

COURT OF APPEALS OF VIRGINIA

Present: Judge Haley, Senior Judges Bumgardner and Fitzpatrick\*  
Argued at Alexandria, Virginia

JEREMY JAYNES

v. Record No. 1054-05-4

COMMONWEALTH OF VIRGINIA

OPINION BY  
JUDGE JAMES W. HALEY, JR.  
SEPTEMBER 5, 2006

FROM THE CIRCUIT COURT OF LOUDOUN COUNTY  
Thomas D. Horne, Judge

Thomas M. Wolf (John H. Craddock, Jr.; Joseph M. Rainsbury;  
David A. Oblon; LeClair Ryan PC; Albo & Oblon L.L.P., on briefs),  
for appellant.

William E. Thro, State Solicitor General (Judith Williams Jagdmann,  
Attorney General; Eric A. Gregory, Associate State Solicitor  
General; Courtney M. Malveaux, Associate State Solicitor General;  
D. Mathias Roussy, Associate State Solicitor General; William R.  
Sievers, Associate State Solicitor General; Richard B. Campbell,  
Deputy Attorney General; Lisa M. Hicks-Thomas, Senior Assistant  
Attorney General; Samuel E. Fishel, IV, Assistant Attorney  
General, on brief), for appellee.

*Amicus Curiae*: The Rutherford Institute (John W. Whitehead; L.  
Ilaine Upton, on brief), for appellant.

*Amicus Curiae*: American Civil Liberties Union of Virginia, Inc.  
(Rebecca K. Glenberg, on brief), for appellant.

*Amicus Curiae*: United States Internet Service Provider  
Association (Jennifer C. Archie; Richard P. Bress; Courtney S.  
Schorr; Alexander Maltas; Latham & Watkins, on brief), for  
appellee.

---

\* Judge Fitzpatrick participated in the hearing and decision of this case prior to the effective date of her retirement on March 31, 2006, and thereafter by designation pursuant to Code § 17.1-400(D).

Jeremy Jaynes (appellant) appeals his conviction by jury of three counts of violating Code § 18.2-152.3:1, the unsolicited bulk electronic mail provisions of the Virginia Computer Crimes Act (“VCCA”). He maintains that (1) the trial court lacked subject matter jurisdiction over this case; (2) the statute violates the First Amendment; (3) the statute violates the Dormant Commerce Clause; and (4) the statute is unconstitutionally vague. We find no merit to these claims and affirm.

I.

THE STATUTE AND PROCEDURAL BACKGROUND

The VCCA, Code §§ 18.2-152.1 to 18.2-152.13, notably, is part of Chapter 5 of the Virginia Criminal Code, entitled “Crimes Against Property.”

The sections of the VCCA here relevant read as follows:

§ 18.2-152.3:1.

A. Any person who:

1. Uses a computer or computer network with the intent to falsify 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 of its subscribers;

\* \* \* \* \*

B. A person is guilty of a Class 6 felony if he commits a violation of subsection A and:

1. The volume of UBE transmitted exceeded 10,000 attempted recipients in any 24-hour period, 100,000 attempted recipients in any 30-day time period, or one million attempted recipients in any one-year time period . . . .

In a motion to dismiss before the trial; in a motion to strike after the prosecution rested; and in a renewed motion to strike after appellant rested his case, appellant objected that the court lacked jurisdiction and that the law was unconstitutional under the First Amendment; was

unconstitutionally vague; and violates the Dormant Commerce Clause of the Constitution. The trial court denied each motion.<sup>1</sup> Following conviction and in accordance with the decision of the jury, the trial court sentenced appellant to nine years in prison. This appeal followed.

## II.

### THE OPERATION OF ELECTRONIC-MAIL

The sending of e-mail is governed by Simple Mail Transfer Protocol (“SMTP”), a set of standards to facilitate the transfer of e-mail. SMTP specifies that a computer sending an e-mail must contain information identifying the sender, generally referred to as “hello domain” information, as well as certain recipient information. The hello domain, in turn, contains the internet protocol (“IP”) address and domain name of the sending party. IP addresses are unique strings of numbers; each computer accessing the Internet is generally assigned one. For convenience and efficiency, IP addresses of many computers are given textual equivalents known as “domain names.” For example, a search known as a “whois” search reveals that the domain name “www.aol.com” is owned by America Online, Inc. (“AOL”), which is located in Dulles, Virginia. Additional contact information is provided as well. The IP addresses of four servers associated with aol.com are also available because “www.aol.com” is the domain name associated with those IP numbers.

When e-mail is sent, the hello domain and sender information exist as part of the transmission information of the e-mail. E-mail servers and routers starting with the sender’s Internet Service Provider (“ISP”)<sup>2</sup> relay the message forward until it reaches the e-mail servers of the recipient’s ISP, which then direct the e-mail to the intended recipient. These server

---

<sup>1</sup> While appellant presented other challenges at trial as to proof of venue and the sufficiency of the evidence, those issues are not before this Court.

<sup>2</sup> Internet users can obtain e-mail service from a different entity than their ISP. For simplicity here, however, we use the term ISP to refer to e-mail service providers as well.

interactions include the presentation of the sending e-mail's hello domain. Essentially, the sending computer identifies itself and presents the hello domain of the e-mail.

Each time the message passes through a different server, a record of that transaction is added to the routing information. Thus, using the e-mail's routing information, one can retrace the exact servers it went through to reach its destination, as if each post office or mail sorting facility added its own postmark to a letter. Furthermore, a server along this chain could choose to block the message from going further. The sender, however, has no way to control or predict the pathway his message will take to arrive at its destination. In fact, the message can be broken up and sent in pieces through multiple unique pathways. Despite this inherent unpredictability, the last server through which the message passes before reaching the recipient is his ISP's server, in this case, AOL's e-mail servers.

One major complaint of e-mail users is the volume of unsolicited bulk e-mail (often called "spam") they receive on a daily basis. To increase subscriber satisfaction and to protect their networks from computer viruses and other problems, ISPs employ a number of tactics to block spam from reaching users. One major tactic is to identify domain names or IP addresses that have sent unwanted e-mail in the past and to automatically prevent the delivery of any messages coming from those senders. Another related tactic is to identify senders of large numbers of messages to verify their legitimacy. Thus, an ISP can learn which companies sending high volumes of e-mail are potentially fraudulent or unwanted.

People sending spam ("spammers"), then, respond by masking their true identities to evade the protective measures. They create false routing information or transmission information, making messages appear as if they come from hundreds or thousands of different domain names and IP addresses. Thus, spammers can ensure that the ISP cannot detect and

block every e-mail they send and can evade detection because the thousands of messages appear to come from hundreds of different sources.

### III.

#### FACTS

The facts in this case are generally undisputed.

Appellant used computers in his home in North Carolina to send over ten thousand e-mails, on each of three different days, to subscribers of AOL, an ISP that provides e-mail accounts as part of its service. That AOL's servers are located in Loudoun County, Virginia, is not challenged.

On July 16, 2003, appellant sent 12,197 pieces of unsolicited bulk e-mail with falsified routing and transmission information onto AOL's proprietary network. On July 19, he sent another 24,172 similarly falsified e-mails, and he followed on July 26 with an additional 19,104. Each message targeted an AOL subscriber. That the sender knew each proposed recipient was an AOL subscriber was clear because the e-mail addresses of all recipients ended in "@aol.com." The messages advertised one of three products: either a FedEx claims product, a stock picker, or a "history eraser." To purchase one of these products, potential buyers would "click" on a hyperlink within the e-mail which redirected them to a website. Notably, this redirection led to thousands of different websites, rather than a single one, to consummate the purchase.

Among those items seized during a search of appellant's home were compact discs (CDs) containing both user names and full e-mail addresses.<sup>3</sup> The CDs contained at least 176 million full e-mail addresses and over 1.3 billion user names. Appellant also possessed a DVD

---

<sup>3</sup> The user name is generally that portion of an e-mail address appearing before the "@" symbol.

containing not only AOL e-mail addresses, but also other personal and private account information for millions of AOL users. Finally, police collected multiple “zip discs” (another type of data storage device) containing 107 million AOL e-mail addresses. All of the AOL user names, e-mail addresses, and account information were stolen and illegally in appellant’s possession.

In this case, appellant employed exactly those spammer tactics outlined in Part II, *supra*, of this opinion. He used thousands of different IP addresses and hello domains to send tens of thousands of e-mails and avoid detection by AOL’s network. Each e-mail advertised a commercial product; none contained any content that was personal, political, religious, or otherwise non-commercial. To aid his deception, appellant registered numerous different domain names using false contact information through Network Solutions, whose offices are located in Virginia. The contracts between appellant and Network Solutions require that appellant provide accurate contact information, update contact information when it changes, and submit to jurisdiction in Virginia for resolution of any contract disputes between appellant and Network Solutions.

#### IV.

#### JURISDICTION

Appellant contends that the trial court lacked jurisdiction because he could not control the pathways his messages took. Numerous servers and routers handled his messages before arriving at the recipient’s mailbox. Since any one of these intervening servers could have blocked his e-mails or since he could not specify which servers his messages went through, appellant argues, charging him with a crime in the jurisdiction of one of those servers is inappropriate. We disagree.

Circuit courts in Virginia have exclusive original jurisdiction over all felony indictments “for offenses committed within their respective circuits.” Code § 19.2-239; see also Code § 17.1-513. The Supreme Court of Virginia has said “a person may be charged in the place where the evil results, though he is beyond the jurisdiction when he starts the train of events of which the evil is the fruit.” Travelers Health Ass’n v. Commonwealth, 188 Va. 877, 892, 51 S.E.2d 263, 269 (1949), aff’d, 339 U.S. 643 (1950). Furthermore, “[j]urisdiction may exist where the immediate harm occurs, even if the criminal act does not physically occur there.” Foster-Zahid v. Commonwealth, 23 Va. App. 430, 441, 477 S.E.2d 759, 764 (1996).

In Travelers Health, the Virginia State Corporation Commission ordered the defendant to stop its solicitations of business by mail until it complied with the Blue Sky Law. The Court held that selling securities by mail in the Commonwealth while not in compliance with the statute was sufficient to give the corporation commission jurisdiction. 188 Va. at 892, 51 S.E.2d at 269. Thus, criminal jurisdiction could lie in the state where the mail was received. Similarly, here, criminal jurisdiction may lie where AOL’s servers are located because it is the trespass upon those servers that constitutes the offense.

We also find that appellant’s actions in sending the e-mails to AOL subscribers are sufficiently direct that Moreno v. Baskerville, 249 Va. 16, 452 S.E.2d 653 (1995), on which appellant relies, does not apply. In Moreno, the defendant sold drugs in Arizona knowing that the buyer intended to take them to Virginia for resale but was not himself involved in that resale. In ruling that the trial court lacked jurisdiction, the Supreme Court noted that the buyer could have chosen to resell the drugs in another state besides Virginia and that the defendant would have had no control over that decision. Id. at 19, 452 S.E.2d at 655. Thus, the actions of the buyer served to intervene and end any criminal liability Moreno might have had for the distribution of the drugs in Virginia.

Appellant argues this situation is akin to Moreno because intervening acts of the servers and routers were what caused the e-mails to pass through Virginia. That is, the arrival of the e-mails at AOL's servers in Loudoun County was the result of any number of computer processes, over which appellant had no control, similar to the lack of control Moreno had over the drugs once he sold them in Arizona. We find no merit to this comparison.

All e-mails in question in this case were addressed to AOL users, meaning that to arrive at the destination intended by appellant, the messages *necessarily* had to pass through AOL's e-mail servers, all of which are in the jurisdiction of the trial court. As one federal court noted, "e-mail transmitted to an ISP subscriber is processed and stored on the ISP's e-mail computer servers. The e-mail server is located in a discrete geographic location." Verizon Online Servs., Inc. v. Ralsky, 203 F. Supp. 2d 601, 606 (E.D. Va. 2002). And, "once the e-mail is transmitted, it must first pass through the ISP's computer server to reach its ultimate destination - the subscriber's computer." Id. Thus, while the e-mails could have taken any number of pathways to reach the intended recipients, each pathway ended at AOL's servers.

Furthermore, the mere fact that delivery could have failed is insufficient to eliminate liability when delivery did not fail. Analogously, a person can be charged with a criminal act committed by mail even though a number of people might handle that mail during the course of its delivery. An appellant cannot claim that a court lacks jurisdiction simply because any number of intervening actions could have disrupted the criminal enterprise, but did not.

In Moreno, the buyer could have taken the drugs from the seller in Arizona, and sold the drugs anywhere, without input from or change in position by the defendant seller. Here, appellant's e-mail solicitations would have been successful only if his messages arrived at their intended destinations, which required that they pass through AOL's servers in Virginia.



Finally, we note that, with respect to intent, appellant cannot challenge that he purposely intended his e-mails to pass through AOL's servers because the address of every intended recipient in this case ends in "@aol.com." Necessarily, if the e-mail is transmitted to the intended recipient, it must pass through AOL's servers.

Accordingly, we hold that the circuit court of Loudoun County, Virginia, properly had criminal jurisdiction to try appellant.

## V.

### THE FIRST AMENDMENT

Appellant argues that the trial court erred in ruling that the VCCA does not violate the First Amendment. Specifically, he contends that the law is overbroad because its language prohibits anonymous speech of a non-commercial nature and that the First Amendment protects such speech. We hold that the law does not violate the First Amendment and affirm the trial court's ruling on this point.

## A.

### Standard of Review

We review arguments regarding the constitutionality of a statute *de novo*. Shivae v. Commonwealth, 270 Va. 112, 119, 613 S.E.2d 570, 574 (citing Wilby v. Gostel, 265 Va. 437, 440, 578 S.E.2d 796, 798 (2003); Eure v. Norfolk Shipbuilding & Drydock Corp., 263 Va. 624, 631, 561 S.E.2d 663, 667 (2002)), cert. denied, 126 S. Ct. 626 (2005). Furthermore,

We are guided by the established principle that all acts of the General Assembly are presumed to be constitutional. In applying this principle, we are required to resolve any reasonable doubt regarding the constitutionality of a statute in favor of its validity. . . . [W]e will declare a statute null and void only when it is plainly repugnant to a state or federal constitutional provision.

In re Phillips, 265 Va. 81, 85-86, 574 S.E.2d 270, 272 (2003) (internal citations omitted).

Appellant seeks to challenge the validity of the VCCA on its face. In normal contexts, one may challenge the constitutionality of a statute only as applied to him. See, e.g., County Court of Ulster County v. Allen, 442 U.S. 140, 154-55 (1979). However, facial challenges are sometimes allowed when an appellant claims First Amendment protections.

As the Supreme Court recently said, “The First Amendment doctrine of overbreadth is an exception to our normal rule regarding the standards for facial challenges.” Virginia v. Hicks, 539 U.S. 113, 118 (2003).

The Supreme Court in Hicks described the overbreadth doctrine in depth.

The showing that a law punishes a “substantial” amount of protected free speech, “judged in relation to the statute’s plainly legitimate sweep,” Broadrick v. Oklahoma, 413 U.S. 601, 615 (1973), suffices to invalidate *all* enforcement of that law . . . .

[The Supreme Court has] provided this expansive remedy out of concern that the threat of enforcement of an overbroad law may deter or “chill” constitutionally protected speech—especially when the overbroad statute imposes criminal sanctions. . . .

[H]owever, there comes a point at which the chilling effect of an overbroad law, significant though it may be, cannot justify prohibiting all enforcement of that law—particularly a law that reflects “legitimate state interests in maintaining comprehensive controls over harmful, constitutionally unprotected conduct.” [Broadrick], 413 U.S. at 615. For there are substantial social costs *created* by the overbreadth doctrine when it blocks application of a law to constitutionally unprotected speech, or especially to constitutionally unprotected conduct. To ensure that these costs do not swallow the social benefits of declaring a law overbroad, we have insisted that a law’s application to protected speech be substantial, not only in an absolute sense, but also relative to the scope of the law’s plainly legitimate applications before applying the strong medicine of overbreadth invalidation.

Id. at 118-20 (emphasis in original) (internal quotations and citations omitted except when appearing within quotation).<sup>4</sup>

---

<sup>4</sup> In Hicks, the Court further held that state law governs whether a party has standing to assert in state court a facial challenge under the First Amendment. “Whether Virginia’s courts

Thus, a law is unconstitutionally overbroad under the First Amendment when it prohibits a substantial amount of protected speech, either absolutely or as compared to the unprotected conduct also encompassed by the statute.

B.

The Relationship of Protected Speech and Code § 18.2-152.3:1

For a law to be unconstitutionally overbroad, it must proscribe a substantial amount of protected speech. Appellant contends that the sending of anonymous e-mails is protected by the First Amendment and that the VCCA proscribes the sending of anonymous e-mails. We take no position on the former contention because we disagree with the latter.

The right to speak anonymously has a long and respected history in First Amendment jurisprudence. In both Talley v. California, 362 U.S. 60 (1960), and McIntyre v. Ohio Election Comm's, 514 U.S. 334 (1995), the Supreme Court struck down requirements that an author's name and address appear on handbills. Both decisions cite the history and power of anonymous or pseudonymous speech in America, noting the Federalist Papers as early examples.

In contrast to requiring that an author's name and address appear on a handbill, the VCCA requires only that the sender not intend "to falsify or forge electronic mail transmission information or other routing information" *in connection with sending spam through an e-mail service provider's network*. Code § 18.2-152.3:1(A)(1). That is, the statute criminalizes the intentional falsification of a sender's identity so as to gain access to a service provider's network.

---

should have entertained this overbreadth challenge is entirely a matter of state law." Id. at 120. Since Hicks, no Virginia appellate court has addressed whether Virginia (as opposed to federal) law authorizes facial claims asserting overbreadth. See Muhammad v. Commonwealth, 269 Va. 451, 497, 619 S.E.2d 16, 42 (2005) (quoting Hicks but not addressing, in any detail, the appellant's facial overbreadth challenge to Virginia's anti-terrorism statutes because the appellant had "confine[d] his argument to vagueness"), cert. denied, 126 S. Ct. 2035 (2006). We need not resolve the issue in this case, however, because of our holding that the claim fails on the merits in any event.

Thus, the statute does not prevent anonymous speech, as appellant argues, but prohibits trespassing on private computer networks through intentional misrepresentation, an activity that merits no First Amendment protection.

Courts have consistently held that an e-mail service provider's computer network is private property and can be subject to trespassing. See, e.g., Ralsky, 203 F. Supp. 2d at 617 (“the sending of spam to and through an ISP's e-mail servers constitutes the tort of trespass to chattel in the state of Virginia”); United States v. Gray, 78 F. Supp. 2d 524, 532 (E.D. Va. 1999) (“[u]nauthorized access into a . . . computer is analogous to breaking and entering in the physical world”); America Online v. LCGM, 46 F. Supp. 2d 444, 452 (E.D. Va. 1998) (“transmission of electrical signals through a computer network is sufficiently ‘physical’ contact to constitute a trespass to property”); America Online v. IMS, 24 F. Supp. 2d 548, 550 (E.D. Va. 1998) (sending unauthorized spam constitutes trespass to chattels); CompuServe Inc. v. Cyber Promotions, 962 F. Supp. 1015, 1021 (S.D. Ohio 1997) (sending of electronic signals with a computer can support a trespass action).

Unauthorized spam can be a particularly harmful type of trespass to a computer network. Spam has been described as “one of the most popular forms of advertising over the Internet” and “the twenty first century version of junkmail.” Ralsky, 203 F. Supp. 2d at 606. In 2003 in an attempt to address the harm caused by spamming, the United States Congress passed 15 USC §§ 7701 to 7713, commonly known as the “CAN-SPAM Act.” Spam now constitutes over half of all e-mail traffic, 15 USC § 7701(a)(2) (2003), and the Senate has found that spam will cost corporations over \$113 billion by 2007. S. Rep. No. 108-102 (2003).

Courts have recognized the damage caused by spammers who trespass upon the private property of ISPs. In CompuServe, the court noted:

High volumes of junk e-mail devour computer processing and storage capacity, slow down data transfer between computers over

the Internet by congesting the electronic paths through which the messages travel, and cause recipients to spend time and money wading through messages that they do not want. It is ironic that if defendants were to prevail on their First Amendment arguments, the viability of electronic mail as an effective means of communication for the rest of society would be put at risk.

962 F. Supp. at 1028.

In State v. Heckel, 24 P.3d 404 (Wash. 2001), the Supreme Court of Washington wrote that:

To handle the increased e-mail traffic attributable to deceptive spam, ISPs must invest in more computer equipment. Operational costs likewise increase as ISPs hire more customer service representatives to field spam complaints and more system administrators to detect accounts being used to send spam.

\* \* \* \* \*

The cost-shifting--from deceptive spammers to businesses and e-mail users--has been likened to sending junk mail with postage due or making telemarketing calls to someone's pay-per-minute cellular phone.

Id. at 409-10 (citations omitted).

The record in this case demonstrates the damage caused to AOL by spammers such as appellant. AOL employs 30 people on its spam response team and receives 7 to 10 million complaints each day regarding spam. Over 1 billion pieces of spam attempt to enter AOL's private network daily. Subscribers often cite spam as their reason for declining to continue using AOL as their ISP. AOL typically blocks 70-80% of the e-mail traffic that attempts to pass into its network because it comes from IP addresses that have a history of sending spam. Of the e-mails that enter the system, another 20-30% are filtered into subscribers' dedicated spam folders. As noted above, appellant purposely falsified his transmission data to evade AOL's attempts to protect its property interest in its servers and better serve its customers.

The protection of private property and the right to keep others off that property have long been recognized as a fundamental sphere of state regulation. Blackstone wrote,

There is nothing which so generally strikes the imagination, and engages the affections of mankind, as the right of property; or that sole and despotic dominion which one man claims and exercises over the external things of the world, in total exclusion of the right of any other individual in the universe.

William Blackstone, 2 Commentaries \*2.

The common law is not without principle or precedent to protect private property - as here codified in the VCCA - applicable to a technological world.

The Supreme Court has consistently recognized the constitutionality of laws prohibiting trespass. In Martin v. Struthers, 319 U.S. 141, 147 (1943), the Court said that “[t]raditionally the American law punishes persons who enter onto the property of another after having been warned by the owner to keep off.” The Court considered free speech rights in public shopping malls in Lloyd Corp. v. Tanner, 407 U.S. 551, 568 (1972), and said, “this Court has never held that a trespasser or an uninvited guest may exercise general rights of free speech on property privately owned and used nondiscriminatorily for private purposes only.”

Rowan v. United States Post Office Dep’t, 397 U.S. 728 (1970), upheld the constitutionality of a law authorizing individuals to have their names removed from mass mailing lists and imposing penalties on organizations that failed to comply. The Court noted that to allow mailings to continue after a property owner has given notice that they must stop would be “to license a form of trespass.” Id. at 737. The opinion “reject[ed] the argument that a vendor has a right under the Constitution or otherwise to send unwanted material into the home of another” and recognized that “the asserted right of a mailer . . . stops at the outer boundary of every person’s domain.” Id. at 738.

The Supreme Court of Virginia addressed an analogous conflict between property rights and free speech in Hall v. Commonwealth, 188 Va. 72, 49 S.E.2d 369 (1948). In Hall, the defendant was convicted of trespassing for distributing religious materials in an apartment building after the building management forbade him from doing so. The Court upheld his conviction after a lengthy discussion of the precedents, concluding that the rule prohibiting visitors within the building unless a tenant allows their entry “is valid and reasonable and does not infringe upon any right or privilege guaranteed the accused by the Constitution . . . .” Id. at 90, 49 S.E.2d at 378.

Appellant has conceded that he has no constitutional right to use AOL’s servers to transmit his spam. Instead, he maintains that the statute prohibits anonymous or pseudonymous speech while not regulating other speech, meaning the VCCA is a content based restriction on speech and is thus subject to strict scrutiny. His reading of the statute ignores the requirement that the forgery be connected to “the transmission of unsolicited bulk e-mail through or into the computer network of an electronic mail service provider or its subscribers.” Code § 18.2-152.3:1(A)(1). The statute prohibits the falsification of the sender’s routing and transmission information to gain access to a computer network that would otherwise be inaccessible. In short, the statute prohibits lying to commit a trespass.

As Rowan and Hall clearly establish, the First Amendment does not prohibit a property owner from protecting his property from a trespass. As the homeowner in Rowan could stop the flow of unwanted junk mail into his home, now, an ISP can prevent the entry of spam into its network. While the method of delivery has changed, the underlying rights of the parties remain the same. The First Amendment gives no one the right to trespass on the property of another. And if the Commonwealth can criminalize the trespass, then certainly it can criminalize falsification to facilitate it.

As the statute in question here regards trespassing, not speech, appellant's reliance on ACLU v. Miller, 977 F. Supp. 1228 (N.D. Ga. 1997), is misplaced. Miller concerned a Georgia statute that, in part, prohibited using an "'individual name . . . to falsely identify the person'" in connection with sending an e-mail. Id. at 1230 (quoting Ga. Code Ann. § 16-9-93.1 (2006)) (omission in original). Unlike the VCCA provisions at issue here, Georgia's statute directly prohibited using a pseudonym in clear violation of established First Amendment jurisprudence, and the district court enjoined enforcement of the law. Because Virginia's statute addresses trespassing rather than the use of a pseudonym, Miller is not relevant to this case.

The First Amendment argument appellant presents is not relevant. The VCCA proscribes no speech. Rather, the statute proscribes intentional falsity as a machination to make massive, uncompensated use of the private property of an ISP. Therefore, the statute cannot be overbroad because no protected speech whatsoever falls within its purview.<sup>5</sup>

## VI.

### THE DORMANT COMMERCE CLAUSE

Appellant contends that the VCCA violates the Dormant Commerce Clause of the Constitution because it regulates transactions that take place outside Virginia's jurisdiction.<sup>6</sup> Generally, "[a] state statute must be upheld if it 'regulates evenhandedly to effectuate a legitimate local public interest, and its effects on interstate commerce are only incidental . . . unless the burden imposed on such commerce is clearly excessive in relation to the putative local benefits.'" Edgar v. Mite Corp., 457 U.S. 624, 640 (1982) (quoting Pike v. Bruce Church, Inc.,

---

<sup>5</sup> We also note that AOL's servers, obviously, do not constitute a public forum.

<sup>6</sup> Appellant, therefore, does not contend that the law discriminates against interstate commerce in favor of intrastate commerce, and we do not engage in such an analysis.



397 U.S. 137, 142 (1970)) (omission in original); see also Fredericksburg Auto Auction v. Dep't of Motor Vehicles, 242 Va. 42, 50, 406 S.E.2d 23, 28 (1991) (applying Pike balancing test).

While appellant contends that regulations which can have a wholly extraterritorial effect are *per se* violations, recent authorities have found such factors to be merely a subset of the Pike balancing test, which is restated above in the quote from Edgar. See Heckel, 24 P.3d at 411 (“the extra territoriality analysis [is] appropriately regarded as [a facet] of the Pike balancing test”); Jack L. Goldsmith & Alan O. Sykes, The Internet and the Dormant Commerce Clause, 110 Yale L.J. 785, 804-05 (2001) (“the appropriate statement of the extraterritoriality concern is that states may not impose burdens on out-of-state actors that outweigh the in-state benefits”). Thus, the issues are whether the VCCA has local benefits and whether the burden imposed on interstate commerce by the law is clearly excessive in relationship to those benefits.

That anti-spam laws, in general, produce local benefits is unquestionable. The United States Congress has found that “[t]he convenience and efficiency of electronic mail are threatened by the extremely rapid growth in the volume of unsolicited commercial electronic mail.” 15 U.S.C. § 7701. Furthermore, Congress found that spam costs recipients extra money, may expose recipients to obscene material, costs e-mail providers money, and is frequently fraudulent or deceptive.<sup>7</sup> Id. Numerous courts have found that states have an interest in protecting residents and service providers from the costs of handling spam and the often fraudulent content it presents. See Heckel, 24 P.3d at 411; MaryCLE, LLC v. First Choice Internet, Inc., 890 A.2d 818, 835 (Md. Ct. Spec. App. 2006) (finding state interest in a personal jurisdiction context); Ralsky, 203 F. Supp. 2d at 621-22 (also in a personal jurisdiction context).

---

<sup>7</sup> In fact, the Senate Report that accompanied the CAN-SPAM act found that two-thirds of all spam contains fraudulent content. S. Rep. No. 108-102, at 2-3 (2003).

As the trial court noted, “[t]he Commonwealth clearly has an interest in the protection of the property interests of its citizens.”

As noted in Part V(B), *supra*, of this opinion, AOL expends significant resources in efforts to protect its private property from spammers and in so doing offer better service to millions of its subscribers. We find that Virginia properly has a significant local interest in protecting the property of its citizens. The VCCA addresses that legitimate interest.

With that finding, then, we next must determine what burden, if any, on commerce that the VCCA presents. The VCCA requires only that senders of unsolicited bulk e-mail not intentionally “falsify or forge electronic mail transmission information or other routing information.” Code § 18.2-152.3:1(A)(1). Thus, as the trial court noted, the only burden on any sender is to present truthful transmission and routing information.

We agree with one pair of commentators who noted

Even assuming that the antispam laws do not significantly further the state’s interest, it is hard to see how the antispam laws burden interstate commerce at all. . . . Far from burdening commerce, the truthfulness requirement facilitates it by eliminating fraud and deception. Compliance with the various antispam statutes is easy compared to noncompliance, which requires the spammer to incur costs of forging, re-mailing, and the like.

Goldsmith & Sykes, *supra*, at 819.

Indeed, it is in furtherance of commerce that the VCCA requires truthful transmission data, enabling the purchasing party to consummate a transaction. As the record shows, the e-mails in this case appeared to come from thousands of e-mail addresses at multiple “hello” domains with thousands of different IP addresses, tactics used to disguise spam and avoid detection by spam filters that ISPs such as AOL employ. Notably, if an e-mail recipient “clicked” to buy one of appellant’s offers, the recipient was redirected to one of the thousands of websites appellant established in his effort to evade AOL’s spam filters.

Finally, we note one court’s observation that “Congress, in enacting CAN-SPAM, expressly accorded the States the right to regulate false and misleading e-mail transmissions. 15 U.S.C. 7707(b)(1). If Congress itself was satisfied that supplementary state legislation would impose no undue burden on interstate commerce, this Court can hardly presume to tell Congress it is wrong.” Beyond Sys., Inc. v. Keynetics, Inc., 422 F. Supp. 2d 523, 535 (D. Md. 2006).

The effort required to violate the VCCA, and its requirement of truthful transmission information, is significant. No effort is required to comply with the law. Applying the balancing test set forth in Pike, Virginia does have a legitimate local public interest in the VCCA and any burden to interstate commerce is incidental and clearly not excessive. Thus, the VCCA does not violate the Dormant Commerce Clause.

## VII.

### CONSTITUTIONAL VAGUENESS

We reiterate that we consider constitutional questions *de novo*, pursuant to the standard of review set forth above in Part V(B), *supra*, of this opinion.

Appellant maintains that the VCCA is unconstitutionally vague in three instances: 1) that the words “unsolicited” and “bulk” in the phrase “unsolicited bulk electronic mail” are undefined, and thus vague; 2) that the phrase “electronic mail transmission information or other routing information” is undefined, and likewise vague; and 3) that the use of the acronym “UBE” for the earlier phrase “unsolicited bulk electronic mail” is vague. In arguing these points, appellant seeks to challenge the validity of the statute on its face, rather than as applied to him.

As discussed above in Part V(A), *supra*, a litigant generally may only challenge the validity of a statute as applied to him and may not present the rights of third parties. A party may present a facial challenge that a statute is overbroad when the statute touches upon First Amendment rights, and a party may likewise make a facial challenge that a statute is vague when

it potentially chills First Amendment rights. Kolender v. Lawson, 461 U.S. 352, 357-58 (1983); Broadrick, 413 U.S. at 611-12; United States v. Nat'l Dairy Prods. Corp., 372 U.S. 29, 36 (1963).

In support of his argument that he is entitled to a facial challenge on these grounds, appellant relies upon Reno v. ACLU, 521 U.S. 844 (1997), and the decision of this Court in Coleman v. City of Richmond, 5 Va. App. 459, 364 S.E.2d 239 (1988).

The Supreme Court addressed a First Amendment facial challenge to two New York statutes “enacted to protect minors from ‘indecent’ and ‘patently offensive’ communications on the Internet” in Reno, 521 U.S. at 849. The core of the Court’s decision turns on the inherent difficulties of sufficiently defining such terms as “obscene” or “indecent” without intruding on constitutionally protected speech.

In Coleman, we found unconstitutionally vague a city ordinance which prohibited loitering with the purpose of finding a prostitute. We noted therein that loitering is a lawful act entitled to constitutional protection on First Amendment grounds. 5 Va. App. at 464, 364 S.E.2d at 242 (citing Papachristou v. City of Jacksonville, 405 U.S. 156, 164 (1972)). As a United States District Court later stated regarding a challenge to a Virginia statute, “Any attempt to prohibit loitering potentially implicates First Amendment rights.” Lytle v. Doyle, 197 F. Supp. 2d 481, 488 (E.D. Va. 2001). Our denial of a petition for rehearing in Coleman makes clear that the decision was based on First Amendment grounds: “Coleman raised freedom of association and first amendment rights. Our decision . . . held the Richmond ordinance unconstitutional on its face in light of first amendment concerns.” Coleman v. City of Richmond, 6 Va. App. 296, 298, 368 S.E.2d 298, 300 (1988).

In Part V(B), *supra*, of this opinion, we hold that the VCCA does not implicate First Amendment rights. Both Reno and Coleman are premised upon such rights. Thus, appellant’s reliance on these decisions to establish his right to a facial challenge to the VCCA is misplaced.

We therefore will consider appellant’s arguments based upon the law as applied to his conduct. “[V]agueness challenges to statutes not threatening First Amendment interests are examined in light of the facts of the case at hand; the statute is judged on an as-applied basis.” Motley v. Virginia State Bar, 260 Va. 243, 247, 536 S.E.2d 98, 99 (2000) (quoting Maynard v. Cartwright, 486 U.S. 356, 361 (1988)); see also Muhammad v. Commonwealth, 269 Va. 451, 501, 619 S.E.2d 16, 44 (2005) (citing Hoffman Estates v. Flipside, Hoffman Estates, Inc., 455 U.S. 489, 494-95 (1982)).

As applied to appellant’s actions, the VCCA “is unconstitutionally vague if it fails to ‘give the person of ordinary intelligence a reasonable opportunity to know what is prohibited . . . .’” County of Fairfax v. S. Iron Works, Inc., 242 Va. 435, 444-45, 410 S.E.2d 674, 680 (1991) (quoting Grayned v. City of Rockford, 408 U.S. 104, 108 (1972)). A law can also be vague if it allows for “arbitrary and discriminatory enforcement.” Kolender, 461 U.S. at 357.<sup>8</sup>

Applying that standard, we analyze each of appellant’s three contentions seriatim.

A.

The word “unsolicited” is not unconstitutionally vague because, among states with laws relating to spam, “unsolicited” has a practically universal definition.<sup>9</sup> An e-mail is unsolicited if

---

<sup>8</sup> Appellant’s only challenge under the “arbitrary and discriminatory enforcement” prong of the vagueness test is a facial one to the misdemeanor provisions of the statute, under which appellant was not charged. As appellant is entitled only to an as-applied challenge, we need not discuss the second prong.

<sup>9</sup> See, e.g., Ark. Code Ann. § 4-88-602 (West Supp. 2005) (“‘Unsolicited’ means without the recipient’s express permission, except that commercial electronic mail is not unsolicited if the sender has a preexisting business or personal relationship with the recipient”); Mich Comp. Laws. Ann. § 445.2502 (West Supp. 2006) (“‘Unsolicited’ means without the recipient’s express

the recipient neither requested nor consented to receive such e-mails and if the sender and recipient have no preexisting business or personal relationship. Generally included within this definition, although sometimes explicitly stated in statutes, is the notion that an organization may send e-mails to its members, employees, or contractors and that such e-mails are not “unsolicited.”

Aside from the consistency with which other states define the term, this seems to be the only logical meaning. No one would argue that an e-mail is unsolicited if the recipient requested or consented to its transmission. Furthermore, once two parties have established a relationship, communications cannot be considered unsolicited for purposes of a criminal statute simply because one party did not specifically request it of the other. Thus, an e-mail is “unsolicited” if the parties have no previously existing relationship, either business or personal, and the recipient did not request or consent to its transmission.

Given the consistency and logical power of this definition as applied to appellant, he would certainly have known that these e-mails were unsolicited. Appellant sent thousands of e-mails at random to AOL subscribers whose addresses were among the 107 million stolen AOL e-mail addresses stored on discs in his possession. Appellant did not compile a mailing list by allowing people to register their names, nor did he build this list from previous contacts with people. He obtained a stolen database of AOL e-mail addresses and sent his messages out blindly.

---

permission. An e-mail is not unsolicited if the sender has a preexisting business or personal relationship with the recipient. An e-mail is not unsolicited if it was received as a result of the recipient opting into a system in order to receive promotional material.”); N.C. Gen. Stat. Ann. § 14-453 (West 2000) (“‘Unsolicited’ means not addressed to a recipient with whom the initiator has an existing business or personal relationship and not sent at the request of, or with the express consent of, the recipient.”).

Appellant's contention that "bulk" is a vague term also fails because the law specifically defines the word. Code § 18.2-152.3:1(B)(1) establishes that transmission "exceed[ing] 10,000 attempted recipients in any 24-hour period" constitutes a felony. Appellant admits that this section sufficiently defines how many e-mails constitute "bulk" but maintains that for lesser amounts of spam, the statute is vague. As noted above, the record reveals that appellant sent 12,197 falsified e-mails on July 16, 2003; 24,172 falsified e-mails on July 19, 2003; and 19,104 falsified e-mails on July 26, 2003. Because the statute clearly prohibits his conduct, appellant's challenge fails. Hoffman Estates, 455 U.S. at 495 ("A plaintiff who engages in some conduct that is clearly proscribed cannot complain of the vagueness of the law as applied to the conduct of others.").

B.

Appellant next contends that the phrase "electronic mail transmission information or other routing information" is vague. Initially, we note that the Supreme Court of Virginia has already defined the word "route" as meaning "a direction of travel from one place to another." Virginia Stage Lines, Inc. v. Commonwealth, 186 Va. 1066, 1076, 45 S.E.2d 318, 323 (1947). Routing information, then, would be the information that directs the message from one place to another, or the record of that travel.

"We give the words of a statute 'their common, ordinary and accepted meaning,' absent an indication by the legislature to the contrary." Saunders v. Commonwealth, 48 Va. App. 196, 201, 629 S.E.2d 701, 703 (2006); see also Stein v. Commonwealth, 12 Va. App. 65, 68, 402 S.E.2d 238, 241 (1991) (citing Lovisi v. Commonwealth, 212 Va. 848, 850, 188 S.E.2d 206, 208 (1972)). "[C]ourts are bound by the plain meaning of clear statutory language." Crawford v. Haddock, 270 Va. 524, 528, 621 S.E.2d 127, 129 (2005) (citations omitted); see also Last v. Virginia State Bd. of Med., 14 Va. App. 906, 910, 421 S.E.2d 201, 205 (1992) ("Where a statute

is unambiguous, the plain meaning is to be accepted without resort to the rules of statutory interpretation.”). Words that have commonly accepted meanings within their statutory *context* are not vague. See, e.g., Gray v. Commonwealth, 260 Va. 675, 681, 537 S.E.2d 862, 865 (2000) (noting contextual meanings of “muffler” and “silencer” in firearms statute).

Appellant maintains that the phrase “transmission information” is vague. Black’s Law Dictionary defines “transmit” as “[t]o send or transfer from one person or place to another, or to communicate.” 1505 (7th ed. 1999). Thus, the common, ordinary and accepted meaning of the term is that it means the data necessary to transmit, or carry, the e-mail from its origin to its intended recipient.

The VCCA’s requirement that the falsification or forgery of the transmission information or routing information be *intentional* further serves to protect that statute from a vagueness challenge. As the Supreme Court noted in National Dairy Products, “a requirement of intent [can serve] to ‘relieve the statute of the objection that it punishes without warning an offense of which the accused was unaware.’” 372 U.S. at 35 (quoting Screws v. United States, 325 U.S. 91, 102 (1945)). This Court has similarly noted that “[b]y requiring specific intent . . . [a] statute gives a person of ordinary intelligence a reasonable opportunity to know what is proscribed.” Woolfolk v. Commonwealth, 18 Va. App. 840, 851, 447 S.E.2d 530, 536 (1994) (citations omitted); see also Hernandez v. Commonwealth, 12 Va. App. 669, 672, 406 S.E.2d 398, 400 (1991) (holding the intent requirement, in part, makes constitutional a statute prohibiting wearing of mask in public).

In National Dairy Products, the Court also held the challenged statute constitutional because the statute “listed as elements of the illegal conduct . . . the intent to achieve a result . . . [and] also the act . . . done in furtherance of that design or purpose.” 372 U.S. at 35. The VCCA operates similarly. It establishes the illegal conduct (lying to commit a trespass on computer



servers), identifies an act done in furtherance (falsification of routing or transmission information), and requires the act be done intentionally.

Here, appellant intended to falsify his identity and the origins of his e-mails in order to avoid detection by AOL's spam filters. The complicated machinations necessary to achieve this criminal purpose negate any contention that the phrase "transmission information or other routing information" is vague. Appellant's conduct is exactly the conduct the statute seeks to criminalize, and appellant intentionally undertook those acts.

### C.

Code § 18.2-152.3:1(A) of the VCCA contains the phrase "unsolicited bulk electronic mail." Subsection B uses the acronym "UBE" for the phrase quoted from subsection A. For example, a sentence in subsection B begins: "The volume of UBE transmitted exceeded 10,000 attempted recipients in any 24-hour period . . . ." Appellant maintains the use of the acronym renders the statute impermissibly vague.

Recently, the Supreme Court of Virginia set out principles of statutory interpretation here applicable:

Generally, the Court "will look to the whole body of [a statute] to determine the true intention of each part." McDaniel v. Commonwealth, 199 Va. 287, 292, 99 S.E.2d 623, 627 (1957); *accord* Rockingham Coop. Farm Bureau, Inc. v. City of Harrisonburg, 171 Va. 339, 344, 198 S.E. 908, 910 (1938). "[A] statute should be read and considered as a whole, and the language of a statute should be examined in its entirety to determine the intent of the General Assembly from the words contained in the statute." Dep't of Med. Assistance Servs. v. Beverly Healthcare of Fredericksburg, 268 Va. 278, 285, 601 S.E.2d 604, 607-08 (2004). "In doing so, the various parts of the statute should be harmonized so that, if practicable, each is given a sensible and intelligent effect." Colchester Towne Condo. Council of Co-Owners v. Wachovia Bank, N.A., 266 Va. 46, 51, 581 S.E.2d 201, 203 (2003) (citing VEPCO v. Prince William County, 226 Va. 382, 387-88, 309 S.E.2d 308, 311 (1983)).

Oraee v. Breeding, 270 Va. 488, 498, 621 S.E.2d 48, 52-53 (2005).

More specifically, the acronym “UBE” is to be given meaning “in the context in which it is used.” Dep’t of Taxation v. Orange-Madison Coop. Farm Serv., 220 Va. 655, 658, 261 S.E.2d 532, 534 (1980). “[T]he context may be examined by considering other language used in the statute.” City of Virginia Beach v. Bd. Of Supervisors of Mecklenburg County, 246 Va. 233, 236-37, 435 S.E.2d 382, 384 (1993).

Applying these principles, the only reasonable interpretation of the acronym within the statute is that it means “unsolicited bulk electronic mail.” We hold that the acronym “UBE” in the context used and in relation to the other language in the VCCA is not so vague that a person of ordinary intelligence could fail to understand its meaning.

For the reasons stated above, the VCCA is sufficiently definite so as to not be unconstitutionally vague as applied to appellant’s conduct.

## VI.

### CONCLUSION

Having concluded that the trial court had jurisdiction over this case and that Code § 18.2-152.3:1 does not violate the First Amendment, does not violate the Dormant Commerce Clause, and is not unconstitutionally vague, appellant’s convictions are affirmed.

Affirmed.