JEREMY JAYNES v. COMMONWEALTH OF VIRGINIA
276 Va. 443 (2008)

OPINION

Jeremy Jaynes appeals from the judgment of the Court of Appeals which affirmed his convictions for violations of Code § 18.2-152.3:1, the unsolicited bulk electronic mail (e-mail) provision of the Virginia Computer Crimes Act, Code §§ 18.2-152.1 through - 152.15. For the reasons set forth below, we will reverse the judgment of the Court of Appeals.

I. BACKGROUND AND MATERIAL PROCEEDINGS BELOW

From his home in Raleigh, North Carolina, Jaynes used several computers, routers and servers to send over 10,000 e-mails within a 24-hour period to subscribers of America Online, Inc. (AOL) on each of three separate occasions. None of the recipients of the e-mails had requested any communication from Jaynes. He intentionally falsified the header information and sender domain names before transmitting the e-mails to the recipients.[1] However, investigators used a sophisticated database search to identify Jaynes as the sender of the e-mails. Jaynes was arrested and charged with violating Code § 18.2-152.3:1, which provides in relevant part:

> 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 or its subscribers . . . is guilty of a Class 1 misdemeanor.
>
> 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 . . .

While executing a search of Jaynes' home, police discovered a cache of compact discs (CDs) containing over 176 million full e-mail addresses and 1.3 billion e-mail user names. The search also led to the confiscation of storage discs which contained AOL e-mail address information and other personal and private account information for millions of AOL subscribers. The AOL user information had been stolen from AOL by a former employee and was in Jaynes' possession. During trial, evidence demonstrated that Jaynes knew that all of the more than 50,000 recipients of his unsolicited e-mails were subscribers to AOL, in part, because the e-mail addresses of all recipients ended in "@aol.com."[2]

---

[1] Simple Mail Transfer Protocol (SMTP) is what an e-mail server uses to transmit an e-mail message, and the SMTP requires verification of the sender's IP address and domain. Evidence at trial demonstrated that Jaynes sent the e-mails with domain names which did not correspond to the domain names assigned to the sending IP addresses.

[2] Jaynes' e-mails advertised one of three products: (1) a FedEx refund claims product, (2) a "Penny Stock Picker," and (3) a "History Eraser" product. To purchase one of these products, potential buyers would click on a hyperlink within the e-mail, which redirected them outside the e-mail, where

An expert witness testified that the e-mails sent by Jaynes were not consistent with solicited bulk e-mail, but rather constituted unsolicited bulk e-mail (sometimes referred to as "spam" e-mail) because Jaynes had disguised the true sender and header information and used multiple addresses to send the e-mails. Other evidence demonstrated that all of AOL's servers were located in Virginia.

A jury convicted Jaynes of three counts of violating Code § 18.2-152.3:1, and the circuit court sentenced Jaynes to three years in prison on each count, with the sentences to run consecutively for an active term of imprisonment of nine years. The Court of Appeals affirmed his convictions, *Jaynes v. Commonwealth*, 48 Va. App. 673, 634 S.E.2d 357 (2006). We awarded Jaynes an appeal.

II. ANALYSIS

Jaynes assigns error to the determination that the circuit court had jurisdiction over him on the crimes charged. Second, Jaynes contends Code § 18.2-152.3:1 "abridge[s] the First Amendment right to anonymous speech," and it was error not to reverse his convictions on that basis.

A. JURISDICTION

Jaynes asserts that the Court of Appeals erred in holding that the circuit court had jurisdiction over him for violating Code § 18.2-152.3:1 because he did not "use" a computer in Virginia. He contends that a violation of that statute can occur only in the location where the e-mail routing information is falsified. Jaynes maintains that because he only used computers to send the e-mails from his home in Raleigh, North Carolina, he committed no crime in Virginia. Further, because he had no control over the routing of the e-mails, he argues his actions did not have an "immediate result" in Virginia, and could not be the basis for jurisdiction over him by Virginia courts. Therefore, according to Jaynes, the circuit court had no jurisdiction over him and his convictions are void.

To successfully prosecute a crime under Code § 18.2-152.3:1(B), the Commonwealth must establish all the elements of that crime. In addition to the element of the volume of transmissions within a specific time period, the Commonwealth must prove the sender used a computer and that such use was with the intent of falsifying routing information. The Commonwealth must also prove that the transmission of such false routing information occurred in connection with the use of an e-mail provider's computer network for that transmission. Thus, the crime is not complete until there is e-mail transmission passing through or into the computer network of the e-mail provider or subscriber containing the false routing information.

Jaynes argues that he "merely sent e-mails that happened to be routed through AOL servers." We disagree. As the evidence established, all e-mail must flow through the recipient's e-mail server in order to reach the intended recipient. By selecting AOL subscribers as his e-mail recipients, Jaynes knew and intended that his e-mails would utilize AOL servers because he clearly intended to send to users whose e-mails ended in "@aol.com." The evidence established that the AOL servers are located in Virginia, and that the location of AOL's servers was information easily accessible to the general public. Applying our standard of review to the evidence presented along with all reasonable inferences therefrom, we conclude that the evidence supports the conclusion that Jaynes knew and intended that the e-mails he sent to AOL subscribers would utilize AOL's servers which are located in Virginia. Thus an intended and necessary result of Jaynes' action, the e-mail transmission through the computer network, occurred in Virginia.

---

they could consummate the purchase.

Furthermore, a state may exercise jurisdiction over criminal acts that are committed outside the state, but are intended to, and do in fact, produce harm within the state. "'It has long been a commonplace of criminal liability that 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 (1949) (citing *Strassheim v. Daily*, 221 U.S. 280, 284-85, 31 S. Ct. 558, 55 L. Ed. 735 (1911)).

Because the use of the computer network of an e-mail service provider or its subscribers is an integral part of the crime charged and because the use of AOL's e-mail servers was the "immediate result" of Jaynes' acts, we hold that Jaynes was amenable to prosecution in Virginia for a violation of Code § 18.2-152.3:1. Accordingly, the circuit court had jurisdiction over Jaynes.

B. FIRST AMENDMENT OVERBREADTH

Jaynes next contends that Code § 18.2-152.3:1 is constitutionally deficient as overbroad under the First Amendment and therefore the statute cannot be enforced. He argues the Court of Appeals erred in affirming the circuit court's ruling denying his motion to dismiss on that basis.

Jaynes does not make an "as-applied challenge" to the statute, meaning he does not contend the application of the statute to the actual acts for which he was convicted violates the First Amendment. Instead, Jaynes challenges the statute by claiming it is unconstitutional as overbroad. That is, Jaynes contends that because the statute could potentially reach the protected speech of a third party, he (Jaynes) is entitled to claim exoneration for his otherwise unprotected speech.

We now turn to Jaynes' contention that Code § 18.2-152.3:1 is unconstitutionally overbroad. To address this challenge, we first review certain technical aspects of the transmission of e-mails. In transmitting and receiving e-mails, the e-mail servers use a protocol which prescribes what information one computer must send to another. This SMTP requires that the routing information contain an IP address and a domain name for the sender and recipient of each e-mail. Domain names and IP addresses are assigned to Internet servers by private organizations through a registration process. To obtain an IP address or domain name, the registrant pays a fee and provides identifying contact information to the registering organization. The domain names and IP addresses are contained in a searchable database which can associate the domain name with an IP address and vice versa.

The IP address and domain name do not directly identify the sender, but if the IP address or domain name is acquired from a registering organization, a database search of the address or domain name can eventually lead to the contact information on file with the registration organizations. A sender's IP address or domain name which is not registered will not prevent the transmission of the e-mail; however, the identity of the sender may not be discoverable through a database search and use of registration contact information.[3]

As shown by the record, because e-mail transmission protocol requires entry of an IP address and domain name for the sender, the only way such a speaker can publish an anonymous e-mail is to enter a false IP address or domain name. Therefore, like the registration record on file in the mayor's office identifying persons who chose to canvass private neighborhoods in *Watchtower Bible & Tract Society v. Village of Stratton*, 536 U.S. 150 (2002), registered IP addresses and domain names discoverable through searchable data bases and registration documents "necessarily result [] in a surrender of [the speaker's] anonymity." The right to engage in anonymous speech, particularly

[3] In this case Jaynes used registered IP addresses, although the domain names were false.

anonymous political or religious speech, is "an aspect of the freedom of speech protected by the First Amendment." *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 342 (1995). By prohibiting false routing information in the dissemination of e-mails, Code § 18.2-152.3:1 infringes on that protected right. The Supreme Court has characterized regulations prohibiting such anonymous speech as "a direct regulation of the content of speech."

State statutes that burden "core political speech," as this statute does, are presumptively invalid and subject to a strict scrutiny test. Under that test a statute will be deemed constitutional only if it is narrowly drawn to further a compelling state interest. In applying this test, we must also consider that state statutes are presumed constitutional, and any reasonable doubt regarding constitutionality must be resolved in favor of validity.

There is no dispute that Code § 18.2-152.3:1 was enacted to control the transmission of unsolicited commercial bulk e-mail, generally referred to as SPAM. In enacting the federal CAN-SPAM Act, Congress stated that commercial bulk e-mail threatened the efficiency and convenience of e-mail. 15 U.S.C. § 7701(a)(2). Many other states have regulated unsolicited bulk e-mail but, unlike Virginia, have restricted such regulation to commercial e-mails. There is nothing in the record or arguments of the parties, however, suggesting that unsolicited non-commercial bulk e-mails were the target of this legislation, caused increased costs to the Internet service providers, or were otherwise a focus of the problem sought to be addressed by the General Assembly through its enactment of Code § 18.2-152.3:1.

Jaynes does not contest the Commonwealth's interest in controlling unsolicited commercial bulk e-mail as well as fraudulent or otherwise illegal e-mail. Nevertheless, Code § 18.2-152.3:1 is not limited to instances of commercial or fraudulent transmission of e-mail, nor is it restricted to transmission of illegal or otherwise unprotected speech such as pornography or defamation speech. Therefore, viewed under the strict scrutiny standard, Code § 18.2-152.3:1 is not narrowly tailored to protect the compelling interests advanced by the Commonwealth.

4. SUBSTANTIAL OVERBREADTH

The Commonwealth argues that we should not preclude enforcement of Code § 18.2-152.3:1 because, even if unconstitutionally overbroad, that remedy is limited to those statutes that are substantially overbroad. The concept of substantial overbreadth is not a test of the constitutionality of a statute, but a policy related to the remedy flowing from a successful facial challenge. A successful facial overbreadth challenge precludes the application of the affected statute in all circumstances. Recognizing the sweep of this remedy, the United States Supreme Court has stated that it will not impose such an expansive result where the chilling effect of an overbroad statute on constitutionally protected rights cannot justify prohibiting all enforcement of the law. "For there are substantial social costs created by the overbreadth doctrine when it blocks application of a law to constitutionally unprotected speech. . . ." Thus a statute should be declared facially overbroad and unconstitutional only if the statute "punishes a 'substantial' amount of protected free speech, 'judged in relation to the statute's plainly legitimate sweep.'"

The Commonwealth argues that Code § 18.2-152.3:1 is not substantially overbroad because it does not impose any restrictions on the content of the e-mail and "most" applications of its provisions would be constitutional, citing its application to unsolicited bulk commercial e-mail, unsolicited bulk e-mail that proposes a criminal transaction, and unsolicited bulk e-mail that is defamatory or contains obscene images. According to the Commonwealth an "imagine[d] hypothetical situation

where the Act might be unconstitutional as applied does not render the Act substantially overbroad."

The United States Supreme Court recently reviewed the First Amendment overbreadth doctrine in *United States v. Williams*, 128 S. Ct. 1830 (2008). The Court noted

> [i]n order to maintain an appropriate balance, we have vigorously enforced the requirement that a statute's overbreadth be *substantial*, not only in an absolute sense, but also relative to the statute's plainly legitimate sweep.
>
> . . . [I]t is impossible to determine whether a statute reaches too far without first knowing what the statute covers.

Applying that inquiry under *Williams* in this case is relatively straightforward as Code § 18.2-152.3:1 would prohibit all bulk e-mail containing anonymous political, religious, or other expressive speech. For example, were the *Federalist Papers* just being published today via e-mail, that transmission by Publius would violate the statute. Such an expansive scope of unconstitutional coverage is not what the Court in *Williams* referenced "as the tendency of our overbreadth doctrine to summon forth an endless stream of fanciful hypotheticals." We thus reject the Commonwealth's argument that Jaynes' facial challenge must fail because the statute is not "substantially overbroad."

5. NARROWING CONSTRUCTION

Lastly, the Commonwealth asserts that we need not declare Code § 18.2-152.3:1 unconstitutional because a limiting construction can be adopted by this Court that would prevent invalidating the statute. Such a construction according to the Commonwealth would be a declaration that the statute does not apply to "unsolicited bulk non-commercial e-mail that does not involve criminal activity, defamation or obscene materials." Alternatively the Commonwealth suggests that we hold the statute applies only in instances where the receiving Internet service provider "actually objects to the bulk e-mail."

Our jurisprudence requires us to interpret a statute to avoid a constitutional infirmity. Nevertheless, construing statutes to cure constitutional deficiencies is allowed only when such construction is reasonable. A statute cannot be rewritten to bring it within constitutional requirements. *Reno v. ACLU*, 521 U.S. 844, 884-85 (1997). The construction urged by the Commonwealth is not a reasonable construction of the statute. Nothing in the statute suggests the limited applications advanced by the Commonwealth. If we adopted the Commonwealth's suggested construction we would be rewriting Code § 18.2-152.3:1 in a material and substantive way. Such a task lies within the province of the General Assembly, not the courts.

III. CONCLUSION

For the foregoing reasons, we hold that Code § 18.2-152.3:1 is unconstitutionally overbroad on its face because it prohibits the anonymous transmission of all unsolicited bulk e-mails including those containing political, religious or other speech protected by the First Amendment to the United States Constitution. Accordingly, we will reverse the judgment of the Court of Appeals and vacate Jaynes' convictions of violations of Code § 18.2-152.3:1.