of an unlawful telecommunications device or unlawful access device.[40]

---

[35] There is nothing in the Delaware legislature's records to indicate that any opposition group argued against that law. *See* State of Delaware, History of H.B. 163, 141st General assembly (Del. 2001) *available at* http://www.legis.state.de.us/lis/lis141.nsf/vwLegislation/HB+163?Opendocument (last visited October 3, 2004). The legislature's page gives links to committee reports, votes, and text of final bill.

[36] The specific parts of the law that differ from the MPAA Model Act will be noted in the section-by-section analysis below. There is also one difference of terminology that appears meaningless that should be mentioned: the Delaware law uses the prefix 'tele-' wherever the MPAA Model Act or MPAA Revised Model Act uses some form of "communication".

[37] This is a brief summary. The complete text is provided in notes 41, 47.

[38] This is a brief summary. The complete text is provided in notes 41, 58.

[39] This is a brief summary. The complete text of this section and the definition of 'unlawful access device' are provided in notes 72, 74.

[40] This is a brief summary. The complete text is provided in note 81.

After analyzing the language of these four subsections the Delaware law is briefly compared with the far narrower Florida SDMCA law. This part of the discussion illustrates that the different focus of the Florida law substantially avoids many of the problems caused by the broad language of the Delaware SDMCA law.

The first two subsections considered here, subsections (a)(1)(a) and (a)(1)(b), both use the same preamble language in defining a violation.[41] This preamble language differs somewhat from that of the MPAA's Model Act in a way that may narrow the scope of the law and thus ameliorates some of the critics' concerns. The Delaware code removes "possesses," "uses" and "develops" from the list of prohibited acts.[42] Perhaps more significantly, the Delaware code adds the term "unlawful" in the first part of this preamble and then defines the term in a way that appears far narrower than the Model Act.[43] However,

---

[41] DEL.CODE.ANN. tit. 11, §850(a)(1)(2001) ("A person is guilty of a violation of this section if the person knowingly: Manufactures, assembles, distributes, possesses with intent to distribute, transfers, sells, promotes or advertises for sale, use or distribution any unlawful telecommunication device or modifies, alters, programs or reprograms a telecommunication device:")

[42] *Id.* Dropping "possesses" and "uses" makes the list of prohibited acts in the preamble less applicable to consumers whose very possession and use of a prohibited device was swept into the MPAA's Model Act language. The Delaware law also adds "possesses with intent to distribute", which prohibits possession of devices, but not likely in the consumer setting. *See* DRAFT MODEL COMMUNICATIONS SECURITY LEGISLATION, (a)(1)(i) (Motion Picture Association of America) *at* http://www.freedom-to-tinker.com/doc/2003/mpaa1_1apr.pdf (last visited October 3, 2004) [hereinafter MPAA MODEL ACT]. The effect of omitting "develops" is much harder to understand. This could narrow the law to not prohibit research into telecommunication technology, but any such effect may be eliminated by the prohibitions in DEL.CODE.ANN. tit. 11, §850(a)(3)(a)(2001).

[43] DEL.CODE.ANN. tit. 11, §850(e)(5)(2001) defines 'Unlawful telecommunication device' as:

> Any electronic serial number . . . or any telecommunication device that is capable of acquiring or facilitating the acquisition of a telecommunication service without the express consent or authorization of the telecommunication service provider, or has been altered, modified, programmed or reprogrammed alone or in conjunction with another telecommunication device or other equipment to so acquire . . . the unauthorized acquisition of a telecommunication service. 'Unlawful telecommunications device' also means:"
>
> (a) "Phones altered to obtain service without express consent . . . of the telecommunication service provider . . . counterfeit or clone phones . . . or other instruments capable of disguising their identity or location or of gaining unauthorized access to a telecommunication system . . . ;and
>
> (b) "Any telecommunication device which is capable of, or has been altered, designed, modified, programmed or reprogrammed, alone or in conjunction with other . . . devices, so as to be capable of facilitating the disruption, acquisition, receipt, transmission or decryption of a telecommunication service without the express consent of the telecommunication service provider, including ,but not limited to, any device, technology . . . service . . . or part thereof, primarily distributed . . . programmed, reprogrammed or used for the purpose of providing the unauthorized receipt of, transmission of, disruption of . . . or acquisition

while the definition of "unlawful telecommunications device" is narrower than that of "communications device" in the Model Act, the Delaware law remains extremely broad.[44] Further, the addition of the "or modifies, alters, programs or reprograms a telecommunications device"[45] may effectively remove these narrowing features of the Delaware preamble since this removes the "unlawful" limit and can essentially punish consumers for "use" of a device when "programming" is necessary to use the device.[46] It is difficult to understand how the law would apply from the preamble alone so the first and second substantive parts of the Delaware law will be discussed separately.

The language of Delaware subsection (a)(1)(a), like the preamble subsection, is extremely close to that of the MPAA Model Act.[47] Again like the preamble subsection, the Delaware code does seem to be a bit

---

of any telecommunication service provided by any telecommunication service provider."

Cf. MPAA MODEL ACT, *supra* note 42, subsection (e)(2):

'Communication device'.

(i) Any type of electronic mechanism, transmission lines or connection 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) Any component thereof, including any electronic serial number . . . or part of any communication device which is capable of facilitating the interception, transmission, retransmission, decryption, acquisition or reception of any telecommunication service

[44] DEL.CODE.ANN. tit. 11, §850(e)(5)(2001) has the same problem with a separate clause for "program" as the preamble subsection(a)(1) itself has. The clause can effectively swallow the other language thus redefining 'Unlawful telecommunication device' as any device that has been programmed to receive a telecommunication service without authorization. Or in the case of subsection (e)(5)(b) any device that is capable of disrupting or receiving a telecommunication service without authorization. The (e)(5)(b) definition would effectively ban almost any device since virtually all wireless devices are 'capable' of disrupting wireless services, even unintentionally. For example, a person's cordless phone could disrupt his neighbor's home WiFi network and even if it did not actually disrupt, it would certainly be capable of it. The "disrupt" language in SDMCA laws may also encroach on the authority of the FCC. *See infra* discussion Part IV.

[45] DEL.CODE.ANN. tit. 11, §850(a)(1)(2001). This language actually does appear in the MPAA MODEL ACT, supra note 42, as separate subsection section (a)(2).

[46] DEL.CODE.ANN. tit. 11, §850(a)(1)(2001). However, this may be overstating the case since the cannon for statutory interpretation *Noscitur a sociis* could make 'program' require an affirmative act to change how a device would normally function as 'alter' and 'modify' suggest.

[47] DEL.CODE.ANN. tit. 11, §850(a)(1)(a)(2001) ("For the unauthorized acquisition or theft of any telecommunication service or to receive, disrupt, transmit, decrypt, acquire or facilitate the receipt, disruption, transmission, decryption or acquisition of any telecommunication service without the express consent or express authorization of the telecommunication service provider;"). The differences between this subsection and MPAA Model Act subsection (a)(1)(i) are discussed in note 48.

narrower than the Model Act.[48] However, just like the preamble, subsection (a)(1)(a) has a separating clause in "or to receive" which effectively broadens the reach of the Delaware law well beyond "unauthorized acquisition or theft of any telecommunication service."[49] When looking at a version of the Model Act, the EFF criticized this language as sweeping up virtually anything you might connect to any wire that you pay for.[50] Regardless of the reading of "receive," the "transmit" language may effectively outlaw all home networking equipment which re-transmits communications that arrive from the Internet.[51] The EFF was also concerned with the "disrupt" language since it moves into areas more properly within the jurisdiction of the FCC.[52] Finally, potentially the most troubling language in this statute is "without the express consent or express authorization of the telecommunication service provider"[53] which would potentially make it criminally prohibited to connect anything to any wire in one's home absent the 'express consent' of one's service provider.[54] This reverses the traditional rule, which has allowed people to be free to connect anything to any service, absent some legal obligation to the contrary.[55] As the EFF's Fred von Lohmann put it "[a]ll things not expressly permit-

---

[48] *Compare id with* MPAA MODEL ACT, *supra* note 42, subsection (a)(1)(i). The Delaware law adds "unauthorized acquisition" but omits "intercept" which effectively covers the same area. The Delaware law also omits "re-transmits", but is otherwise identical to the Model Act.

[49] DEL.CODE.ANN. tit. 11, §850(a)(1)(a)(2001).

[50] EFF LINE-BY-LINE, *supra* note 5. The EFF gives a few examples: Every TV, VCR, TiVo or media PC is capable of 'receiving' signals from cable television. *Id.* This language would thus regulate what people who legitimately pay for services are allowed to connect to the home entertainment centers in their own living rooms. *Id.* The Delaware statute differs from the Model Act the EFF was evaluating, especially in regard to the preamble. However, these concerns are probably still present because of the potentially broad reading of DEL.CODE.ANN. tit. 11, §850(e)(5)(a)(2001), and the separating clause for "program" as discussed *infra* in notes 44, 46. Further, even if consumer acts are not covered under the Delaware law because of the omission of "possess" and "use" from the preamble, the effect is the same because no devices would be able to be manufactured for sale unless "express consent" from telecommunication services.

[51] EFF LINE-BY-LINE, *supra* note 5. This term when combined with the 'authorization' language discussed in note 53 and accompanying text, may outlaw all home networking equipment that has not been 'expressly authorized' by your ISP. However, the language difference between the Delaware law and the Model Act may be significant here since Delaware omitted 're-transmit' from the prohibited acts and this is the language that most directly effects home networking equipment. However, it is arguable that 'transmit' can be read to cover the same acts.

[52] EFF LINE-BY-LINE, *supra* note 5. This came up before during the interpretation of the definition of 'unlawful telecommunication device' *infra* note 44. See *infra* discussion Part IV.

[53] DEL.CODE.ANN. tit. 11, §850(a)(1)(a)(2001).

[54] EFF LINE-BY-LINE, *supra* note 5.

[55] *Id.*

ted are forbidden."[56] Thus on a broad reading of the Delaware statute, a telecommunication service provider could require patrons to only use those devices of which they expressly approve, and the use of anything else could result in criminal and civil liability under this act.[57]

Delaware subsection (a)(1)(b) is structurally very similar to subsection (a)(1)(a) as it also falls under the preamble section discussed above and is virtually identical to its corresponding MPAA Model Act provision.[58] Like both the preamble and subsection (a)(1)(a), this subsection of the Delaware code in some ways appears a bit narrower than the Model Act.[59] However, the apparently narrowing language "evincing an intent to use the same in the commission of any offense," while adding an intent requirement, also seems to radically expand the reach of subsection (a)(1)(b).[60] Because the Delaware law says "any offense" it can conceivably be used as an additional offense to virtually any crime that involves anonymous communication, even though that goes far beyond the MPAA's stated purpose of stopping cable and other telecommunication service theft.[61] This also is ambiguous because "offense" is not defined; it is impossible to know if it extends to felonies, misdemeanors, or even city ordinance violations. Further, a broad reading of subsection (a)(1)(a) like that of the EFF would expand this even further. For example, if a phone company prohibited the use of Caller-ID block devices, a subscriber who used one would be in violation of both subsections (a)(1)(a) and (a)(1)(b).[62] Because the sub-

[56] EFF STEALTH, *supra* note 15.

[57] Discussion of "fair use" case split as to whether this broad reading in reasonably possible.

[58] To conceal, or to assist another to conceal from any telecommunication service provider or from any lawful authority, the existence or place of origin or destination, or the originating and receiving telephone numbers, of any telecommunication under circumstances evincing an intent to use the same in the commission of any offense. DEL.CODE.ANN. tit. 11, §850(a)(1)(b)(2001). *See infra* note 55 for a discussion of the differences from Model Act (a)(1)(ii).

[59] *Compare id. with* MPAA MODEL ACT, *supra* note 42, subsection (a)(1)(ii). The Delaware law adds "evincing an intent to use the same in the commission of any offense" creating a new intent requirement. The other added language "originating and receiving telephone numbers" doesn't seem to have any real effect as "origin and destination of . . . any telecommunication" would seem to cover everything as the added term and more.

[60] The MPAA REVISED MODEL ACT, *supra* note 3, subsection (a)(1)(ii) includes the language "provided that such concealment is for the purpose of committing a violation of subparagraph (i) above", which limits the reach of the intent language to only the SDMCA law itself.

[61] A possible example would be kidnappers calling in a ransom note and taking precautions to avoid being traced. While it may be a societal bonus to punish such people more, it does seem to go far a field of what SDMCA laws are supposed to be regulating.

[62] This example assumes that violating the contract term would be violating subsection (a)(1)(a) by acting to 'receive' a telecommunication service using a device 'without express authorization.' *See infra* notes 50-57.

scriber "concealed the origin" and "telephone number" of her call and did so knowing it was a violation of her contract with the phone company,[63] she has violated subsection (a)(1)(b) through her violation of subsection (a)(1)(a), which is "any offense."

Ignoring the intent language for a moment, it is possible to see a host of other issues raised by Delaware subsection (a)(1)(b).[64] Because the law bans concealing the origin or destination of any telecommunication, the Delaware law could actually ban legitimate computer security measures.[65] Concealment of the origin or destination of messages is a legitimate security measure that is commonly used, and thus a blanket ban could seriously impair computer security efforts.[66]

A common example is "firewall" technology, which places an electronic boundary between an internal computer network and the Internet.[67] These "firewalls" use a technology that hides the origin and destination of data packets to prevent hackers from learning the addresses of critical computers, and thus make it more difficult to break into these networks.[68] The ban on concealment would also stop many legitimate uses of encryption technology like virtual private networks, which allow off-site computers to act as though they were part of a secure network.[69] Both of these technologies hide information from eavesdropping hackers, but also have the effect of hiding the same information from telecommunication service providers and thus run afoul

---

[63] Even if she lacked actual knowledge, knowledge would be imputed because it was a term in a contract that she willingly entered into.

[64] These other issues are also raised by MPAA MODEL ACT, *supra* note 42, subsection (a)(1)(ii).

[65] *See* EDWARD W. FELTEN, 1 *at* http://www.freedom-to-tinker.com/doc/2003/security_29mar.doc (last visited October 3, 2004). Felten is an associate Professor of Computer Science at Princeton University and is one of the leaders in the fight against SDMCA laws. JOHN PALFREY, SING CANARIES SING, *at* http://blogs.law.harvard.edu/palfrey/2003/04/02#a82 (last visited October 3, 2004).

[66] FELTEN, *supra* note 65, 1.

[67] *Id.*

[68] *Id.*

[69] *See Id* at 2. Professor Felten gives an example to illustrate a legitimate use of encryption:

> [S]uppose an executive is waiting in an airport lounge, and she wanted to use the airport's wireless network to send a confidential email message to a client. To protect the message against the possibility of wireless eavesdropping, the executive's computer would establish an encrypted connection to her company's network. The email would travel through this encrypted "tunnel" back to the company network, and would then be forward on to its destination.This prudent use of encryption has the side effect of concealing the email message's destination from the provider of the airport's wireless communication service; so it would apparently run afoul of a ban on concealing message destinations.

Id.

of subsection (a)(1)(b).[70] One commentator suggested SDMCA provisions like Delaware's subsection (a)(1)(b) are unconstitutional because they prohibit anonymous communication, which is a constitutional right guaranteed by the First Amendment.[71]

The third main substantive section of the Delaware SDMCA law is subsection (a)(2).[72] This subsection, like the subsections discussed above, is extremely close to the language of the Model Act. Like the preamble language of subsection (a)(1), this section omits the terms "possesses", "uses" and "develops" from the list of prohibited acts.[73] The main issue in this subsection is how broadly "unlawful access device" and the prohibited acts of this section are defined, and thus how broadly the Delaware law outlaws certain technologies.[74] In some ways the definition of 'unlawful access device' is very narrow, since it prohibits only devices that are "primarily" for circumventing measures the telecommunication service providers take to prevent unauthorized access and does not simply bar any acts not expressly authorized by the telecommunication service provider.[75] This language thus seems to prohibit a different set of devices than subsections (a)(1)(a) or (a)(1)(b).[76] However, the apparent narrowness of subsection (a)(2)

---

[70] *See id.*

[71] TURNER, *supra* note 20. However, as we shall see later, subsection (a)(1)(b) does not likely violate this constitutional right. *See infra* discussion Part V.

[72] DEL.CODE.ANN. tit. 11, §850(a)(2)(2001) ("A person is guilty of a violation of this section if the person knowingly: Manufactures, assembles, distributes, possesses with intent to distribute, transfers, sells, offers, promotes or advertises for sale, use or distribution any unlawful access device").

[73] The effects of the language difference here is likely the same as in subsection (a)(1). *See infra* note 42.

[74] The Delaware law defines an 'Unlawful access device' as:

> Any type of instrument, device, machine, equipment, technology or software which is *primarily* designed, assembled, manufactured, sold, distributed, possessed, used or offered, promoted or advertised for the purpose of defeating or circumventing any technology, device or software, or any component thereof, used by the provider, owner or licensee of any telecommunication service . . . to protect such telecommunication . . . from unauthorized receipt, acquisition, access, decryption, disclosure, communication, transmission or retransmission."

DEL.CODE.ANN. tit. 11, §850(e)(6)(2001) (emphasis added). This language is word-for-word identical to the MPAA MODEL ACT, *supra* note 42, subsection (e)(5). Note, however, that this language appears to prohibit making or possessing a tool that is designed to circumvent, even where the circumvention might otherwise be permitted under the Federal DMCA. EFF LINE-BY-LINE, *supra* note 5. Also note that the MPAA REVISED MODEL ACT, *supra* note 3, subsection (e)(5), specifically includes the phrase "in violation of otherwise applicable law" after "circumventing" to explicitly deal with this problem.

[75] *See* discussion *infra* notes 50-57 and accompanying text.

[76] However, it may be a somewhat broad group of devices since the devices prohibited in subsection (a)(2) are prohibited from doing additional acts: "interception", "disclosure", and "re-transmission"

may be illusory because of the definition of "manufacture or assembly of any unlawful access device."[77] This definition goes far beyond devices used "primarily" for circumvention with the separating phrase "or modif[ies], alter[s], program[s], or reprogram[s] any instrument . . . so that it is capable of defeating or circumventing."[78] However, given the context this expansion just fleshes out the rule rather than expanding it, since the subsection taken as a whole is arguably only prohibiting the changing of any device into one "primarily" for "circumvention" purposes.[79] Thus while subsection (a)(2) could potentially ban a broad range of devices, on balance it is the least troubling subsection of the four discussed here.[80]

The final subsection of the Delaware SDMCA law that will be analyzed is subsection (a)(3)(a).[81] This subsection, again like those before it is very close to the language of the Model Act. The more significant differences in language are again are the omission of the terms "pos-

---

[77] The Delaware law defines the 'Manufacture or assembly of any unlawful access device' as:

> To make, produce or assemble an unlawful access device *or modify, alter, program, or reprogram any instrument, device, machine, equipment, technology or software so that it is capable of defeating or circumventing* any technology, device or software used by the provider . . . of a telecommunication service . . . to protect any such telecommunication . . . from unauthorized receipt, acquisition, access, decryption, disclosure, communication, transmission or retransmission, or to knowingly assist other in those activities.

DEL.CODE.ANN. tit. 11, §850(e)(7)(2001) (emphasis added). This language is word-for-word identical to the MPAA MODEL ACT, *supra* note 42, subsection (e)(6).

[78] DEL.CODE.ANN. tit. 11, §850(e)(7)(2001).

[79] This is not necessarily true however, since a device could be programmed to be 'capable' of 'circumvention', but still be primarily for non-circumvention uses. The broadness of this section really depends on how broadly 'program' is read. *See infra* note 44.

[80] *See* EFF LINE-BY-LINE, *supra* note 5. The EFF suggests that the revised Model Act version of this definition, makes no sense within the SDMCA because it only prohibits three verbs of the thirteen prohibited elsewhere. *Id.* Further, it is a meaningless narrowing because the remaining verbs reach anything that "manufacture, assemble or develop" might reach. *Id.*

[81] Subsection (a)(3)(a) states:

> A person is guilty of a violation of this section if the person knowingly: Prepares, distributes, possesses with intent to distribute, transfers, offers, promotes or advertises for sale, use or distribution; Plans or instructions for the manufacture or assembly of an unlawful telecommunication or access [sic] device under circumstances evincing an intent to use or employ the unlawful telecommunication access device, or to allow the unlawful telecommunication or access device to be used, for a purpose prohibited by this section, or knowing or having reason to believe that the unlawful telecommunication of access device is intended to be so used, or that the plan or instruction is intended to be used for the manufacture o[r] assembly of the unlawful telecommunication or access device

DEL.CODE.ANN. tit. 11, §850(a)(3)(a)(2001). Note, this is nearly identical to MPAA MODEL ACT, *supra* note 42, subsection (a)(4)(i). The differences are pointed out in note 82 *infra* and accompanying text.

sesses" and "uses" from the list of prohibited acts.[82] However, these minor differences are not the source of the potential problems with this section of the Delaware law. This prohibition on "plans or instructions" could effectively outlaw the publication of computer security and circumvention research.[83] The EFF has suggested this section "pushes the boundaries of the First Amendment" by attacking the mere publication of "instructions [or] plans."[84] The EFF admits, however, that the intent language in the law may rescue it from obvious constitutional difficulties, although the MPAA has made no showing that criminalizing the publication of truthful information is necessary here.[85]

It is difficult, on just the language of the statute, to determine exactly what intent would be necessary under this subsection.[86] An example may help illustrate this difficulty. Suppose a computer security researcher discovered a way to use a simple piece of software to circumvent a telecommunication service protection measure.[87] If she publishes her findings, would she be doing so with "reason to believe" that someone else would duplicate this method? Our researcher may well be guaranteed to violate subsection (a)(3)(a) because other researchers would attempt to duplicate this method to test the accuracy of her claims. If this is the result, a great deal of computer security and circumvention research could thus be illegal under SDMCA laws with provisions like subsection (a)(3)(a).[88]

Overall the four substantive subsections of the Delaware SDMCA law raise many potential problems. However, because this law has yet to be applied it is impossible to know how broadly a court will read this language. Given this environment of uncertainty, it may be useful to compare this potentially problematic statute, with the narrower Florida SDMCA law that was passed after the critics were able to have their

---

[82] The effect of the language difference here is likely the same as in subsection (a)(1). *See infra note* 42.

[83] Indeed, a graduate student who studies computer security has moved all of his research papers and tools overseas because of potential liability under a similar Michigan provision. Kevin Poulsen, *'Super-DMCA' Fears Suppress Security Research*, SECURITYFOCUS, Apr. 14, 2003, *available at* http://www.securityfocus.com/news/3912 (last visited October 3, 2004).

[84] EFF LINE-BY-LINE, *supra* note 5 (looking at identical language in the revised Model Act). This is not an unreasonable interpretation, *See infra* discussion Part V.

[85] *Id.* This First Amendment concern will be addressed *infra* Part V.

[86] The statute gives no further definitions to help clarify this issue.

[87] This alone may violate DEL.CODE.ANN. tit. 11, §850(a)(1)(a)(2001), because he 'programmed' a 'telecommunication device' to 'receive' or possibly 'decrypt' a telecommunication service.

[88] This is another point of potential conflict with the Federal DMCA as will be discussed in Part V *infra*.

views known.[89] The Florida law, unlike the Delaware law, is radically different from the MPAA's Model Act.[90]

For each of the four substantive parts of the Delaware law discussed above, the Florida law has a much narrower version or no law at all. The Florida version of Delaware's preamble subsection (a)(1) has a higher mens rea requirement and focuses on the service itself.[91] However, it is difficult to determine if the "intent to defraud" language is much of an improvement because it causes almost as much ambiguity as the Delaware law.[92] The focus on the service is a better fit for the stated goal of SDMCA laws: to crack down on theft of service and piracy. However, this positive aspect of the law may be overridden by the subsection of this Florida law, which closely matches Delaware's (a)(1)(a).[93] This subsection, like its Delaware counterpart, focuses on the manufacture and distribution of devices for the unauthorized receipt of a communication service. But, the language is still narrower in

---

[89] However, the critics are still trying to get rid of even this narrower law. Letter from Consumer Federation of America, Consumer Project on Technology, Consumers Union, Digitalconsumer.org, Electronic Frontier Foundation, and Public Knowledge, to Governor Jeb Bush (Apr. 17, 2003) *available at* http://www.eff.org/IP/DMCA/states/letter-gov-bush.php (last visited October 1, 2004) (urging the governor to veto this bill).

[90] FLA. STAT. ANN. §812.15 (2003).

[91] The Florida law states:

> A person may not knowingly intercept, receive, decrypt, disrupt, transmit, retransmit, or acquire access to any communications service without the express authorization of the cable operator or other communications service provider, as stated in contract or otherwise, with the intent to defraud the cable operator or communications service provider, or to knowingly assist other in doing those acts with the intent to defraud the cable operator or other communications provider.

Id. at (2)(a). Note, however, that the Florida law still has the same problems with "disrupt" as the Delaware law, *See infra* note 44. The "transmit" and "retransmit" language also have the same potentially broad reading as their Delaware counterparts, *See infra* note 51. Also note the term "develop" remains in the Florida law though it was omitted from the Delaware law. This could have an effect of chilling communication device research and development which is not present in the Delaware law. *See infra* note 42.

[92] *See* EFF LINE-BY-LINE, *supra* note 5 (discussing similar language in the revised Model Act). While this added "intent to defraud" language appears to add a higher level of mens rea, it is almost as ambiguous as the Delaware law. If a customer were to defy the terms of the contract and hook up a device not expressly authorized, would that be with intent to defraud? One favorable aspect of the Florida language is that a court is more likely to interpret it more narrowly because the "intent to defraud" is more in line with the stated purpose of SDMCA laws than the pure "express authorization" laws like Delaware's.

[93] The Florida law states:

> For the purposes of [(2)(a)], the term 'assist others' includes: The sale, transfer, license, distribution, deployment, lease, manufacture, development, or assembly of a communications device for the purpose of facilitating the unauthorized receipt, acquisition, interception, disruption, decryption, transmission, retransmission, or access to any communications service offered by a cable operator or any other communications service provider.

FLA. STAT. ANN. §812.15 (2)(a)(1) (2003).

the Florida law because it lacks any separating clause and thus the requirement of "purpose" in facilitating unauthorized acts runs through the whole statute. Another part of the Florida law under the preamble is narrower than its corresponding subsection in the Delaware law. Florida's section (2)(a)(1) very roughly corresponds to Delaware's section (a)(2).[94] While these two statutes generally cover the same types of devices and acts, the Florida definitions make it a much narrower rule. Where the Delaware law's definition of 'unlawful access device' had a potentially broad application due to the separating clause "or modifies, alter, program, or reprogram any instrument . . . so that it is capable of defeating or circumventing,"[95] the Florida definitions specifically exempt "multipurpose devices."[96] As well as adding the higher mens rea of "intent to defraud" already discussed,[97] the Florida language also significantly limits and carefully defines exactly which devices are exempted from prohibition.

Further, some of the problems noted in the Delaware law are not even present in the narrower Florida law. There is no language in the Florida statute that corresponds to the "conceal" language of Delaware subsection (a)(1)(b) or the "plans or instructions" language of Delaware subsection (a)(3)(a). Although critics of SDMCA laws still have problems with the Florida law, it is a much better law than Delaware's.

---

[94] The Florida law states:

> For the purpose of this section, the term 'assist others' includes: The sale, transfer, license, distribution, deployment, lease, manufacture, development, or assembly of a communications device for the purpose of defeating or circumventing any effective technology, device, or software, or any component part thereof, used by a cable operator or other communications service provider to protect any communications service from unauthorized receipt, acquisition, interception, disruption, access, decryption, transmission, or retransmission.

FLA. STAT. ANN. §812.15 (2)(a)(2) (2003). While generally narrower and thus less problematic than the Delaware statute, this language still has the difficulties associated with "disrupt", "transmit" and "retransmit" *See infra* notes 44, 51, 91.

[95] *See infra* discussion Part III.

[96] The Florida law states:

> A person that manufactures, produces, assembles, designs, sells, distributes, licenses, or develops a multipurpose device shall not be in violation of this section unless that person acts knowingly and with an intent to defraud a communications service provider and the multipurpose device: (a) Is manufactured, developed, assembled, produced, designed, distributed, sold, or licensed for the primary purpose of committing a violation of this section; (b) Has only a limited commercially significant purpose or use other than for the commission of any violation of this section; or (c) Is marketed by that person or another acting in concert with that person's knowledge for the purpose of committing any violation of this section.

FLA. STAT. ANN. §812.15 (5)(12) (2003). "'Multipurpose device' means any communications device that is capable of more than one function and includes any component thereof." *Id.* at (1)(g).

[97] *See infra* discussion Part III.

The Florida law still advances the MPAA's stated purposes for the Model Act. However, it does so without broadly prohibiting beneficial activities, which the Model Act and Delaware SDMCA laws do.

Thus the critics have some excellent reasons to believe SDMCA laws are overly broad and have the potential to go well beyond the stated purposes of the MPAA. However, there are also significant constitutional issues that may further plague SDMCA laws like Delaware's.

IV. SDMCA AND PREEMPTION

Laws with potentially broad reach, like Delaware's SDMCA law, may go so far as to create federal preemption issues. Generally speaking there are three ways that a state law can be preempted by federal law: explicit preemption, conflict preemption, and field preemption.[98] Congress' preemption power comes directly from the Supremacy Clause of the Constitution.[99] Explicit preemption occurs where Congress' command is stated directly by statute or implicitly contained in the structure or purpose of a statute.[100] Conflict preemption arises when complying with both federal and state laws is physically impossible or where state law stands as an obstacle to accomplishing and executing the full purposes and objectives of Congress.[101] Finally, field preemption occurs where the federal regulation scheme is so pervasive that it makes a reasonable inference that Congress left no room for the States to supplement it, and thus the federal interest is so dominant that it precludes the enforcement of state laws on the same subject.[102] In copyright law, courts usually do not deal with field preemption because Congress acted in explicit terms through section 301. Thus courts focus exclusively on explicit preemption through section 301 of the Copyright

---

[98] ROBERT A. GORMAN & JANE C. GINSBURG, COPYRIGHT: CASES AND MATERIALS 900 (6th ed. 2002).

[99] The Supremacy Clause states:

> This Constitution, and the Laws of the United States which shall be made in Pursuance thereof; and all Treaties made, or which shall be made, under the Authority of the United States, shall be the supreme Law of the Land; and Judges in every State shall be bound thereby, any Thing in the Constitution or Laws of any State to the contrary notwithstanding.

U.S. CONST. ART. VI, cl. 2. However, the Supremacy clause is generally only considered in conflict and field preemption.

[100] GORMAN & GINSBURG, *supra* note 98, at 900 (giving a copyright section, 17 USC §301, as an example of this type of preemptory statute).

[101] *Id.* This is how Supremacy clause preemption is usually analyzed in copyright law. *See* DAVID NIMMER, COPYRIGHT: SACRED TEXT, TECHNOLOGY, AND THE DMCA, 302 (2003) ("[S]tate law need not fall within Congress's authority under the Copyright Clause to interfere with the objectives of Congress.")

[102] GORMAN & GINSBURG, *supra* note 98, at 900.

Act and conflict preemption by the power of the Supremacy clause itself.[103] The Delaware law may fit into this more limited preemption analysis because the subject matter of the law is so similar to parts of the copyright code.[104] As illustrated below, the Delaware SDMCA law appears to be preempted in all three ways despite the copyright focus of the law.

Section 301 of the Copyright Act of 1976 has broad reach to all rights within the general scope of copyright law, but it may not be broad enough to reach the Delaware SDMCA law.[105] As the critics have pointed out by calling it a "Super-DMCA" law, the Delaware law is far more analogous to the section 1201 rights under the federal DMCA than it is to any of the rights under 106.[106] Two elements must coalesce in order for any state law to be preempted under section 301: firstly, the state law must create "legal or equitable rights that are equivalent to any of the exclusive rights within the general scope of copyright as specified by section 106;"[107] and secondly, such rights under state law may be claimed in "works of authorship that are fixed in a tangible medium of expression and come within the subject matter of copyright as specified by sections 102 and 103."[108] Thus, if under state law the act of reproduction, performance, or display will in itself infringe the state-created right, then such right is preempted.[109] If instead, qualitatively other elements are required instead of or in addition to the acts of reproduction, performance, or display in order to constitute a state-related cause of action, then the right does not lie "within the general scope of copyright."[110]

In general the title of "SDMCA" as given by the critics is accurate; for the most part the Delaware law covers the anti-circumvention rules in section 1201 of the DMCA. However, there is one part of the Delaware law that may meet the two-element requirements and thus may be

---

[103] 1 MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT § 1.01B (2003).

[104] However, as we shall see, the broader nature of the Delaware SDMCA law makes field preemption specifically applicable.

[105] *See* 17 U.S.C. §301 (2001). This section only covers "all legal or equitable rights that are equivalent to any of the exclusive rights within the general scope of copyright as specified by section 106 in works of authorship that are fixed in a tangible medium of expression and come within the subject matter specified by sections 102 and 103." *Id.*

[106] *See* 17 U.S.C. §106 (2001). This section generally covers rights of reproduction, distribution, performance, and display of copyrighted works. *Id.* Superficially this does not appear to correspond to any of the prohibitions in the Delaware SDMCA law. However, 17 USC §1201, deals with prohibitions of circumventing access and copy controls protecting copyrighted works.

[107] NIMMER &NIMMER, *supra* note 103, at §1.01B.

[108] *Id.*

[109] *Id.*

[110] *Id.*

preempted under section 301 of the Copyright Act: the prohibition on transmissions under subsection (a)(1)(a).[111] An example may help illustrate how this works. If a person were to program her computer to transmit a streaming version of a copyrighted movie from her cable service to a member of the public, she would be in violation of the author's exclusive right to perform the work under section 106.[112] This very same act would violate Delaware's subsection (a)(1)(a) because the separating clauses only require that the person "knowingly . . . program . . . a telecommunication device" "to transmit . . . any telecommunication service without the express consent . . . of the telecommunication service provider."[113] Only the additional mens rea requirement differs from copyright law, which is strict liability. However, several courts have suggested that the mere fact that a state law requires scienter cannot save that state law from preemption.[114] Although this example is on uncertain ground to preempt this part of the Delaware SDMCA law, other sections of the Delaware law are far more suspect.

Beyond the section 301 problem, the Delaware law may also be preempted by its conflict with the federal DMCA. Specifically, the Delaware law's potentially broad reach and lack of exceptions may directly eliminate some of the exceptions in the federal DMCA and thus conflict with Congress's purpose.

Under the reverse engineering exception of the federal DMCA, the information acquired through circumventing technological control measures for the purpose of achieving interoperability of an independently created program with technical means or devices, may be made available to others if done to enable interoperability of other programs.[115] Looking again at Delaware subsection (a)(3)(a),[116] there appears to be a conflict, if not physical impossibility. The Delaware law prohibits all publishing of plans or instructions regarding telecommuni-

---

[111] The text of 11 Del.C §850(a)(1)(a) is quoted *infra* at notes 37 and 43.

[112] This example assumes that the person transmitting does not own the work or have the permission of the author.

[113] DEL.CODE.ANN. tit. 11, §850(a)(1)(a)(2001). Under this interpretation the definition of 'unlawful telecommunication device' is irrelevant. This analysis does however assume that the cable service provider did not give the transmitter permission to stream the movie over the Internet, which is certainly more likely than actual express consent.

[114] NIMMER &NIMMER, *supra* note 103, at §1.01B n. 58 (citing Rand McNally & Co. v. Fleet Management Sys., Inc., 591 F.Supp 726 (N.D. Ill. 1983); Peckarsky v. American Broadcasting Co., 603 F.Supp 688 (D.D.C. 1984); Sygma Photo News, Inc. v. Globe Int'l, Inc., 616 F.Supp 1153 (S.D.N.Y. 1985).

[115] 17 U.S.C. §1201(f)(3) (2001) (referencing (f)(1) and (f)(2) as to what the information can be).

[116] For full text of statute *See infra* note 81.

cations devices that can access services without the express authorization of the service provider. Where an engineer wishes to share a tool he used to discover or accomplish interoperability, he may be within the federal 1201(f) exception and be in violation of the Delaware law.

This same issue arises in an even stronger form in the encryption research exception under the federal DMCA. There are several factors under this section that must be considered to determine whether information about circumventing technology measures can be made publicly available.[117] Among these factors are whether the information derived from the research is disseminated in a way that advances the knowledge in the field of encryption research and development of encryption technology,[118] and whether the person is engaged in a legitimate course of study.[119] The Delaware law, while focusing on a slightly different area of circumvention,[120] would deny encryption researchers the ability to publish any plans or instructions regarding flaws in communication service access protections no matter how much it may advance the knowledge of in the field or how legitimately the research was conducted. Thus, again there seems to be a direct conflict between Delaware's subsection (a)(3)(a) and an exception Congress put into the federal DMCA.

A final area where the Delaware law may conflict with the federal DMCA is in the area of personally identifying information. Under section 1201(i) of the federal law, circumvention is permitted to disable technological measures protecting works which collect or disseminate personally identifying information.[121] Although this is not a broad right to circumvent, those users who do fall under section 1201(i) would likely be in violation of Delaware subsection (a)(1)(b).[122] A person acting to protect his or her anonymity in regard to online works, thus falling within this federal exception, would be in direct violation of the

---

[117] 17 U.S.C. §1201(g)(3) (2001).

[118] 17 U.S.C. §1201(g)(3)(A) (2001) As opposed to being distributed in a way that facilitates infringement.

[119] 17 U.S.C. §1201(g)(3)(B) (2001)

[120] The Delaware law is focused on technological measures surrounding telecommunication services as opposed to technological measures preventing unauthorized access and copying of copyrighted works like the DMCA. Since much of what goes over telecommunication services is copyrighted work (hence it is the MPAA is who is pushing the SDMCA laws), there is significant overlap.

[121] 17 U.S.C. §1201(i)(1) (2001). This exception is somewhat qualified as the technological measure must collect or disseminate information reflecting the online activities of a natural person and it does so without disclosing this collection or dissemination function and giving the user a chance to disable it. *Id.* Further the act of circumvention must be for the sole purpose of disabling this collection or dissemination function, and have no other effect. *Id.*

[122] Full text available at *infra* note 58.

Delaware law by concealing the destination of a communication service.

Thus it appears that there are several parts of the Delaware statute that may be in direct conflict with the federal DMCA under certain circumstances. However, this does not mean that those sections are certainly preempted, because no courts have yet interpreted SDMCA laws like Delaware's. It is possible that a sufficiently narrow reading or judicially created exceptions matching those of the federal DMCA, could save these sections from preemption.

This is, however, not the end of the preemption analysis. While generally field preemption analysis is not done in the copyright context, the para-copyright qualities of SDMCA laws make it relevant. As mentioned before, field preemption occurs where the federal regulation scheme is so pervasive that it expresses a reasonable inference that Congress left no room for the States to supplement it.[123] This scheme includes any federal administrative regulations that are validly adopted.[124] It is arguable that such a scheme may be in effect in the area of telecommunication services. This conclusion was reached by a legislative report analyzing the similar, but narrower Florida law:

> Under the Communications Act of 1934, the Federal Communications Commission ("FCC") has extremely broad authority to regulate all aspects of communication. Indeed, the FCC has repeatedly stated that it has the authority to preempt state and local regulation in this area as it sees fit. Although [later legislation] specifically allows for state or local enfranchisement of cable providers, the FCC retains the authority to preempt any state or local regulation in furtherance of Congress's stated policy of ensuring that interstate communication remains a uniform field throughout the country. At a *minimum*, this may mean that all the provisions of this bill are subject to preemption by the FCC at any time; arguably, it may mean many if not all of its provisions are invalid due to federal occupation of the field.[125]

This analysis is just as valid in regard to the Delaware SDMCA law, if not more so. Because the Delaware law is so much broader in its regulation of communications, it has a greater propensity to interfere with the FCC's regulatory scheme. Further, because the Delaware law makes communication service regulation in that state so different than in other states, it is more directly in conflict with Congress's stated policy of uniformity throughout the nation.

---

[123] GORMAN & GINSBURG, *supra* note 98, at 900.

[124] STATE OF FLA. LEGISLATIVE STAFF, JUDICIAL ANALYSIS OF HB 79, 186th Session, at 5 *available at* http://www.flsenate.gov/data/session/2003/House/bills/analysis/pdf/h0079a.ju.pdf [herinafter JUDICIAL ANALYSIS] (citing Fidelity Federal Savings & Loan Assn. v. De la Cuesta, 458 U.S. 141 (1982)) (last visited October 3, 2004).

[125] *Id.* (citations omitted)(emphasis added).

As one can see, the Delaware SDMCA law raises significant preemption issues and thus may be in violation of the Supremacy Clause. As Part V explains, this law may also have serious constitutional problems.

V. Constitutional Problems with SDMCA Laws

Two significant constitutional problems are raised by the Delaware SDMCA law. First, the Delaware law may impermissibly delegate state legislative power to private parties. Second, the Delaware law may violate the First Amendment. These issues will be discussed here only in regard to the application at hand, since a more complete analysis is beyond the scope of this article.

A. *Delegation of Legislative Power*

As a general rule, it is impermissible for Congress or a state legislature to delegate the legislative powers of that body to another group or agency.[126] In this case, the Delaware law delegates legislative power to private parties. While the Delaware Supreme Court has not directly addressed this issue,[127] the United States Supreme Court has.[128] In *A.L.A. Schechter Poultry Corp. v. United States*,[129] the Court struck down a federal statute as unconstitutional solely on delegation grounds.[130] However, this general ban on legislative delegation is not absolute and does not bar a legislature from delegating powers that are not strictly legislative in nature.[131] The power delegated in the Delaware SDMCA law is, however, central to legislative power: the determination of what constitutes a crime. The phrase "without the express consent or authorization of the telecommunication service provider" in Delaware (a)(1)(a) appears to delegate to private parties the authority to determine what acts do or do not constitute a crime.[132] This point, combined with the criminal rule of lenity, strongly suggests that the Delaware SDMCA law may unconstitutionally delegate legislative power.[133] Note, further, that the Delaware SDMCA law's definition of "unlawful telecommunication device" in section (e)(5) also includes

---

[126] AMJUR CONSTLAW § 297.

[127] However, a superior court did strike down a state law partially due to this delegation issue in 1936. *See* Becker v. State 185 A. 92 (Del. Super. 1936).

[128] *See* A.L.A. Schechter Poultry Corp. v. United States, 295 U.S. 495 (1935).

[129] *Id.*

[130] Judicial Analysis, *supra* note 124, at 4 (citing A.L.A. Schechter Poultry Corp., 295 U.S. 495 (1935)).

[131] 16 Am. Jur. 2d *Constitutional Law* § 297 (1997).

[132] *See* Judicial Analysis, *supra* note 124, at 4 (discussing the Florida SDMCA law).

[133] *See Id.*

this 'without express authorization' language.[134] This makes the delegation issue far more troublesome, because it taints all uses of the term 'unlawful telecommunication device' with this constitutional issue.[135]

B. *First Amendment Issues*

Two specific sections of the Delaware SDMCA law create other serious constitutional concerns regarding the First Amendment. The concealing section (a)(1)(b),[136] and the plans or instruction section (a)(3)(a),[137] create distinct First Amendment problems. Subsection (a)(1)(b) may infringe on a citizen's First Amendment right to communicate anonymously. Subsection (a)(3)(a) involves a more direct regulation of speech. However, because (a)(3)(a) outlaws crime-facilitating speech, this restriction may be permissible. Both of the issues created by these sections are in somewhat uncharted areas of First Amendment jurisprudence

1. Subsection (a)(1)(b) and Anonymous Speech

By criminalizing the concealment of one's online identity, section (a)(1)(b) appears to infringe, though somewhat indirectly, on a citizen's right to communicate anonymously.[138] In *McIntyre v. Ohio Elections Commission*[139] the Supreme Court struck down a law prohibiting the circulation of political pamphlets that did not include the author's name and address.[140] This name requirement served both as a speech compulsion and a speech restriction since the law either required an author to give his or her name or restricted the circulation of any anonymous

[134] *See infra* note 43.

[135] This term is used in three of the four substantive sections of the Delaware law discussed in this article. Thus all of the section discussed except subsection (a)(2) which is solely concerned with unlawful access devices, may be made unconstitutional by this delegation issue.

[136] *See infra* note 58 for the exact language of the section.

[137] *See infra* note 81 for the exact language of the section.

[138] The Supreme Court discussed the right to speak anonymously in Buckley v. American Constitutional Law Foundation, Inc., 525 U.S. 182, 200 (1999) (holding the First Amendment was violated by requiring people circulating petitions to wear name badges); McIntyre v. Ohio Elections Commission, 514 U.S. 334, 347 (1995) (holding that a state statute which prohibited the distribution of anonymous campaign literature was unconstitutional); Buckley v. Valeo, 424 U.S. 1 (1976) (holding the federal statute requiring disclosure of donors to political parties to be constitutional, although it noted there may be circumstances in which the statute may be unconstitutionally applied); Talley v. California, 362 U.S. 60, 66-8 (1960) (holding that a Los Angeles ordinance requiring that any handbill must contain the names of the persons who wrote and distributed it was invalid on its face); NAACP v. Alabama, 357 U.S. 449, 462 (1958) (holding the state could not compel the NAACP to reveal its membership without violating the First Amendment).

[139] *McIntyre*, 514 U.S. 334 (1995)

[140] *Id.* at 338 n.3, 357.

pamphlet.[141] The Ohio law challenged in this case restricted speech due to its communicative impact, and was thus subject to strict scrutiny review.[142] Delaware subsection (a)(1)(b) is also focused on the communicative impact of the speech, and thus would be subject to this same level of scrutiny.[143]

The strict scrutiny analysis requires that the restriction be necessary to serve a compelling state interest and be narrowly tailored to achieve that end.[144] To be narrowly tailored a law must substantially advance the compelling interest, not be ex ante over-inclusive,[145] be the least intrusive means, and not be under-inclusive.[146]

In applying strict scrutiny to the Ohio statute in *McIntyre,* the Supreme Court strongly suggested that a law like Delaware's section (a)(1)(b) might be constitutionally valid. The statute in *McIntyre* was struck down because the state attempted to prevent misuses of anonymous speech, like fraud, by prohibiting all uses of that speech.[147] The Court suggested that a State "cannot . . . punish fraud indirectly by indiscriminately outlawing a category of speech, based on its content, with no necessary relationship to the danger sought to be prevented."[148]

This brings us back to the language of subsection (a)(1)(b) which prohibits, "conceal[ing] . . . the existence or place of origin or destination . . . of any telecommunication *under circumstances evincing an in-*

---

[141] This point may be meaningless however as the Supreme Court suggested that speech compulsions and speech restrictions are equivalent for First Amendment purposes. Riley v. National Federation for the Blind of North Carolina, Inc., 487 U.S. 781, 796-7 (1988).

[142] *McIntyre*, 514 U.S. at 347.

[143] The Delaware law prohibits "conceal[ing] . . . the existence or place of origin or destination . . . of any telecommunication." DEL.CODE.ANN. tit. 11, §850(a)(1)(b)(2001). This relates to the communicative impact because sending a telecommunication without an IP address or phone number attached to it specifically prohibits telecommunications that do not include identifying information, which is arguably part of the speech. Restating this conclusion in the negative: subsection (a)(1)(b) does not restrict this conduct for its non-communicative element as the law at issue in Clark v. Community for Creative Non-Violence, 468 U.S. 288 (1984). In that case the Supreme Court determined that restricting the non-communicative aspects of camping as part of a protest were constitutional under the First Amendment because they were mere time/place/manner restrictions which were made without regard to the content of the expressive conduct. *Id.* at 293. Delaware's subsection (a)(1)(b) has no similarly content-neutral justification, and thus should be subject to strict scrutiny analysis.

[144] Perry Educ Ass'n v. Perry Local Educators' Ass'n, 460 U.S. 37, 45 (1983).

[145] This means the law cannot restrict speech, which does not implicate the interest that could have been excluded ex ante.

[146] EUGENE VOLOKH, THE FIRST AMENDMENT: PROBLEMS, CASES AND POLICY ARGUMENTS, Part II. I. (2001).

[147] McIntyre v. Ohio Elections Commission, 514 U.S. 334, 357 (1995).

[148] *Id.*

tent to use the same in the commission of any offense."[149] This intent language, while somewhat vague,[150] does appear to tailor subsection (a)(1)(b) to only apply to speech related to the fraud and other crime.[151] Thus, given the language in *McIntyre*, subsection (a)(1)(b) appears sufficiently tailored to pass the strict scrutiny test.[152]

Thus it appears that subsection (a)(1)(b) is able to meet the strict scrutiny standard required for laws that burden conduct for its communicative elements. As such, although subsection (a)(1)(b), creates considerable problems for computer security,[153] it does not appear likely to violate the First Amendment.

2. Subsection (a)(3)(a) and Crime-Facilitating Speech

In contrast to subsection (a)(1)(b), subsection (a)(3)(a) more directly restricts speech, and thus is easier to understand as a potential First Amendment issue.[154] Subsection (a)(3)(a) states that:

> A person is guilty of a violation of this section if the person knowingly: Prepares, distributes, possesses with intent to distribute, transfers, offers, promotes or advertises for sale, use or distribution; Plans or instructions for the manufacture or assembly of an unlawful telecommunication or access [sic] device under circumstances evincing an intent to use or employ the unlawful telecommunication access device, or to allow the unlawful telecommunication or access device to be used, for a purpose prohibited by this section, or knowing or having reason to believe that the unlawful telecommunication of access device is intended to be so used, or that the plan or instruction is

---

[149] DEL.CODE.ANN. tit. 11, §850(a)(1)(b)(2001) (emphasis added).

[150] For a full discussion of the problems caused by this language generally, *see infra* discussion Part III.

[151] The REVISED MODEL ACT, *supra* note 3, subsection (a)(1)(ii), which corresponds to Delaware subsection (a)(1)(3), is also likely constitutionally tailored. In fact the revised Model Act is even more narrowly tailored as it only prohibits concealment that is "for the purpose of committing a violation of subparagraph (i) above", which limits the reach of the intent language to only the SDMCA law itself. The original version of the Model Act, however, did not include any such intent language and thus is likely unconstitutional for the same reason as the Ohio statute in *McIntyre*. *See* MPAA MODEL ACT, *supra* note 42, subsection (a)(1)(ii).

[152] However, this conclusion is far from certain. In only one case in history has a majority of the Supreme Court found the strict scrutiny test passed. Austin v. Michigan Chamber of Commerce, 494 U.S. 652 (1990).

[153] *See infra* notes 65-71 and accompanying text.

[154] "[However, a few] lower court cases have suggested that there's no First Amendment problem with punishing crime-facilitating speech because it is 'speech brigaded with action' and 'an integral part' of a crime.'" Eugene Volokh, *Crime-Facilitating Speech*, 57 Stan. L. Rev. 1095, 1130 (2005) (citing e.g. NOW v. Operation Rescue, 37 F.3d 646, 655 (D.C. Cir. 1994)). However, using the 'conduct-speech' distinction to avoid First Amendment scrutiny is unsound. *Id.*

> intended to be used for the manufacture o[r] assembly of the unlawful telecommunication or access device.[155]

This section thus criminalizes speech (in the form of "plans or instructions") because of its content. As mentioned in the previous discussion of subsection (a)(1)(b), content-based restrictions are generally disfavored and are thus subject to strict scrutiny.

However, only protected speech receives this level of scrutiny, and it has been suggested by courts and legislatures that 'crime-facilitating' speech should not be constitutionally protected. The Supreme Court has not yet directly faced this issue.[156] Several federal circuit courts have considered this issue, but they did not come to a single standard.[157] Some of these circuit courts have found that speech, which intentionally or knowingly facilitates crime is not constitutionally protected.[158] Legislatures have also suggested that crime-facilitating speech is constitutionally unprotected by punishing crime-facilitating speech by statute.[159] Indeed, while not discussing the specifics, Justice Stevens suggested in a dissenting opinion that a crime-facilitating speech exception should be recognized.[160]

Given this background, subsection (a)(3)(a) appears to be saved from First Amendment scrutiny because of the "knowingly" and "intent" language that is littered throughout. Indeed one of the harshest critics of SDMCA laws, the Electronic Frontier Foundation, acknowledged that this kind of mens rea language may wipe away any First

---

[155] DEL.CODE.ANN. tit. 11, §850(a)(3)(a)(2001).

[156] This is by choice as the Court denied certiorari on a case that would have addressed the issue. *See* Stewart v. McCoy, 537 U.S. 993 (2002) (Stevens, J., respecting the denial of certiorari).

[157] Volokh, *supra* note 154, at 1129-30.

[158] *Id.* The courts which have used the intentional standard have found speech which "facilitates tax evasion, illegal immigration, drugmaking, and contract killing [to be] constitutionally unprotected." *Id.* at 1129, n.137 (citing e.g. United States v. Raymond, 228 F.3d 804, 815 (7th Cir. 2000) (tax evasion); Rice v. Paladin Enterprises, Inc., 128 F.3d 233, 243 (4th Cir. 1997) (contract killing); United States v. Aguilar, 883 F.2d 662 (9th Cir. 1989), *superseded by statute as noted in* United States v. Gonzalez-Torres, 273 F.3d 1181 (9th Cir. 2001) (immigration laws); United States v. Barnett, 667 F.2d 835, 842-43 (9th Cir. 1982) (drugmaking)). Three federal circuit courts have found the knowingly standard sufficient where the speech "facilitates bombmaking, bookmaking, [or] illegal circumvention of copy protection." *Id.* at 129, n.138 (citing Universal City Studios, Inc., v. Corley, 273 F.3d 429, 457 (2nd Cir. 2001) (circumventing copy protection); United States v. Mendelsohn, 896 F.2d 619, 624 (9th Cir. 1990) (bookmaking); United States v. Featherston, 461 F.2d 1119, 1122 (9th Cir. 1972) (bombmaking)).

[159] *Id.* at 1130, nn. 142-43 (citing e.g. 50 U.S.C. §1861(d) (added by the USA Patriot Act) and MINN. STAT. ANN. §609.4971). 50 U.S.C. §1861(d) is an example of a law which punishes crime-facilitating speech without an intent requirement. *Id.* at 1130. MINN. STAT. ANN. §609.4971 is an example of a law which punishes crime-facilitating speech, but unlike the previous example, has an intent requirement. *Id.*

[160] Stewart v. McCoy, 537 U.S. 993 (Stevens, J., respecting the denial of certiorari)).

Amendment problem.[161] However, Professor Volokh suggested that a crime-facilitating speech exception should not depend on the speakers' mens rea.[162] A 'knowing' or 'reckless' requirement would be far too broad because it would outlaw lots of 'dual-use' speech, which while it could facilitate crime, also has many beneficial non-criminal uses to society.[163] For example, much of the research done in computer security necessarily explains current flaws and how to exploit them.[164] An 'intentional' or 'purposeful' requirement, although narrower than a 'knowingly' standard, is equally unhelpful as a way to distinguish crime-facilitating speech which should and should not be protected.[165] It is very difficult to prove what someone is thinking or intending, and factfinders can easily mistake 'knowledge' for 'intent.'[166] The advantages of an intent test are thus substantially outweighed by the difficulty of applying it.[167]

Further, refusing to protect speech on the speakers' mens rea focuses on the wrong issue. The harm caused by the speech is not affected by what the speaker's intent was, but rather the harm that flows from the damage caused by the speech.[168] Thus if a crime-facilitating speech exception is to be formulated, it should balance the potential harm caused by the speech as opposed to the 'dual-use' value of the speech.[169] Volokh's proposed crime-facilitating speech exception suggests that the only speech that should fall under such an exception is speech that either helps listeners "facilitates extraordinarily serious harms, such as nuclear or biological attacks" or has "virtually no non-criminal uses—for instance if it reveals social security numbers or computer security passwords."[170] Subsection (a)(3)(a) of the Delaware SDMCA would not fit within such an exception, and would thus have to be analyzed under strict scrutiny.

---

[161] EFF LINE-BY-LINE, *supra* note 5 (discussing the corresponding and nearly identical Model Act section).

[162] Volokh, *supra* note 154, at 1174-87.

[163] *Id.* at 1176.

[164] Consider the example of the Michigan graduate student whose studies may be illegal under the Michigan SDMCA law. *See infra* note 83.

[165] Volokh, *supra* note 154, at 1179-87.

[166] *Id* at 1185-87.

[167] *Id.* at 1194.

[168] *See id.* at 1194-5.

[169] *See id.* at 1208-09.

[170] *Id.* at 1217. Professor Volokh also suggests an exception for speech which is communicated to a "few people who the speaker knows are likely to commit a crime or to escape punishment." This proposed exception covers normal aiding and abetting and is not relevant to the present discussion because it does not involve widely distributed speech.

However, Professor Volokh has suggested that the strict scrutiny test is particularly ambiguous when applied to 'dual-use' speech, like that covered by Delaware's subsection (a)(3)(a).[171] The narrowly tailored requirement for strict scrutiny analysis in this context is troublesome because there are two possible meanings of the requirement and two meanings of a subpart of that requirement.[172] One meaning of narrowly tailored "is that an attempt to prevent the improper uses of speech must be narrowly tailored to only affect those uses."[173] The other view of narrow tailoring "is that the government interest may justify whatever is the least restrictive law necessary to prevent the harmful uses, even if the law also interferes with the valuable uses."[174] Thus, if the first definition of narrowly tailored is applied to subsection (a)(3)(a) the restriction will certainly fail because many valuable uses of the 'plans or instructions' will be prohibited.[175] The result under the second definition of narrow tailoring is less clear, since blocking the valuable use of such 'plans or instructions' may be necessary to prevent the criminal use of such speech.[176] Professor Volokh suggests that it is not clear that a court would even apply either version of strict scrutiny above because the Supreme Court has sometimes "struck down speech restrictions without even applying strict scrutiny."[177]

Taken together, this all suggests that strict scrutiny analysis is not very helpful in determining whether subsection (a)(3)(a) violates the First Amendment.[178] However, because of the broad sweep of the 'knowingly' language, as well as the damage this prohibition will do to computer security research, it seems unlikely that (a)(3)(a) could survive strict scrutiny.

VI. Conclusion

This paper illustrates many potential problems with the SDMCA legislation that the MPAA is currently pushing through state legislatures throughout the country. The Delaware SDMCA is a useful exam-

---

[171] *Id.* at 1132-33.

[172] *Id.*

[173] *Id.* at 1133 (citing Ashcroft v. Free Speech Coalition, 535 U.S. 234 (2002) as an example of this approach).

[174] *Id.* at 1134-35 (citing Buckley v. Valeo, 424 U.S. 1 (1976) as an example of this approach).

[175] Even if the mens rea language could be seen as limiting the ban, speakers would still be chilled by the potential of liability under this law. *See id.* (applying this definition to crime-facilitating speech generally).

[176] *See id.* at 1134-35 (applying this definition to crime-facilitating speech generally).

[177] *Id.* at 1135.

[178] *See id.* at 1136.

ple through which to examine these problems. It serves this purpose because it is current law and closely tracks the MPAA's Model Act on which all SDMCA laws are based. Thus the Delaware law shows both the feasibility and form of the SDMCA legislation that the MPAA is intent to bring to all fifty states

SDMCA laws are controversial and have been the subject of heated debate. This analysis suggests that the critics of SDMCA laws have the stronger side of the argument. The language of the Delaware SDMCA law is vague and overly broad. This legislation could be interpreted to grant invasive new powers to entertainment and telecommunications companies, at the cost of everyone else. Although these concerns are significant, perhaps even more significant are the problems that the critics have not fully addressed.

The SDMCA laws appear to encroach into areas of federal jurisdiction and some subsections may be preempted under express, field, and conflict preemption.

There are also significant constitutional issues raised by this law. Three of the four substantive subsections of the Delaware SDMCA may violate the constitution on delegation grounds. The language "unless expressly authorized" appears to give private entities the discretion to determine when a crime has been committed.

Finally two subsections of the Delaware SDMCA law raise First Amendment issues. Subsection (a)(1)(b) appears constitutional by virtue of the 'intent' language, which does not appear in the original MPAA Model Act. However, subsection (a)(3)(b) is a more direct restriction of speech and most likely violates the First Amendment.

Hopefully this analysis will help legislators understand the dangers of SDMCA laws and help critics in their fight to protect consumers' rights.