IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

AMERICA ONLINE, INC.,	)	
	)	
Plaintiff,	)	
	)	
v.	)	Civil Action No. 99-1186-A
	)	
NETVISION AUDIOTEXT, INC., et al.,	)	
	)	
Defendants.	)	
_____	)	

MEMORANDUM OF AMICUS CURIAE ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF MOTIONS FOR SUMMARY JUDGMENT BY DEFENDANTS NETVISION AUDIOTEXT, INC. ET AL., AND BY DEFENDANTS ROBERT L. ATKINSON ET AL.

TABLE OF CONTENTS

TABLE OF AUTHORITIES ii

INTEREST OF THE *AMICUS CURIAE* 1

INTRODUCTION 2

A. The Statutory Scheme 2

B. Possible Interpretations of the UBE Provisions of the Computer Crimes Act . . . 4

ARGUMENT 9

I. VIRGINIA'S LAWS GOVERNING THE UNAUTHORIZED TRANSMISSION OF UNSOLICITED BULK E-MAIL VIOLATES THE FIRST AMENDMENT 9

A. Virginia's UBE Statute Is Unconstitutionally Vague 9

1. Virginia's UBE Provisions Do Not Give Notice of What Conduct is Prohibited 9

2. Virginia's UBE Statute Impermissibly Delegates to Private Parties the Right to Determine What Conduct Is Prohibited 12

B. The UBE Provisions of Virginia's Computer Crimes Act Are Overbroad 14

C. Even if the UBE Provisions Governed Only Commercial Speech, They Nonetheless Would Violate the First Amendment 17

II. A CAUSE OF ACTION FOR TRESPASS TO CHATTELS BASED ON THE TRANSMISSION OF E-MAILS VIOLATES THE FIRST AMENDMENT 20

A. Judicial Enforcement of an Action for Trespass to Chattels Constitutes State Action 21

B. Application of the Tort of Trespass to Chattels to the Transmission of E-mails Should Be Limited to Protect First Amendment Rights 22

CONCLUSION 24

TABLE OF AUTHORITIES

Amicus Curiae Electronic Frontier Foundation ("EFF") hereby submits this memorandum in support of the motions for summary judgment of defendants Netvision Audiotext, Inc, John Bennett, and Joseph Elkind, and the motion for summary judgment of defendants Robert L. Atkinson, James Cattanach, Timothy Perkins, Tracey Rizzitello, Kyle Vernon, Michael Clark, Tiger Allen Yim, Kyle Fanning, and Margaretha Maak (collectively, "Defendants"). Plaintiff's claims brought pursuant to the Virginia Computer Crimes Act, Va. Code § 18.2-152 *et seq*., fail because the statute violates the First and Fourteenth Amendments to the U.S. Constitution. Moreover, plaintiff's claim for trespass to chattels should be dismissed because, when applied to the transmission of e-mail, such a broad claim violates the First Amendment.

INTEREST OF THE *AMICUS CURIAE*

Amicus EFF is a non- profit, civil liberties organization founded in 1990 that works to protect rights in the digital world. Based in San Francisco, California, EFF has members all over the United States, including the Commonwealth of Virginia, and maintains one of the most-linked-to Web sites (http://www.eff.org) in the world. EFF's Board of Directors includes such renowned legal scholars as Prof. Lawrence Lessig of Stanford Law School and Prof. Pamela Samuelson of Boalt Hall School of Law at the University of California, Berkeley.

As part of its online civil-liberties mission, EFF often participates in Internet-related litigation as a party, as counsel, and as *amicus curiae*: censorship cases like *Reno v. ACLU*, 521 U.S. 844 (1997), and *Multnomah County Public Library. v. United States*, 01-CV-1322 (E.D.Pa.); electronic privacy cases like *Steve Jackson Games v. U.S. Secret Service*, 36 F.3d 457 (5th Cir. 1994) and *U.S. Telecom Ass'n v. FCC*, 227 F.3d 450 (D.C. Cir. 2000), cases pitting intellectual property against free speech, like *Felten v. RIAA*, 01-CV-2669 (D.N.J.); and cases involving unwanted e-mail, like *Intel Corp. v. Hamidi*, No. 98 AS05067, 1999 WL 450944 (Cal. App. Dep't Super. Ct. Apr. 28, 1999),

appeal pending, No. 01 C033076 (Cal. Ct. App.).

Thus, EFF's interest in this case. Digital networks offer great opportunities for free speech, and the ability of individuals to send and receive e-mail is one of the Internet's most important features. But tension is growing between the First Amendment rights of members of the public, both as speakers and as hearers, society's interest in free expression, and the interests of those who fight what the Internet community calls "spam."

EFF believes that any attempt to address the "spam" problem must not violate the fundamental free speech right to be able to send and receive messages, regardless of medium. Non-spammers must not be harmed by overreaching anti-spam laws and policies. Because the statute at issue in this case is vague and overbroad, and because application of a claim for trespass to chattels to e-mail impinges on Free Speech rights, EFF files this brief in support of Defendants.

INTRODUCTION

Virginia's Computer Crimes Act purports to prohibit speech without defining what speech is prohibited. Although it seems unlikely that a legislature would seek to regulate an activity without telling anyone what that activity is, that is exactly what the legislature has done here.

A. The Statutory Scheme

In 1999, Virginia amended its Computer Crimes Act to include expansive provisions prohibiting the unauthorized transmission of unsolicited bulk e-mail, also known as "UBE." The amendments begin with the definition of what is unauthorized:

> A person is "without authority" when . . . (ii) he uses a computer, a computer network, or the computer services of an electronic mail service provider to transmit unsolicited bulk electronic mail in contravention of the authority granted by or in violation of the policies set by the electronic mail service provider.

Va. Code § 18.2-152.2. The statute, however, does not define "unsolicited" or "bulk," and it places

no limits on the policies that may be set by an electronic mail service provider and then enforced – as criminal prohibitions – by state law.

The statute prohibits various actions taken "without authority." "Theft of computer services," for example, occurs when "[a]ny person . . . willfully uses a computer or computer network, with intent to obtain computer services without authority." Va. Code § 18.2-152.6. "Computer fraud" occurs when "[a]ny person . . . uses a computer or computer network without authority and with the intent to: (1) obtain property or services by false pretenses; (2) embezzle or commit larceny; or (3) convert the property of another." *Id.* § 18.2-152.3. And "computer trespass" occurs when a person "use[s] a computer or computer network without authority and with the intent to. . . . [f]alsify or forge electronic mail transmission information or other routing information in any manner in connection with the transmission of unsolicited bulk electronic mail through or into the computer network of an electronic mail service provider or its subscribers." *Id*. § 18.2-152.4.

The penalties for violations of the Computer Crimes Act are severe. The actions for theft and fraud are punishable as Class 1 misdemeanors, and a violation of the trespass provision may be punishable as a felony. Va. Code §§ 18.2-152.3, 152.4, 152.6. Moreover, the Act provides for civil liability and substantial statutory damages. "If the injury arises from the transmission of unsolicited bulk electronic mail, an injured electronic mail service provider . . . may elect, in lieu of actual damages, to recover the greater of ten dollars for each and every unsolicited bulk electronic mail message transmitted in violation of this article, or $25,000 per day." Va. Code § 18.2-152.12(C). The statute also provides that "other injured persons" – which, presumably, includes the recipients of unsolicited bulk e-mails – may recover money damages. Va. Code § 18.2-152.12(B).

B. Possible Interpretations of the UBE Provisions of the Computer Crimes Act

One thing about the UBE amendments is beyond dispute: a sender of an e-mail will pay dearly for violating them. Unfortunately, nothing else about these provisions is clear. The Act does not specify what the term "unsolicited" means. Nor does it define the term "bulk." And it delegates the decision of which e-mail transmissions are unauthorized to e-mail service providers, each of which may not only choose what types of e-mails to exclude, but also write its policy in terms as specific or vague as it chooses. Accordingly, the UBE provisions cast their net over a wide range of e-mails, provide virtually no notice by their own terms of what e-mails are prohibited, and provide no assurance that the service provider's policy will provide meaningful notice.

There is no agreed-upon definition of "unsolicited" e-mail, either within the Internet community or under proposed federal legislation. "Unsolicited," for example, could describe any number of things. It could mean the sending of any e-mail that is not specifically requested, or it could mean only the sending of an e-mail to a person who has no prior relationship with the sender. Indeed, in the internet industry, there are several different approaches to the sending of group e-mails. There is the "opt-out" approach, whereby the recipient of an e-mail may ask not to receive any e-mails from the sender in the future. One statute considered by Congress proposes such a standard. See H.R. Rep. No. 106-700, at 3-4 (2000). Under the "opt-out" standard, an e-mail would be unsolicited only if the recipient had asked not to receive it, and that request had been ignored. There is the "opt-in" approach, whereby the recipient will receive e-mails only after asking to receive messages from the sender. That standard, which is advocated by the "Internet Mail Consortium" (see www.imc.org/ube-def.html), provides that an e-mail would be unsolicited if the recipient did not ask to receive e-mails from the sender. A variation of the opt-in approach, which is adopted in the

"Unsolicited Commercial Electronic Mail Act of 2001" (H.R. 95) and supported by the "Coalition Against Unsolicited Commercial Email" (see www.cauce.org/legislation/index.shtml), provides that e-mails may not be sent in the absence of a pre-existing business relationship between the sender and the recipient. Finally, there is the "double opt-in" approach, whereby the recipient will receive e-mails only after asking to receive messages from the sender, *and* sending an e-mail confirming his or her willingness to receive messages. The "Mail Abuse Prevention System" advocates such a standard. See www.mail-abuse.org/standard.html. Under this standard, an e-mail would be unsolicited if the recipient did not send an e-mail confirming the desire to receive e-mails from the sender.[1]

Equally unclear is the definition of "bulk." That term could describe only e-mails sent to thousands of people unknown to the transmitter. Or it could cover any e-mail "sent to a group of persons who have not requested it." Internet Mail Consortium Report: UBE-DEF IMCR-005 (Oct. 5, 1997), www.imc.org/ube-def.html. Under this definition, "bulk" e-mail includes an e-mail sent to an individual's entire personal e-mail list, an e-mail sent from one employee to all of the employees in his or her office, and an e-mail sent by one student to all of the other students in his or her school. Indeed, in the absence of a definition, there is nothing to preclude such extreme interpretations as treating any e-mail (other than a specifically requested e-mail) sent to two or more

[1] It could be argued that whether an e-mail is "unsolicited" depends on the attitude of the recipient. Suppose, for example, that a company sends an e-mail to ten people who visited its website, and, in doing so, proceeded past the homepage which states that "proceeding further constitutes the consent to receiving e-mail from our company." Two people object to the e-mail, and eight do not. Suppose also that the recipients' Internet service provider's policy adopts the "double opt-in" approach. Could the ISP's policy trump the recipients' consent to receiving e-mail? And, if it does, does it trump the consent only as to the recipients who objected to the company's e-mail, or as to all of the recipients?

recipients as "bulk" e-mail. An e-mail from counsel in a lawsuit to two or more opposing counsel proposing deposition dates could subject the sender to damages or criminal prosecution under the vague, expansive terms of Virginia's statute.

Moreover, because individual e-mail service providers are given the discretion to define what is unauthorized, there are additional potential limitations on the transmission of e-mails. Some providers prohibit the transmission of e-mails that are "vulgar" or "harm minors in any way." Both Yahoo! and God'sNetwork.net have implemented such policies. See http://docs.yahoo.com/info/terms; www.godsnetwork.net/policies/comm_standards.htm. Some, including the Federal Trade Commission, would limit the transmission of only commercial e-mails. *See Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2001: Hearing Before the Senate Committee on Commerce, Science and Transportation* (2001) (Statement of Eileen Harrington) (proposing limits on "unsolicited *commercial* e-mail") (emphasis added); see also H.R. Rep. No 106-700, at 3 (proposing limit on "commercial electronic mail message[s]"). And some policies, such as EarthLink's, prohibit all unsolicited bulk e-mails, whether commercial or noncommercial. See www.earthlink.net/about/policies/use (prohibiting the "us[e] the Services to transmit any unsolicited commercial e-mail or unsolicited bulk e-mail").

What is worse, the sender of an e-mail may have no way of making itself aware of the recipient's terms of service. Internet service providers may change their terms, without any notice to their members or to others. *See, e.g.*, http://docs.yahoo.com/infor/terms (terms of service "may be updated from time to time without notice to you"); www.eathlink.com/about/policies/use/ ("EarthLink reserves the right to revise, amend, or modify this AUP, our Internet Service Agreement and our other policies and agreements at any time and in any manner"). Accordingly, a sender may

know one day what is permitted by an ISP, and not know the next. Additionally, it is not always ascertainable what ISP is associated with an individual's e-mail account. Many individuals have accounts where their last name is the domain name, and that account is carried by whichever e-mail service provider they choose. It would be difficult, with regard to such accounts, to know which ISP's policy governs that person's receipt of e-mail.[2]

The policy at issue in this case is so broad that it gives no notice of what is prohibited. The policy itself states that AOL "does not authorize the use of its proprietary computers and computer network ('the AOL Network') to accept, transmit or distribute unsolicited bulk e-mail sent from the Internet to AOL members." No sender of e-mail would have the slightest idea what this policy prohibits just from reading it. In discovery, AOL has made its policy worse, not better, from a constitutional overbreadth and vagueness standpoint by stating that it has "its *broadest meaning*, and includes *any* meaning of the word as used in *any* 'anti-spam' statutes. . . or as used in *any other* lawfully enacted statutes, rules, regulations *or* common law standards that *might be applied* to bar or limit the transmission of UBE messages." AOL's Answers to Bennett's First Set of Interrogatories, No. 1 (Netvision Ex. 2) (emphasis added). Accordingly, applying the Mail Abuse Prevention System's definition of "unsolicited" and the Internet Mail Consortium's definition of "bulk," the AOL policy prohibits the sending of e-mail to any group of people who have not specifically requested e-mail from a particular source *and* sent the source a confirmation that they wish to receive e-mail from that source. The seemingly fanciful assertion that a lawyer could commit a crime by

---

[2] Another complicating issue is that many persons utilize "automatic" forwarding of their e-mails from one account (such as their account at work) to another (such as their account at home). If the employer's e-mail service provider is EarthLink, but the individual's home e-mail service provider is AOL, which policy applies?

using E-mail to propose deposition dates to two or more opposing counsel is, apparently, exactly what AOL intends.

These varying policies simply confirm that Virginia's computer crimes act could, and does, prohibit a wide variety of e-mail messages. Certainly, it encompasses a mass advertisement sent to thousands of potential customers, none of whom have had any previous contact with the sender. But it targets much more. It encompasses an e-mail by an individual to his friends circulating a petition to the United Nations protesting discrimination by the Taliban. It includes an e-mail requesting sponsorship from one's friends and colleagues for a charity run. It covers an e-mail from an on-line legal service advising recipients about how to vote, or about changes in the tax laws. It targets an e-mail from a financial magazine to visitors to its website providing information on the performance of mutual funds. It covers an e-mail to the guests of a wedding enclosing wedding pictures.

Because the UBE provisions therefore may be used to exclude constitutionally protected speech, it is overbroad in violation of the First Amendment. Moreover, because the language of the statute does not provide notice of which e-mail transmissions are prohibited, and instead delegates this decision to private companies, the statute is also unconstitutionally vague. Indeed, even if the statute targeted *only* commercial speech, it still would not be sufficiently tailored to survive constitutional scrutiny.

Free speech concerns also defeat plaintiff's claim for trespass to chattels. Although plaintiff's allegations may technically meet the elements of a trespass to chattels claim under Virginia common law, the First Amendment mandates that enforcement of this cause of action be limited to situations where a plaintiff can establish physical injury to a computer or computer system, or disruption of the operation of a computer or computer system.

ARGUMENT

I. VIRGINIA'S LAWS GOVERNING THE UNAUTHORIZED TRANSMISSION OF UNSOLICITED BULK E-MAIL VIOLATES THE FIRST AMENDMENT

A. Virginia's UBE Statute Is Unconstitutionally Vague[3]

As the Supreme Court has held, "[v]agueness may invalidate a [] law for either of two independent reasons. First, it may fail to provide the kind of notice that will enable ordinary people to understand what conduct it prohibits; second, it may authorize and even encourage arbitrary and discriminatory enforcement." *City of Chicago v. Morales*, 527 U.S. 41, 56 (1999) (holding that city's gang loitering ordinance was unconstitutionally vague). Virginia's statute is invalid for both of these reasons.

1. Virginia's UBE Provisions Do Not Give Notice of What Conduct is Prohibited

Virginia's legislature has purported to ban the transmission of unauthorized, unsolicited bulk e-mail, but the legislature has failed to explain what it means by "unsolicited" or "bulk," and has delegated to private parties the right to define "unauthorized." Given the numerous possible definitions of these terms, and the variation in policies of different e-mail service providers, the statute does not give reasonable notice of what conduct is prohibited.

In *City of Chicago v. Morales*, the U.S. Supreme Court held that an ordinance prohibiting street gang members from "loitering" in a public place was unconstitutionally vague. The Court began its analysis by noting that "'[i]t is established that a law fails to meet the requirements of the Due Process Clause if it is so vague and standardless that it leaves the public uncertain as to the

---

[3] EFF concurs with Netvision's argument that the statute is a content-based regulation and cannot survive strict scrutiny.

conduct it prohibits.'" 527 U.S. at 56 (quoting *Giaccio v. Pennsylvania,* 382 U.S. 399, 402-03 (1966)). Under the ordinance, "loitering" was defined as remaining in one place with no apparent purpose; the Court recognized that this definition did not put citizens on notice as to the difference between innocent and illegal conduct: "Since the city cannot conceivably have meant to criminalize each instance a citizen stands in public with a gang member, the vagueness that dooms this ordinance is not the product of uncertainty about the normal meaning of 'loitering,' but rather about what loitering is covered by the ordinance and what is not." 527 U.S. at 57. Similarly, here, it is inconceivable that Virginia meant to criminalize every transmission of any e-mail to a group of persons who had not requested it, yet the statute does not draw a sufficiently clear line between permissible and impermissible transmissions.

Hirschkop v. Snead, 594 F.2d 356 (4th Cir. 1979), also is instructive. There, the Fourth Circuit struck down part of a Virginia disciplinary rule limiting the statements an attorney could make to the press during a criminal trial. The rule purported to prohibit "a lawyer participating in a criminal trial from making any statements about 'other matters that are reasonably likely to interfere with a fair trial.'" *Id*. at 371. The court observed that "[t]his proscription is so imprecise that it can be a trap for the unwary." *Ibid.* Such is the case here – the limitation on any "bulk" e-mail that is "unsolicited" and against the policy of an e-mail service provider (which policies vary from provider to provider) is "so imprecise" that it constitutes an unconstitutional "trap." See also *Chatin v. Coombe,* 186 F.3d 82, 87 (2d Cir. 1999) (holding that statute regulating prison inmates' religious services and speeches did not give fair notice that solitary, demonstrative prayer was prohibited).

As described above, lack of fair notice is not a hypothetical problem in this case; it is a real,

concrete issue. E-mail service providers each have their own, different policy as to what types of transmissions are permitted; few, if any, of these policies define either "unsolicited" or "bulk." Moreover, some providers' policies are no clearer than the statute. AOL's policy, for example, simply prohibits "unsolicited bulk e-mail," and AOL takes the position that this policy has "its broadest meaning." AOL's Answers to Bennett's First Set of Interrogatories, No. 1 (Netvision Ex. 2). Accordingly, even resort to the individual policies of each e-mail service provider, in many cases, will not provide any more detailed notice as to what transmissions are prohibited.

The Virginia statute's failure to give reasonable notice as to what conduct is illegal is especially troublesome because of the statute's "obvious chilling effect on free speech." *Reno v. ACLU*, 521 U.S. 844, 872 (1997); see also *Bartnicki v. Vopper*, 531 U.S. 990, ____, 121 S. Ct. 1753, 1769 (2001) (Rehnquist, C.J., dissenting) (noting that it violates "the purposes of the First Amendment" to "chill[] the speech of the millions of Americans who rely upon electronic technology to communicate each day"). Because the statute could penalize a computer programmer for sending an e-mail to his college roommates just as easily as it could penalize a bank marketing a credit card to a mailing list it purchased, people may choose to "remain silent rather than communicate even arguably unlawful words, ideas, and images." *Reno v. ACLU*, 521 U.S. at 872. Such a result, of course, would run contrary to the very policies underlying the First Amendment. "[T]he growth of the Internet has been and continues to be phenomenal. As a matter of constitutional tradition, in the absence of evidence to the contrary, we presume that governmental regulation of the content of speech is more likely to interfere with the free exchange of ideas than to encourage it. The interest in encouraging freedom of expression in a democratic society outweighs any theoretical but unproven benefit of censorship." *Id.* at 885.

2. Virginia's UBE Statute Impermissibly Delegates to Private Parties the Right to Determine What Conduct Is Prohibited

By its very terms, the statute at issue delegates to private parties the discretion to determine what conduct is permissible and what conduct is penalized. The statute regulates only those e-mails sent "without authority" (see Va. Code §§ 18.2-152.3, 152.4, 152.6), and defines "without authority" as "in contravention of the authority granted by or in violation of the policies set by the electronic mail service provider" (*id*. § 18.2-152.2). By abdicating the responsibility to decide what e-mail transmissions fall within its scope, the statute is impermissibly vague.

Federal courts have not hesitated to invalidate statutes or regulations that delegate too much authority to a single decisionmaker – even a governmental rather than private decisionmaker. In *Kolender v. Lawson*, 461 U.S. 352 (1983), for example, the Supreme Court concluded that a California anti-vagrancy statute was unconstitutional. The statute in that case required persons who loitered or wandered on the streets to provide "credible and reliable" identification and to account for their presence when requested by a peace officer. *Id*. at 353. Rather than define what type of identification would satisfy the statute, the statute left such a determination to the individual police officer. *Id*. at 359. The Supreme Court held that such delegation was inappropriate: "It is clear that the full discretion accorded to the police to determine whether the suspect has provided a 'credible and reliable' identification necessarily entrusts lawmaking to the moment-to-moment judgment of the policeman on his beat." *Id*. at 360 (internal quotation omitted).

Similarly, in *Forsyth County v. Nationalist Movement*, 505 U.S. 123 (1992), the Supreme Court struck down an ordinance allowing a county administrator to set the fee for the issuance of permits. Reviewing the county's construction and implementation of the ordinance, the Court held that "it simply cannot be said that there are any narrowly drawn, reasonable and definite

standards . . . . Nothing in the law or its application prevents the official from encouraging some views and discouraging others through the arbitrary application of fees. The First Amendment prohibits the vesting of such unbridled discretion in a government official." *Id*. at 132-33 (internal quotation and footnote omitted). See also *Chatin*, 186 F.3d at 89 (striking down prison rule because prison employees had "unfettered discretion in interpreting what conduct is prohibited").

Of course, this doctrine applies with equal, if not greater, force when discretion is vested in private parties, rather than government officials. See, *e.g.*, *Eubank v. City of Richmond*, 226 U.S. 137, 143-44 (1912) (holding unconstitutional a Richmond ordinance giving discretion to private property owners to determine whether street line should be drawn); see also *Reno v. ACLU*, 521 U.S. at 880 (holding statute unconstitutional in part because it would "confer broad powers of censorship, in the form of a 'heckler's veto,' upon any opponent of indecent speech"); *Hill v. Colorado*, 530 U.S. 703, 735 n.43 (2000) (acknowledging "constitutionally problematic" nature of enactments that "allowed a single, private actor to unilaterally silence a speaker even as to willing listeners").

In sum, it cannot be disputed that the Virginia statute delegates to individual e-mail service providers the discretion to distinguish between permissible and impermissible e-mail transmissions. Moreover, because the Act provides no detail as to the policies of each e-mail service provider, and because it does not define "unsolicited" or "bulk" (each of which is susceptible to numerous interpretations), the Act does not give fair notice as to what conduct falls within its scope. Because the Act "fails to establish standards. . . that are sufficient to guard against the arbitrary deprivation of [free speech] interests" (*City of Chicago v. Morales*, 527 U.S. at 52), the statute is unconstitutionally vague.

B. The UBE Provisions of Virginia's Computer Crimes Act Are Overbroad

Whatever the Court may think of the speech of the particular defendants in this case, the First Amendment requires an analysis of *all* the speech prohibited or chilled by the statute, not just the speech in which these defendants allegedly engaged. "The 'overbreadth' doctrine, which is a departure from traditional rules of standing, permits a defendant to make a facial challenge to an overly broad statute restricting speech, even if he himself has engaged in speech that could be regulated under a more narrowly drawn statute." *Alexander v. United States*, 509 U.S. 544, 555 (1993). "The use of overbreadth analysis reflects the conclusion that the possible harm to society from allowing unprotected speech to go unpunished is outweighed by the possibility that protected speech will be muted." *Bates v. State Bar*, 433 U.S. 350, 380 (1977). See generally *Broadrick v. Oklahoma*, 413 U.S. 601 (1973); *Secretary of State v. Joseph H. Munson Co.*, 467 U.S. 947 (1984). "'Freedoms of expression require '"breathing space."'" *Hustler Magazine, Inc. v. Falwell*, 485 U.S. 46, 52 (1988) (Rehnquist, C.J.) (quoting *Philadelphia Newspapers, Inc. v. Hepps*, 475 U.S. 767, 772 (1986) (quoting *New York Times v. Sullivan*, 376 U.S. at 272)).

It goes without saying that certain transmissions that could be characterized as "unsolicited bulk e-mails" may properly be regulated by Virginia's legislature. For example, no individual has a right to send an e-mail soliciting investments in "oceanfront" property in Kansas. Nor does anyone have the unfettered right to transmit obscene materials. But the statute's UBE provisions reach far more than fraudulent commercial or obscene speech and, accordingly, are overbroad.

"[T]he overbreadth doctrine permits the facial invalidation of laws that inhibit the exercise if First Amendment rights if the impermissible applications of the law are substantial when judged in relation to the statute's plainly legitimate sweep." *City of Chicago v. Morales*, 527 U.S. at 52.

In other words, if a statute "sweeps too broadly, penalizing a substantial amount of speech that is constitutionally protected" (*Forsyth County*, 505 U.S. at 130), it is unconstitutional.

Here, there is no doubt that the statute's UBE provisions "sweep[] too broadly." For example, both God'sNetwork & Yahoo! prohibit the transmission of e-mails that are "vulgar" or "harm minors in any way." Certain transmissions that are "vulgar" are nonetheless protected speech: "[s]exual expression which is indecent but not obscene is protected by the First Amendment." *Reno v. ACLU*, 521 U.S. at 874 (internal quotation omitted). And, although there is a governmental interest in protecting children from harmful materials, "that interest does not justify an unnecessarily broad suppression of speech addressed to adults." *Id*. at 874. Even if it could be argued that Virginia's statute (despite its seeming purpose to "protect" adults as well as children) simply imposes a duty on the senders of e-mail to ensure that minors do not receive "harmful" e-mails, the Supreme Court has rejected exactly that argument. In holding that the "Communications Decency Act" ("CDA") violated the First Amendment, the Court noted that "[g]iven the size of the potential audience for most messages, in the absence of a viable age verification process, the sender must be charged with knowing that one or minors will likely view it. Knowledge that, for instance, one or more members of a 100-person chat group will be a minor – and therefore that it will be a crime to send the group an indecent message – would surely burden communication among adults." *Id.* at 876. See also *Mainstream Loudon v. Board of Trustees*, 2 F. Supp. 2d 783, 796-97 (E.D. Va. 1998) (in denying motion to dismiss, holding that public library policy implementing software to block child pornography, obscene material, and material harmful to juveniles could violate First Amendment).

Of course, those policies that purport to exclude *any* unsolicited group e-mail prohibit even

more protected speech. AOL's policy provides an example, as does EarthLink's, which explicitly applies to both commercial and non-commercial e-mails. That policy would ban a petition forwarded from personal address list to personal address list seeking to voice opposition to proposed legislation. It would prohibit a tax preparer from sending a newsletter about changes in the tax laws to persons who had visited its site. "The line between speech unconditionally guaranteed and speech which may legitimately be regulated, suppressed, or punished is finely drawn. Error in marking that line exacts an extraordinary cost." *United States v. Playboy Entertainment Group, Inc.*, 529 U.S. 803, 817 (2000) (provision of Telecommunications Act requiring cable operators to scramble or block sexually explicit channels violated First Amendment) (internal quotation and citation omitted). Here, neither the Virginia legislature nor AOL has "finely drawn" a line between unconditionally guaranteed and legitimately regulated speech; instead, they have blacked out both with a wide brush.

Even if AOL's confessed effort to pursue the "broadest" possible ban on speech were ignored, no limiting construction could save the Virginia statute or the AOL policy that it enforces from unconstitutional overbreadth. "[T]he challenged [statute and policy are] not 'open to one or a few interpretations, but to an indefinite number,' and . . . '[i]t is fictional to believe that anything less than extensive adjudications, under the impact of a variety of factual situations, would bring the [statute or policy] within the bounds of permissible constitutional certainty.' . . . [I]t is difficult to imagine that the [statute or policy] could be limited by anything less than a series of adjudications, and the chilling effect of the resolution on protected speech in the meantime would make such a case-by-case adjudication intolerable." *Board of Airport Commissioners v. Jews for Jesus, Inc.*, 482 U.S. 569, 575-576 (1998) (quoting *Baggett v. Bullitt*, 377 U.S. 360, 378 (1964)). The UBE

provisions of the Computer Crimes Act are therefore unconstitutionally overbroad.[4]

C. Even if the UBE Provisions Governed Only Commercial Speech, They Nonetheless Would Violate the First Amendment

AOL has taken the position that the UBE Provisions of the Computer Crimes Act reach only commercial speech. See AOL Reply Brief in Support of TRO at 21. As explained above, this a gross understatement of the statute's scope, and especially disingenuous in light of AOL's own explanation, in discovery, of its own policy. Nonetheless, even if AOL were correct, the statute would still be unconstitutional. For one, it would still be unconstitutionally vague. For another, it is not a sufficiently tailored regulation of even purely commercial speech.

Pure commercial speech is not subject to unlimited regulation. To the contrary, any regulation must serve a "substantial" governmental interest. *Bolger v. Youngs Drug Products, Inc.*, 463 U.S. 60, 68 (1983). Additionally, the statute must "directly advance the government interest asserted" and most do so in a manner that "is not more extensive than necessary to serve that interest." *Id*. at 69. We will assume, only for purposes of argument, that AOL will articulate a significantly substantial governmental interest for the computer theft provision, Va. Code § 18.2-152.6. See AOL Reply at 22 ("The Virginia Computer Crimes Act protects Virginia ISPs and their

---

[4] The statute's computer trespass provision, which prohibits a person from "us[ing] a computer or computer network without authority and with the intent to. . . . [f]alsify or forge electronic mail transmission information or other routing information in any manner in connection with the transmission of unsolicited bulk electronic mail through or into the computer network of an electronic mail service provider or its subscribers" (Va. Code § 18.2-152.4) is overbroad for yet another reason. Although Virginia may have intended to prohibit only fraudulent transmissions or commercial misappropriations, the statute's plain language prohibits the sending of any anonymous or pseudonymous e-mail, including those where the sender has chosen to hide its identity "to avoid social ostracism, to prevent discrimination and harassment, and to protect privacy." *ACLU of Georgia v. Miller*, 977 F. Supp. 1228, 1233 (N.D. Ga. 1997). For these reasons, a federal court has ruled that a Georgia statute similar to the statute at issue here is unconstitutionally overbroad. *Ibid*.

customers from the high costs of spam"). We will also assume, only for purposes of argument, that the computer fraud provision, which prohibits the conversion of another's property (see Va. Code § 18.2-152.3), is also designed to prevent e-mail service providers from incurring the costs of increased traffic on their servers. And we will assume that the computer trespass provisions (Va. Code § 18.2-152.4) is intended to prevent consumers from being deceived as to the identity of a seller of goods and services.[5] Nonetheless, these provisions do not "direct[ly] advance" this interest in a manner that "is not more extensive than necessary."

In *Bolger*, the Supreme Court held unconstitutional a federal statute prohibiting any matter advertising contraception from being carried by the U.S. mail. The government asserted that the statute was necessary to shield recipients of mail from materials that they are likely to find offensive. 463 U.S. at 71. The Court, however, held that this rationale did not justify a prohibition on such mailings: "Recipients of objectionable mailings, however, may effectively avoid further bombardment of their sensibilities simply by averting their eyes. Consequently, *the short, though regular journey from mail box to trash can is an acceptable burden, at least so far as the Constitution is concerned*." *Id*. at 71 (emphasis added, internal quotations and citations omitted). And, although the Court recognized the substantial nature of the state's desire to aid parents in controlling the manner in which their children learn about birth control, it observed that, "as a *means* of effectuating this interest, . . . [the statute] fails to withstand scrutiny." *Id*. at 73 (emphasis in

---

[5] EFF does not concede that these interests are substantial, or even legitimate. Moreover, as described in more detail in Netvision's memorandum in support of summary judgment, Virginia's Computer Crime Act covers the transmission of e-mails to non-Virginia residents, and the transmission of e-mails by electronic mail service providers that are not based in Virginia. See Netvision Memo. at 10-20. Virginia has no apparent interest in regulating these transmissions. Netvision's Commerce Clause objections to the statute appear to have merit, though EFF is not briefing those issues.

original). Specifically, the Court concluded that the statute provided "only the most limited incremental support for the interest asserted" (*ibid.*), and therefore that "the justifications offered by the Government are insufficient to warrant the sweeping prohibition" of the statute. *Id*. at 75.

Such is the case here. It may well be that the Commonwealth has an interest in preventing its citizens from receiving unwanted e-mail. But unless that statute's crucial terms – including "without authority" – have a definite meaning, the statute, by its own terms, cannot be narrowly tailored. It simply is not tailored at all. To the extent Virginia is trying to reduce the costs to e-mail service providers of handling mass e-mails sent to thousands of recipients, the statute is simply too broad. Because its "sweeping prohibition" encompasses e-mails sent to an individual user's personal e-mail list as well as a e-mail sent out by a commercial venture to thousands of potential customers, the statute is "more extensive than necessary."

Indeed, Virginia's statute is far broader than other statutes or proposals governing commercial e-mails. Colorado's legislation, for example, requires that e-mails contain a label ("ADV") in the subject line of a commercial e-mail, and that the e-mail include the sender's e-mail address and an opt out provision. Colo. Rev. St. § 6-2.5-103 (2000). One of the statutes considered by Congress required that the e-mail contain a return address, accurate routing information, and an opt-out provision. See H.R. Rep. No. 106-700, at 3-4. And Pennsylvania's statute requires commercial e-mails containing "explicit sexual materials" to contain a label ("ADV-ADULT") at the beginning of the subject line. 18 Pa. Cons. Stat. Ann. § 5903. Although EFF does not endorse any of these specific approaches or limitations, they do highlight just how overly broad Virginia's legislation is. Virginia did not even attempt to tailor its legislation to achieve its goals, and instead has promulgated an expansive statute banning substantial amounts of speech that cannot be regulated. "The provision

before us does not reveal the caution and care that the standards underlying these various verbal formulas impose upon laws that seek to reconcile the critically important interest in protecting free speech with very important, or even compelling, interests that sometimes warrant restrictions." *Denver Area Educational Telecommunications Consortium, Inc. v. FCC,* 518 U.S. 727, 756 (1996). Accordingly, the statute cannot survive a constitutional challenge, even under "intermediate scrutiny" or the standards applied to commercial speech.

II. A CAUSE OF ACTION FOR TRESPASS TO CHATTELS BASED ON THE TRANSMISSION OF E-MAILS VIOLATES THE FIRST AMENDMENT

AOL has asserted a cause of action for "trespass to chattels" based on Defendants' transmissions of unsolicited bulk e-mails. According to AOL, Defendants have made use of AOL's computers and computer network to transmit these messages, thereby causing AOL to incur the increased costs of maintaining its computers as well as loss of customers and loss of goodwill. Second Amended Complaint ¶¶ 149, 151. This is not the first time AOL has invoked the tort of trespass to chattels in a challenge to the transmission of bulk e-mails, and, indeed, this court has previously concluded that such conduct may constitute a trespass to chattels under Virginia common law. See *America Online, Inc. v. LCGM, Inc.*, 46 F. Supp. 2d 444, 451-52 (E.D. Va. 1998); *America Online, Inc. v. IMS,* 24 F. Supp. 2d 548, 550-551 (E.D. Va. 1998). Neither of these decisions, however, addressed the First Amendment implications of the application of this tort to e-mail.[6] As we explain below, because e-mails communicate protected speech, application of common law tort

[6] Judge Lee's opinion in *LCGM,* moreover, noted that the defendant in that case was precluded, as a result of a prior discovery sanction imposed by Judge Poretz, from raising any claim or defense not asserted before August 14, 1998. Because of its peculiar posture, the *LCGM* decision should not serve as a precedent foreclosing or even limiting full consideration of Netvision's defenses on the merits.

doctrine to their transmission must be tailored to protect First Amendment rights.

A. Judicial Enforcement of an Action for Trespass to Chattels Constitutes State Action

As Netvision explains in its memorandum, judicial enforcement of a common law tort in a manner infringing First Amendment rights constitutes state action. See Netvision Memo. at 35-37. Of course, in *New York Times v. Sullivan*, 376 U.S. 254 (1964), the Supreme Court held that judicial enforcement of state tort law constituted state action: "[t]he test is not the form in which the state power has been applied, but, whatever the form, whether such power has in fact been exercised." *Id*. at 265. See also *NAACP v. Claiborne Hardware Co.*, 458 U.S. 886, 916 n. 51 (1982) ("Although this is a civil lawsuit between private parties, the application of state rules of law by the Mississippi state courts in a manner alleged to restrict First Amendment freedoms constitutes 'state action' . . . ."). Recently, the Supreme Court held that a private cause of action for promissory estoppel involves state action:

> The rationale of our decision in *New York Times v. Sullivan* . . . and subsequent cases compels the conclusion that there is state action here. Our cases teach that the application of state rules of law in state courts in a manner alleged to restrict First Amendment freedoms constitutes "state action" under the Fourteenth Amendment.

Cohen v. Cowles Media Co., 501 U.S. 663, 668 (1991). Likewise, the First Amendment was applied, in an action by a private plaintiff against a private defendant, to limit Virginia's common law tort of intentional infliction of emotional distress in *Hustler Magazine Inc. v. Falwell*, 485 U.S. 46 (1988); see *id*. at 50 n.3 (noting elements of an action for intentional infliction of emotional distress under Virginia law).

In still more recent decisions involving private plaintiffs' invocation of judicial authority to try to stop, or to recover damages for, speech by private defendants – including cases in which the

Court held that the party asserting First Amendment freedoms must prevail – the Supreme Court has thought the presence of state action so clear as to require no discussion. *E.g., Bartnicki v. Vopper*, 531 U.S. 990 (2001); *Hurley v. Irish-American Gay, Lesbian & Bisexual Group*, 515 U.S. 557 (1995). And the Court continues to find state action in cases in which no allegedly unconstitutional statute is involved and the only relevant state actor is the judiciary. *E.g., Georgia v. McCollum*, 505 U.S. 42 (1992); *Masson v. New Yorker Magazine, Inc.*, 501 U.S. 496 (1991); *Edmonson v. Leesville Concrete, Inc.*, 500 U.S. 614 (1991); *Milkovich v. Lorain Journal Co.*, 497 U.S. 1 (1990). By the same logic, application of the tort of trespass to chattels in a manner alleged to restrict the right of free speech obviously constitutes state action.

B. Application of the Tort of Trespass to Chattels to the Transmission of E-mails Should Be Limited to Protect First Amendment Rights

It is beyond dispute that the exchange of information over the internet is speech. *See, e.g.*. *ACLU v. Reno*, 521 U.S. at 850-52; *id.* at 882 ("The CDA, casting a far darker shadow over free speech, threatens to torch a large segment of the Internet community."); *Cyberspace Communications, Inc. v. Engler*, 55 F. Supp. 2d 737, 742 (E.D. Mich. 1999) ("Once an individual signs on to the Internet, there are a wide variety of methods for communicating and exchanging information with other users."), *aff'd* 228 F.3d 420 (6th Cir. 2000).

When common law tort liability is based on what is otherwise constitutionally protected free speech, the law may not be enforced without reference to First Amendment principles. In *New York Times v. Sullivan*, for example, the Court held that the First Amendment limits the power of state courts to award damages in a libel action, and requires that a plaintiff prove "actual malice." 376 U.S. at 279-80. Similarly, in *NAACP v. Claiborne Hardware*, merchants filed a state law tort action for malicious interference with business. The Court held that the state could *not* award damages "for

the consequences of nonviolent, protected activity" (458 U.S. at 918), but instead could enjoin only the "*direct consequences*" of violent conduct. *Ibid* (emphasis added, citation omitted). And in *Hustler Magazine v. Falwell*, 485 U.S. at 56, the Supreme Court held that the right to free speech prohibited a public figure from recovering damages for intentional infliction of emotional distress based on a parody published in a magazine, unless the plaintiff could point to a false statement of material fact made with actual malice.

This case presents the same issue. Despite the oddity of treating as "trespass" the use of computer facilities of a company that opens its facilities to millions of members of the public, we assume for the sake of argument that Defendants' conduct could be deemed to satisfy each of the element of common law trespass to chattels. But the defendant's conduct in *New York Times v. Sullivan* met the common law test for defamation, just as the defendant's conduct in *NAACP v. Claiborne Hardware* constituted malicious interference with business, and just as the defendant's conduct in *Hustler v. Falwell* was alleged to constitute intentional interference with emotional distress. The lesson of those cases is that, when *speech* could be construed as giving rise to tort liability, then tort liability must be limited in a manner so as not to interfere unduly with free speech.

With regard to a cause of action for trespass to chattels based on the transmission of e-mail, a workable rule is that an action will lie only if the transmission resulted in physical damage or physical disruption, even if only temporary, to an e-mail system. Additionally, liability should lie only if damages are substantial. This rule has several benefits. For one thing, it does not allow liability to attach if the only injuries are harm to goodwill (in the form of customer complaints) or loss of customers: these injuries most likely result from an objection to the *content* of the message, rather than the *quantity* of e-mails sent. Moreover, it limits liability to those situations in which a

plaintiff can show a concrete, objective harm based on the quantity of the e-mails transmitted, rather than permitting an e-mail service provider to choose to object, citing marginal increased costs, if it does not like the sender or its message. This rule would therefore ensure that a defendant is not held liable merely because someone disagrees with its point of view, and instead holds a defendant responsible only when the volume of its transmission causes damage.

As applied to this case, then, AOL could recover for trespass to chattels only if it can show that Defendants' conduct caused physical damage or disruption. As AOL has alleged only loss of customer goodwill and increased costs, it could not recover on this cause of action.

CONCLUSION

Virginia's effort to regulate the transmission of unsolicited bulk e-mails, and AOL's effort to halt such e-mails sent to its users, penalize constitutionally protected speech in a manner that is not permitted by the First Amendment. Accordingly, Virginia's Computer Crimes Statute, insofar

as it purports to regulate unsolicited bulk electronic mail transmissions, should be declared unconstitutional. Additionally, AOL's cause of action for trespass to chattels should be dismissed.

Dated: October 5, 2001

Respectfully submitted,

_____

John L. Carter (Va. Bar No. _____)
Carter, Fullerton & Hayes
120 South Fairfax St., Ste. 400
Alexandria, VA 22314

Roy T. Englert, Jr.
Kathryn Schaefer Zecca
Robbins, Russell, Englert, Orseck & Untereiner
1801 K St., NW, Suite 411
Washington, DC 20006

Cindy Cohn
Lee Tien
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110