B. The First Amendment Applied to Other Types of Internet Speech

BROWN v. ENTERTAINMENT MERCHANTS ASSOCIATION
131 S. Ct. 2729 (2011)

Justice Scalia delivered the opinion of the Court.

California Assembly Bill 1179 (2005), Cal. Civ. Code Ann. §§1746-1746.5 (Act), prohibits the sale or rental of "violent video games" to minors, and requires their packaging to be labeled "18." The Act covers games "in which the range of options available to a player includes killing, maiming, dismembering, or sexually assaulting an image of a human being, if those acts are depicted" in a manner that "[a] reasonable person, considering the game as a whole, would find appeals to a deviant or morbid interest of minors," that is "patently offensive to prevailing standards in the community as to what is suitable for minors," and that "causes the game, as a whole, to lack serious literary, artistic, political, or scientific value for minors." Violation of the Act is punishable by a civil fine of up to $1,000.

Respondents, representing the video-game and software industries, brought a preenforcement challenge to the Act in the United States District Court for the Northern District of California. That court concluded that the Act violated the First Amendment and permanently enjoined its enforcement. The Court of Appeals affirmed, and we granted certiorari.

California correctly acknowledges that video games qualify for First Amendment protection. The Free Speech Clause exists principally to protect discourse on public matters, but we have long recognized that it is difficult to distinguish politics from entertainment, and dangerous to try. "Everyone is familiar with instances of propaganda through fiction. What is one man's amusement, teaches another's doctrine." Like the protected books, plays, and movies that preceded them, video games communicate ideas--and even social messages--through many familiar literary devices (such as characters, dialogue, plot, and music) and through features distinctive to the medium (such as the player's interaction with the virtual world). That suffices to confer First Amendment protection. Under our Constitution, "esthetic and moral judgments about art and literature . . . are for the individual to make, not for the Government to decree, even with the mandate or approval of a majority." And whatever the challenges of applying the Constitution to ever-advancing technology, "the basic principles of freedom of speech and the press do not vary" when a new and different medium for communication appears.

The most basic of those principles is this: "[A]s a general matter, . . . government has no power to restrict expression because of its message, its ideas, its subject matter, or its content." There are of course exceptions. These limited areas--such as obscenity, incitement, and fighting words--represent "well-defined and narrowly limited classes of speech, the prevention and punishment of which have never been thought to raise any Constitutional problem."

Because speech about violence is not obscene, it is of no consequence that California's statute mimics the New York statute regulating obscenity-for-minors that we upheld in *Ginsberg v. New York*, 390 U. S. 629 (1968). That case approved a prohibition on the sale to minors of sexual

material that would be obscene from the perspective of a child. We held that the legislature could "adjus[t] the definition of obscenity 'by permitting the appeal of this type of material to be assessed in terms of the sexual interests' of minors." And because "obscenity is not protected expression," the New York statute could be sustained so long as the legislature's judgment that the proscribed materials were harmful to children "was not irrational."

The California Act is something else entirely. It does not adjust the boundaries of an existing category of unprotected speech to ensure that a definition designed for adults is not uncritically applied to children. Instead, it wishes to create a wholly new category of content-based regulation that is permissible only for speech directed at children.

That is unprecedented and mistaken. "[M]inors are entitled to a significant measure of First Amendment protection, and only in relatively narrow and well-defined circumstances may government bar public dissemination of protected materials to them." No doubt a State possesses legitimate power to protect children from harm, but that does not include a free-floating power to restrict the ideas to which children may be exposed. "Speech that is neither obscene as to youths nor subject to some other legitimate proscription cannot be suppressed solely to protect the young from ideas or images that a legislative body thinks unsuitable for them."

III

Because the Act imposes a restriction on the content of protected speech, it is invalid unless California can demonstrate that it passes strict scrutiny--that is, unless it is justified by a compelling government interest and is narrowly drawn to serve that interest. The State must specifically identify an "actual problem" in need of solving, and the curtailment of free speech must be actually necessary to the solution. That is a demanding standard. "It is rare that a regulation restricting speech because of its content will ever be permissible."

California cannot meet that standard. It cannot show a direct causal link between violent video games and harm to minors. The State claims that it need not produce such proof because the legislature can make a predictive judgment that such a link exists, based on competing psychological studies. But California's burden is much higher, and because it bears the risk of uncertainty, ambiguous proof will not suffice.

California claims that the Act is justified in aid of parental authority: By requiring that the purchase of violent video games can be made only by adults, the Act ensures that parents can decide what games are appropriate. At the outset, we note our doubts that punishing third parties for conveying protected speech to children just in case their parents disapprove of that speech is a proper governmental means of aiding parental authority. Accepting that position would largely vitiate the rule that "only in relatively narrow and well-defined circumstances may government bar public dissemination of protected materials to [minors]."

But leaving that aside, California cannot show that the Act's restrictions meet a substantial need of parents who wish to restrict their children's access to violent video games but cannot do so. The video-game industry has in place a voluntary rating system designed to inform consumers about the content of games. This system does much to ensure that minors cannot purchase seriously violent games on their own, and that parents who care about the matter can readily

evaluate the games their children bring home. Filling the remaining modest gap in concerned-parents' control can hardly be a compelling state interest.

The Act's purported aid to parental authority is vastly overinclusive. While some of the legislation's effect may be in support of what some parents of the restricted children actually want, its entire effect is only in support of what the State thinks parents ought to want. This is not the narrow tailoring to "assisting parents" that restriction of First Amendment rights requires.

California's legislation straddles the fence between (1) addressing a serious social problem and (2) helping concerned parents control their children. Both ends are legitimate, but when they affect First Amendment rights they must be pursued by means that are neither seriously underinclusive nor seriously overinclusive. As a means of protecting children from portrayals of violence, the legislation is seriously underinclusive, not only because it excludes portrayals other than video games, but also because it permits a parental veto. And as a means of assisting concerned parents it is seriously overinclusive because it abridges the First Amendment rights of young people whose parents think violent video games are a harmless pastime. And the overbreadth in achieving one goal is not cured by the underbreadth in achieving the other.

Justice Alito, with whom The Chief Justice joins, concurring in the judgment.

The California statute represents a pioneering effort to address a potentially serious social problem. Although the statute is well intentioned, its terms are not framed with the precision that the Constitution demands, and I therefore agree that this particular law cannot be sustained.

I disagree, however, with the approach taken in the Court's opinion. In considering the application of unchanging constitutional principles to new and rapidly evolving technology, this Court should proceed with caution. We should make every effort to understand the new technology. We should take into account the possibility that developing technology may have important societal implications that will become apparent only with time. We should not jump to the conclusion that new technology is fundamentally the same as some older thing with which we are familiar. And we should not hastily dismiss the judgment of legislators, who may be in a better position than we are to assess the implications of new technology. The opinion of the Court exhibits none of this caution.

In the view of the Court, all those concerned about the effects of violent video games--federal and state legislators, educators, social scientists, and parents--are unduly fearful, for violent video games really present no serious problem. Spending hour upon hour controlling the actions of a character who guns down scores of innocent victims is not different in "kind" from reading a description of violence in a work of literature. The Court is sure of this; I am not. There are reasons to suspect that the experience of playing violent video games just might be very different from reading a book, listening to the radio, or watching a movie or a television show.

Respondents, representing the video-game industry, ask us to strike down the California law on two grounds: The broad ground adopted by the Court and the narrower ground that the law's definition of "violent video game" is impermissibly vague. Because I agree with the latter argument, I see no need to reach the broader First Amendment issues addressed by the Court.

Justice Thomas, dissenting.

The Court's decision does not comport with the original public understanding of the First Amendment. The practices and beliefs of the founding generation establish that "the freedom of speech," as originally understood, does not include a right to speak to minors (or a right of minors to access speech) without going through the minors' parents or guardians. I would hold that the law at issue is not facially unconstitutional under the First Amendment.

Justice Breyer, dissenting.

Applying traditional First Amendment analysis, I would uphold the statute as constitutional on its face and would consequently reject the industries' facial challenge.

In determining whether the statute is unconstitutional, I would apply both this Court's "vagueness" precedents and a strict form of First Amendment scrutiny. In doing so, the special First Amendment category I find relevant is not "depictions of violence," but rather the category of "protection of children." This Court has held that the " 'regulatio[n] of communication addressed to [children] need not conform to the requirements of the [F]irst [A]mendment in the same way as those applicable to adults.' " *Ginsberg v. New York*, 390 U. S. 629, 638, n. 6 (1968).

In my view, California's statute provides "fair notice of what is prohibited," and consequently it is not impermissibly vague. All that is required for vagueness purposes is that the terms "kill," "maim," and "dismember" give fair notice as to what they cover, which they do. The remainder of California's definition copies, almost word for word, the language this Court used in *Miller v. California*, 413 U. S. 15 (1973).

Both the *Miller* standard and the law upheld in *Ginsberg* lack perfect clarity. But that fact reflects the difficulty of the Court's long search for words capable of protecting expression without depriving the State of a legitimate power to regulate. As is well known, at one point Justice Stewart thought he could do no better in defining obscenity than, "I know it when I see it." And Justice Douglas dissented from *Miller's* standard, which he thought was still too vague. Ultimately, however, this Court accepted the "community standards" tests used in *Miller* and *Ginsberg*. They reflect the fact that sometimes, even when a precise standard proves elusive, they seek to draw a line, which, while favoring free expression, will nonetheless permit a legislature to find the words necessary to accomplish a legitimate objective.

What, then, is the difference between *Ginsberg* and *Miller* on the one hand and the California law on the other? It will often be easy to pick out cases at which California's statute directly aims, involving, say, a character who shoots out a police officer's knee, douses him with gasoline, lights him on fire, urinates on his burning body, and finally kills him with a gunshot to the head. As in *Miller* and *Ginsberg*, the California law clearly protects even the most violent games that possess serious literary, artistic, political, or scientific value. And it is easier here than in *Miller* or *Ginsberg* to separate the sheep from the goats at the statute's border. That is because here the industry itself has promulgated standards and created a review process, in which adults who "typically have experience with children" assess what games are inappropriate for minors.

There is, of course, one obvious difference: The *Ginsberg* statute concerned depictions of

"nudity," while California's statute concerns extremely violent video games. But for purposes of vagueness, why should that matter? The Court relied on "community standards" in *Miller* precisely because of the difficulty of articulating "accepted norms" about depictions of sex. Thus, I can find no meaningful vagueness-related differences between California's law and the law upheld in *Ginsberg*. Consequently, for purposes of this facial challenge, I would not find the statute unconstitutionally vague.

Video games combine physical action with expression. Were physical activity to predominate in a game, government could appropriately intervene, say by requiring parents to accompany children when playing a game involving actual target practice. But because video games also embody important expressive and artistic elements, I agree with the Court that the First Amendment significantly limits the State's power to regulate.

Like the majority, I believe that the California law must be "narrowly tailored" to further a "compelling interest," without there being a "less restrictive" alternative that would be "at least as effective." *Reno v. American Civil Liberties Union*, 521 U. S. 844 (1997). I would not apply this strict standard "mechanically." Rather, in applying it, I would evaluate the degree to which the statute injures speech-related interests, the nature of the potentially-justifying "compelling interests," the degree to which the statute furthers that interest, the nature and effectiveness of possible alternatives, and, in light of this evaluation, whether, overall, "the statute works speech-related harm . . . out of proportion to the benefits that the statute seeks to provide."

First Amendment standards applied in this way are difficult but not impossible to satisfy. California's law imposes no more than a modest restriction on expression. The statute prevents no one from playing a video game, it prevents no adult from buying a video game, and it prevents no child or adolescent from obtaining a game provided a parent is willing to help. All it prevents is a child or adolescent from buying, without a parent's assistance, a gruesomely violent video game of a kind that the industry itself tells us it wants to keep out of the hands of those under the age of 17. Nor is the statute, if upheld, likely to create a precedent that would adversely affect other media, say films, or videos, or books. A typical video game involves a significant amount of physical activity. And pushing buttons that achieve an interactive, virtual form of target practice (using images of human beings as targets), while containing an expressive component, is not just like watching a typical movie.

The interest that California advances in support of the statute is compelling. As this Court has previously described that interest, it consists of both (1) the "basic" parental claim "to authority in their own household to direct the rearing of their children," which makes it proper to enact "laws designed to aid discharge of [parental] responsibility," and (2) the State's "independent interest in the well-being of its youth." And where these interests work in tandem, it is not fatally "underinclusive" for a State to advance its interests in protecting children against the special harms present in an interactive video game medium through a default rule that still allows parents to provide their children with what their parents wish.

Both interests are present here. As to the State's independent interest, we have recognized "a compelling interest in protecting the physical and psychological well-being of minors." There is considerable evidence that California's statute significantly furthers this compelling interest. In

particular, extremely violent games can harm children by rewarding them for being violently aggressive in play, and thereby often teaching them to be violently aggressive in life. And video games can cause more harm in this respect than can typically passive media, such as books or films or television programs.

There are many scientific studies that support California's views. Unlike the majority, I would find sufficient grounds in these studies and expert opinions for this Court to defer to an elected legislature's conclusion that the video games in question are particularly likely to harm children. This Court has always thought it owed an elected legislature some degree of deference in respect to legislative facts of this kind, particularly when they involve technical matters that are beyond our competence, and even in First Amendment cases. The majority, in reaching its own, opposite conclusion about the validity of the relevant studies, grants the legislature no deference at all.

I can find no "less restrictive" alternative to California's law that would be "at least as effective." The majority points to a voluntary alternative: The industry tries to prevent those under 17 from buying extremely violent games by labeling those games with an "M" (Mature) and encouraging retailers to restrict their sales to those 17 and older. But this voluntary system has serious enforcement gaps. When California enacted its law, a Federal Trade Commission (FTC) study had found that nearly 70% of unaccompanied 13- to 16-year-olds were able to buy M-rated video games. Subsequently the voluntary program has become more effective. But as of the FTC's most recent update to Congress, 20% of those under 17 are still able to buy M-rated video games. And the industry could easily revert back to the substantial noncompliance that existed in 2004, particularly after today's broad ruling. The industry also argues for an alternative technological solution, namely "filtering at the console level." But it takes only a quick search of the Internet to find guides explaining how to circumvent any such technological controls.

The upshot is that California's statute, as applied to its heartland of applications (i.e., buyers under 17; extremely violent, realistic video games), imposes a restriction on speech that is modest at most. That restriction is justified by a compelling interest (supplementing parents' efforts to prevent their children from purchasing potentially harmful violent, interactive material). And there is no equally effective, less restrictive alternative. California's statute is consequently constitutional on its face.

I add that the majority's different conclusion creates a serious anomaly in First Amendment law. A State can prohibit the sale to minors of depictions of nudity; a State cannot prohibit the sale to minors of the most violent interactive video games. But what sense does it make to forbid selling to a 13-year-old boy a magazine with an image of a nude woman, while protecting a sale to that 13-year-old of an interactive video game in which he actively, but virtually, binds and gags the woman, then tortures and kills her? What kind of First Amendment would permit the government to protect children by restricting sales of that extremely violent video game only when the woman--bound, gagged, tortured, and killed--is also topless?

This anomaly is not compelled by the First Amendment. It disappears once one recognizes that extreme violence, where interactive, and without literary, artistic, or similar justification, can prove at least as, if not more, harmful to children as photographs of nudity. That is why I believe that California's law is constitutional on its face.

KOWALSKI v. BERKELEY COUNTY SCHOOLS
652 F.3d 565 (4th Cir. 2011), *cert. denied*, 80 U.S.L.W. 3427 (2012)

NIEMEYER, Circuit Judge:

When Kara Kowalski was a senior at Musselman High School in Berkeley County, West Virginia, school administrators suspended her from school for five days for creating and posting to a MySpace.com webpage called "S.A.S.H.," which Kowalski claims stood for "Students Against Sluts Herpes" and which was largely dedicated to ridiculing a fellow student. Kowalski commenced this action, under 42 U.S.C. § 1983, against the Berkeley County School District and five of its officers, contending that in disciplining her, the defendants violated her free speech and due process rights under the First and Fourteenth Amendments. She alleges, among other things, that the School District was not justified in regulating her speech because it did not occur during a "school-related activity," but rather was "private out-of-school speech."

The district court entered summary judgment in favor of the defendants. Reviewing the summary judgment record *de novo*, we conclude that the School District's imposition of sanctions was permissible. Kowalski used the Internet to orchestrate a targeted attack on a classmate, and did so in a manner that was sufficiently connected to the school environment as to implicate the School District's recognized authority to discipline speech which "materially and substantially interfere[es] with the requirements of appropriate discipline in the operation of the school and collid[es] with the rights of others." *Tinker v. Des Moines Indep. Community Sch. Dist*., 393 U.S. 503, 513 (1969). Accordingly, we affirm.

I

On December 1, 2005, Kara Kowalski, who was then a 12th grade student at Musselman High School in the Berkeley County School District, returned home from school and, using her home computer, created a discussion group webpage on MySpace.com with the heading "S.A.S.H." Under the webpage's title, she posted the statement, "No No Herpes, We don't want no herpes." Kowalski claimed in her deposition that "S.A.S.H." was an acronym for "Students Against Sluts Herpes," but a classmate, Ray Parsons, stated that it was an acronym for "Students Against Shay's Herpes," referring to another Musselman High School Student, Shay N., who was the main subject of discussion on the webpage.

After creating the group, Kowalski invited approximately 100 people on her MySpace "friends" list to join the group. Approximately two dozen Musselman High School students responded and joined the group. Kowalski later explained that she had hoped that the group would "make other students actively aware of STDs," which were a "hot topic" at her school.

Ray Parsons responded to the MySpace invitation at 3:40 p.m. and was the first to join the group, doing so from a school computer during an after hours class at Musselman High School. Parsons uploaded a photograph of himself and a friend holding their noses while displaying a sign that read, "Shay Has Herpes," referring to Shay N. The record of the webpage shows that Kowalski promptly responded, stating, "Ray you are soo funny!=)." It shows that shortly thereafter, she posted another response to the photograph, stating that it was "the best picture [I]'ve seen on myspace so far! ! ! !" Several other students posted similar replies. Parsons also

uploaded to the "S.A.S.H." webpage two additional photographs of Shay N., which he edited. In the first, he had drawn red dots on Shay N.'s face to simulate herpes and added a sign near her pelvic region, that read, "Warning: Enter at your own risk." In the second photograph, he captioned Shay N.'s face with a sign that read, "portrait of a whore."

The commentary posted on the "S.A.S.H." webpage mostly focused on Shay N. The first five comments were posted by other Musselman High School students and ridiculed the pictures of Shay N. One student stated that "shay knows about the sign" and then stated, "wait til she sees the page lol." The next comment replied, "Haha.. screw her" and repeatedly stated, "This is great." After expressing her approval of the postings, this student noted the "Shay has herpes sign" and stated, "Kara sent me a few interesting pics. . . Would you be interested in seeing them Ray?" One student posted, "Kara= My Hero," and another said, "your so awesome kara...i never thought u would mastermind a group that hates [someone] tho, lol." A few of the posts assumed that Kowalski had posted the photographs of Shay N., but Parsons later clarified that it was he who had posted the photographs.

A few hours after the photographs and comments had been posted to the MySpace.com page, Shay N.'s father called Parsons on the telephone and expressed his anger over the photographs. Parsons then called Kowalski, who unsuccessfully attempted to delete the "S.A.S.H." group and to remove the photographs. Unable to do so, she renamed the group "Students Against Angry People."

The next morning, Shay N.'s parents, together with Shay, went to Musselman High School and filed a harassment complaint with Vice Principal Becky Harden regarding the discussion group, and they provided Harden with a printout of the "S.A.S.H." webpage. Shay thereafter left the school with her parents, as she did not want to attend classes that day, feeling uncomfortable about sitting in class with students who had posted comments about her on MySpace.

After receiving Shay N.'s complaint, Principal Ronald Stephens contacted the central school board office to determine whether the issue was one that should be addressed with school discipline. A school board official indicated that discipline was appropriate. Principal Stephens then conducted an investigation into the matter. As part of the investigation, Principal Stephens and Vice Principal Harden questioned Parsons, who admitted that he had posted the photographs. Vice Principal Harden met with Kowalski, who admitted that she had created the "S.A.S.H." group but denied that she posted any of the photographs or disparaging remarks.

School administrators concluded that Kowalski had created a "hate website," in violation of the school policy against "harassment, bullying, and intimidation." For punishment, they suspended Kowalski from school for 10 days and issued her a 90-day "social suspension," which prevented her from attending school events in which she was not a direct participant. Kowalski was also prevented from crowning the next "Queen of Charm" in that year's Charm Review, having been elected "Queen" herself the previous year. In addition, she was not allowed to participate on the cheerleading squad for the remainder of the year. After Kowalski's father asked school administrators to reduce or revoke the suspension, Assistant Superintendent Deuell reduced Kowalski's out-of-school suspension to 5 days, but retained the 90-day social suspension. Kowalski commenced this action in November 2007.

II

Kowalski contends that the school administrators violated her free speech rights by punishing her for speech that occurred outside the school. She argues that because this case involved "off-campus, non-school related speech," school administrators had no power to discipline her. As she asserts, "The [Supreme] Court has been careful to limit intrusions on students' rights to conduct taking place on school property, at school functions, or while engaged in school-sponsored or school-sanctioned activity." She maintains that "no Supreme Court case addressing student speech has held that a school may punish students for speech away from school--indeed every Supreme Court case addressing student speech has taken pains to emphasize that, were the speech in question to occur away from school, it would be protected."

The Berkeley County School District and its administrators contend that school officials "may regulate off-campus behavior insofar as the off-campus behavior creates a foreseeable risk of reaching school property and causing a substantial disruption to the work and discipline of the school," citing *Doninger v. Niehoff*, 527 F.3d 41 (2d Cir. 2008). Relying on *Doninger*, the defendants note that Kowalski created a webpage that singled out Shay N. for harassment, bullying and intimidation; that it was foreseeable that the off-campus conduct would reach the school; and that it was foreseeable that the off-campus conduct would "create a substantial disruption in the school."

The question thus presented is whether Kowalski's activity fell within the outer boundaries of the high school's legitimate interest in maintaining order in the school and protecting the well-being and educational rights of its students.

The First Amendment prohibits Congress and, through the Fourteenth Amendment, the States from "abridging the freedom of speech." It is a "bedrock principle" of the First Amendment that "the government may not prohibit the expression of an idea simply because society finds the idea offensive or disagreeable." *Texas v. Johnson*, 491 U.S. 397, 414 (1989).

While students retain significant First Amendment rights in the school context, their rights are not coextensive with those of adults. *See Tinker v. Des Moines Indep. Community Sch. Dist*., 393 U.S. 503, 506 (1969). Because of the "special characteristics of the school environment," school administrators have some latitude in regulating student speech to further educational objectives. Thus in *Tinker*, the Court held that student speech, consisting of wearing armbands in political protest against the Vietnam War, was protected because it did not "'materially and substantially interfer[e] with the requirements of appropriate discipline in the operation of the school' [or] collid[e] with the rights of others," and thus did not "materially disrupt[ ] classwork or involve[ ] substantial disorder or invasion of the rights of others." Student speech also may be regulated if it is "vulgar and lewd." *See Bethel Sch. Dist. No. 403 v. Fraser*, 478 U.S. 675 (1986). Finally, the Supreme Court has held that school administrators are free to regulate and punish student speech that encourages the use of illegal drugs. *Morse v. Frederick*, 551 U.S. 393 (2007).

Although the Supreme Court has not dealt specifically with a factual circumstance where student speech targeted classmates for verbal abuse, in *Tinker* it recognized the need for regulation of speech that interfered with the school's work and discipline, describing that interference as speech that "disrupts classwork," creates "substantial disorder," or "collid[es]

with" or "inva[des]" "the rights of others." *Tinker*, 393 U.S. at 513.

In *Tinker*, the Court pointed out how wearing black armbands was passive and did not create "disorder or disturbance" and therefore did not interfere with the school's work or collide with other students' rights "to be secure and to be let alone." Of course, a mere desire to avoid "discomfort and unpleasantness" was an insufficient basis to regulate the speech; there had to be disruption in the sense that the speech "would materially and substantially interfere with the requirements of appropriate discipline in the operation of the school." The Court amplified the nature of the disruption it had in mind when it stated:

> [C]onduct by [a] student, in class or out of it, which for any reason--whether it stems from time, place, or type of behavior--materially disrupts classwork or involves substantial disorder or invasion of the rights of others is, of course, not immunized by the constitutional guarantee of freedom of speech.

The *Tinker* Court referred to this amplified statement of its test later in its opinion when it concluded that the regulation of armbands "would violate the constitutional rights of students, at least if it could not be justified by a showing that the students' activities would materially and substantially disrupt *the work and discipline of the school*." Because wearing armbands "neither interrupted school activities nor sought to intrude in the school affairs or the lives of others," there was "no interference with work and no disorder" to justify regulation of the speech.

Thus, the language of *Tinker* supports the conclusion that public schools have a "compelling interest" in regulating speech that interferes with or disrupts the work and discipline of the school, including discipline for student harassment and bullying.

According to a federal government initiative, student-on-student bullying is a "major concern" in schools across the country and can cause victims to become depressed and anxious, to be afraid to go to school, and to have thoughts of suicide. *See* StopBullying.gov. Just as schools have a responsibility to provide a safe environment for students free from messages advocating illegal drug use, schools have a duty to protect their students from harassment and bullying in the school environment. Far from being a situation where school authorities "suppress speech on political and social issues based on disagreement with the viewpoint expressed," school administrators must be able to prevent and punish harassment and bullying in order to provide a safe school environment conducive to learning.

We are confident that Kowalski's speech caused the interference and disruption described in *Tinker*. The "S.A.S.H." webpage functioned as a platform for Kowalski and her friends to direct verbal attacks towards classmate Shay N. The webpage contained comments accusing Shay N. of having herpes and being a "slut," as well as photographs reinforcing those defamatory accusations by depicting a sign across her pelvic area, which stated, "Warning: Enter at your own risk" and labeling her portrait as that of a "whore." One student's posting dismissed any concern for Shay N.'s reaction with a comment that said, "screw her." This is not the conduct and speech that our educational system is required to tolerate, as schools attempt to educate students about "habits and manners of civility" or the "fundamental values necessary to the maintenance of a democratic political system." *Fraser*, 478 U.S. at 681.

While Kowalski does not seriously dispute the harassing character of the speech on the

"S.A.S.H." webpage, she argues mainly that her conduct took place at home after school and that the forum she created was therefore subject to the full protection of the First Amendment. This argument, however, raises the metaphysical question of where her speech occurred when she used the Internet as the medium. Kowalski indeed pushed her computer's keys in her home, but she knew that the electronic response would be, as it in fact was, published beyond her home and could reasonably be expected to reach the school or impact the school environment. She also knew that the dialogue would and did take place among Musselman High School students whom she invited to join the "S.A.S.H." group and that the fallout from her conduct and the speech within the group would be felt in the school itself. Indeed, the group's name was "*Students* Against Sluts Herpes" and a vast majority of its members were Musselman students. As one commentator on the webpage observed, "wait til [Shay N.] sees the page lol." Moreover, as Kowalski could anticipate, Shay N. and her parents took the attack as having been made in the school context, as they went to the high school to lodge their complaint.

There is surely a limit to the scope of a high school's interest in the order, safety, and well-being of its students when the speech at issue originates outside the schoolhouse gate. But we need not fully define that limit here, as we are satisfied that the nexus of Kowalski's speech to Musselman High School's pedagogical interests was sufficiently strong to justify the action taken by school officials in carrying out their role as the trustees of the student body's well-being.

Of course, had Kowalski created the "S.A.S.H." group during school hours, using a school-provided computer and Internet connection, this case would be more clear-cut, as the question of where speech that was transmitted by the Internet "occurred" would not come into play. To be sure, a court could determine that speech originating outside of the schoolhouse gate but directed at persons in school and received by and acted on by them was in fact in-school speech. In that case, because it was determined to be in-school speech, its regulation would be permissible not only under *Tinker* but also, as vulgar and lewd in-school speech, under *Fraser. See Fraser*, 478 U.S. at 685. *But cf. Layshock v. Hermitage Sch. Dist*., 650 F.3d 205 (3d Cir. 2011) (en banc) (holding that a school could not punish a student for online speech merely because the speech was vulgar and reached the school). We need not resolve, however, whether this was in-school speech and therefore whether *Fraser* could apply because the School District was authorized by *Tinker* to discipline Kowalski, regardless of where her speech originated, because the speech was materially and substantially disruptive in that it "interfer[ed] . . . with the schools' work [and] colli[ded] with the rights of other students to be secure and to be let alone."

Given the targeted, defamatory nature of Kowalski's speech, aimed at a fellow classmate, it created "actual or nascent" substantial disorder and disruption in the school. *See Tinker*, 393 U.S. at 508, 513. First, the creation of the "S.A.S.H." group forced Shay N. to miss school in order to avoid further abuse. Moreover, had the school not intervened, the potential for continuing and more serious harassment of Shay N. as well as other students was real. Experience suggests that unpunished misbehavior can have a snowballing effect, in some cases resulting in "copycat" efforts by other students or in retaliation for the initial harassment.

Other courts have similarly concluded that school administrators' authority to regulate student speech extends, in appropriate circumstances, to speech that does not originate at the school itself, so long as the speech eventually makes its way to the school in a meaningful way. Thus,

even though Kowalski was not physically at school when she operated her computer to create the webpage and form the MySpace group and to post comments there, it was foreseeable that Kowalski's conduct would reach the school via computers, smartphones, and other electronic devices, given that most of the "S.A.S.H." group's members and the target of the group's harassment were Musselman High School students. Indeed, the "S.A.S.H." webpage did make its way into the school and was accessed first by Musselman student Ray Parsons at 3:40 p.m., from a school computer during an after hours class. Furthermore, as we have noted, it created a reasonably foreseeable substantial disruption there. At bottom, we conclude that the school was authorized to discipline Kowalski because her speech interfered with the work and discipline of the school.

Kowalski's role in the "S.A.S.H." webpage, which was used to ridicule and demean a fellow student, was particularly mean-spirited and hateful. The webpage called on classmates, in a pack, to target Shay N., knowing that it would be hurtful and damaging to her ability to sit with other students in class and have a suitable learning experience. While each student in the "S.A.S.H." group might later attempt to minimize his or her role, at bottom, the conduct was indisputably harassing and bullying, in violation of Musselman High School's regulations.

Kowalski asserts that the protection of free speech insulate her activities from school discipline because her activity was not sufficiently school-related to be subject to school discipline. Yet, every aspect of the webpage's design and implementation was school-related. Kowalski designed the website for "students;" she sent it to students inviting them to join; and those who joined were mostly students. The victim understood the attack as school-related, filing her complaint with school authorities. Ray Parsons, who provided the vulgar and lewd photographs understood that the object of the attack was Shay N., and he participated from a school computer during class, to the cheering of Kowalski and her fellow classmates.

Rather than respond constructively to the school's efforts to bring order and provide a lesson following the incident, Kowalski has rejected those efforts and sued school authorities for damages and other relief. Regretfully, she yet fails to see that such harassment and bullying is inappropriate and hurtful and that it must be taken seriously by school administrators in order to preserve an appropriate pedagogical environment. Suffice it to hold that, where such speech has a sufficient nexus with the school, the Constitution is not written to hinder school administrators' good faith efforts to address the problem. The judgment of the district court is *AFFIRMED*.

OSTERGREN v. CUCCINELLI

615 F.3d 263 (4th Cir. 2010)

DUNCAN, Circuit Judge:

This appeal arises from a First Amendment challenge to Virginia's Personal Information Privacy Act, Va. Code §§ 59.1-442 to -444. Section 59.1-443.2 prohibits "[i]ntentionally communicat[ing] another individual's social security number to the general public." The district court found this section unconstitutional as applied to an advocacy website that criticized Virginia's release of private information and showed publicly available Virginia land records

containing unredacted Social Security numbers ("SSNs"). For the reasons that follow, we affirm.

I.

Betty Ostergren resides in Hanover County, Virginia, and advocates for information privacy across the country. Calling attention to Virginia's practice of placing land records on the Internet without first redacting SSNs, she displayed copies of Virginia land records containing unredacted SSNs on her website. After section 59.1-443.2 was amended to prohibit this practice, but before the amendment took effect, Ostergren brought this constitutional challenge.

A.

The clerk of court for each county in Virginia maintains documents affecting real property within the county. These "land records" reflect the ownership, conveyance, encumbrance, or financing of real property. Virginia law requires that clerks make land records available for public inspection. Any person can review and copy land records by visiting the courthouse and requesting them.

During the 1990s, many clerks of court began placing land records on the Internet. The impetus came mainly from the real estate industry. The Virginia General Assembly encouraged this practice by allowing clerks to charge a fee for online access. In 2007, the General Assembly imposed guidelines for posting land records online, and required that "[e]very circuit court clerk shall provide secure remote access to land records . . . on or before July 1, 2008."

The parties stipulated that "[u]nder Virginia's 'secure remote access' system, any person may, for a nominal fee, obtain online access to all of the land records for a given locality." Guidelines require that an individual must register and obtain a username and password before using the system. This involves signing an agreement, paying a fee (possibly several hundred dollars per year), and providing certain personal information (first and last names, business name, mailing address, telephone number, email address, and citizenship status).

By July 2008, every county in Virginia had made its land records available on the Internet through secure remote access. This included over 200 million Virginia land records.

B.

Virginia's decision to place land records online raised certain concerns about information privacy. For many decades, attorneys included SSNs on real estate documents submitted for recording. When clerks of court began placing land records online, they did nothing to redact SSNs. At that time, Virginia law neither required such redaction nor prevented attorneys from submitting documents for recording that contained unredacted SSNs. In 2003 and 2004, however, the General Assembly provided that "clerk[s] may refuse to accept any instrument submitted for recordation that includes a grantor's, grantee's or trustee's social security number."

The General Assembly finally addressed redaction in the 2007 legislation mandating that clerks provide secure remote access by July 1, 2008. The General Assembly noted clerks' authority to redact SSNs from digital land records available through secure remote access, authorized hiring private vendors to run redaction software, and authorized using Technology Trust Fund money for this purpose. The legislation would have also required clerks to complete

the redaction process by July 1, 2010, but this provision never went into effect. These efforts focused solely on digital land records available online. Virginia does not redact SSNs from original land records maintained at local courthouses even though Virginia law requires that such records remain publicly accessible.

The redaction process involves two steps--one electronic, the other manual. First, computer software checks digital land records and, in essence, labels each document "SSN found," "SSN probably found," "SSN possibly found," and "SSN not found." Individuals then manually review all but the last category, which they randomly sample. According to stipulation,

> The accuracy of the redaction methods used by the circuit court clerks with regard to images that actually have social security numbers is between 95% and 99%. After redaction, a social security number that remains un-redacted in the online land records will be redacted if the Clerk is informed of the inaccuracy. If not brought to the Clerk's attention, it will remain accessible in the online land records.

One company, Computing System Innovations ("CSI"), handled redaction for 67 counties. In processing about 50 million images, CSI manually reviewed about 5 million and discovered that 1,575,422 (about 3.21%) contained SSNs.

By July 2008, 105 of Virginia's 120 counties reported that they had completed the redaction process. Among the 15 that remained, two planned to finish by July 2010 and the rest planned to finish by December 2009. Despite the incomplete redaction, these 15 counties nonetheless continued to make their land records available online through secure remote access.

C.

When Virginia clerks of court started placing land records containing unredacted SSNs online, Ostergren began lobbying the General Assembly in opposition and contacting individuals whose SSNs were compromised. She has engaged in similar advocacy across the country, but such advocacy alone met with little success. Ostergren created her website www.TheVirginiaWatchdog.com in 2003 and, two years later, began posting copies of public records containing unredacted SSNs obtained from government websites. Since then, Ostergren has posted numerous Virginia land records showing SSNs that she herself obtained through Virginia's secure remote access website.

In posting records online, Ostergren seeks to publicize her message that governments are mishandling SSNs and generate pressure for reform. She explained that "seeing a document containing an SSN posted on my website makes a viewer understand instantly, at a gut level, why it is so important to prevent the government from making this information available on line." She added that merely explaining the problem lacks even "one-tenth the emotional impact that is conveyed by the document itself, posted on the website." Perhaps for this reason, Ostergren received considerable media attention when she began posting records online. Furthermore, many government agencies outside Virginia responded by removing public records from the Internet or redacting private information.

Despite this success, Ostergren's website has also contributed to the underlying social concern that motivates her advocacy. Because one can visit her website and find public records

showing SSNs without needing to register or input search terms, Ostergren makes Virginia land records showing SSNs more accessible to the public than they are through Virginia's secure remote access system. Indeed, one person has pleaded guilty to using Ostergren's website to obtain fraudulent credit cards.

D.

The controversy that spurred this case arose from Ostergren's disclosure of others' SSNs printed in Virginia land records that she posted online. Section 59.1-443.2 of the Code of Virginia provides that "a person shall not . . . [i]ntentionally communicate another individual's social security number to the general public." In Spring 2008, the General Assembly removed a statutory exception for "records required by law to be open to the public." The Attorney General of Virginia later indicated that, after this change took effect on July 1, 2008, Ostergren would be prosecuted under section 59.1-443.2 for publicly disseminating Virginia land records containing unredacted SSNs.

On June 11, 2008, Ostergren brought this action. She contended that enforcing section 59.1-443.2 against her for publishing copies of public records lawfully obtained from a government website violates the First Amendment. On August 22, 2008, the district court concluded that "Virginia Code § 59.1-443.2 is unconstitutional as applied to Ostergren's website as it presently exists." The Attorney General appealed, challenging the district court's determination.

II.

First we review the district court's August 22, 2008, constitutional determination. Virginia argues that SSNs are unprotected speech that may be prohibited entirely. Alternatively, Virginia argues that the state interest in preserving citizens' privacy by limiting SSNs' public disclosure justifies barring Ostergren's speech. We address each argument in turn.

A.

The First Amendment's protection of "freedom of speech, or of the press," was designed to allow individuals to criticize their government without fear. This protection also precludes the government from silencing the expression of unpopular ideas. Accordingly, laws restricting the content of expression normally are invalid under the First Amendment unless narrowly tailored to promote a compelling state interest.

The Supreme Court has nevertheless identified certain categories of "unprotected" speech that may be circumscribed entirely. Fighting words, obscenity, incitement of illegal activity, and child pornography are examples. The Court has said that these categories of unprotected speech "are no essential part of any exposition of ideas, and are of such slight social value as a step to truth that any benefit that may be derived from them is clearly outweighed by the social interest in order and morality."

Virginia argues that the unredacted SSNs on Ostergren's website should not be protected under the First Amendment because they facilitate identity theft and are no essential part of any exposition of ideas. *See* Eugene Volokh, *Crime-Facilitating Speech*, 57 Stan. L. Rev. 1095, 1146-47 (2005) (arguing that SSNs and computer passwords are "likely to have virtually no noncriminal uses" and that "[r]estricting the publication of full social security numbers or

passwords . . . will not materially interfere with valuable speech"). Although these observations might be true under certain circumstances, we cannot agree with Virginia's argument here. The unredacted SSNs on Virginia land records that Ostergren has posted online are integral to her message. Indeed, they *are* her message. Displaying them proves Virginia's failure to safeguard private information and powerfully demonstrates why Virginia citizens should be concerned.[1]

We find particularly significant just how Ostergren communicates SSNs. She does not simply list them beside people's names but rather provides copies of entire documents maintained by government officials. Given her criticism about how public records are managed, we cannot see how drawing attention to the problem by displaying those very documents could be considered unprotected speech. Indeed, the Supreme Court has deemed such speech particularly valuable within our society:

> Public records by their very nature are of interest to those concerned with the administration of government, and a public benefit is performed by the reporting of the true contents of the records by the media. The freedom of the press to publish that information appears to us to be of critical importance to our type of government in which the citizenry is the final judge of the proper conduct of public business.

Thus, although we do not foreclose the possibility that communicating SSNs might be found unprotected in other situations, we conclude, on these facts, that the First Amendment does reach Ostergren's publication of Virginia land records containing unredacted SSNs.

B.

We next consider whether enforcing section 59.1-443.2 against Ostergren for posting online Virginia land records containing unredacted SSNs survives First Amendment scrutiny. Although Ostergren's political speech criticizing Virginia "lies at the very center of the First Amendment," publishing SSNs online undermines individual privacy. Freedom of speech must therefore be weighed against the "right of privacy" which the Supreme Court has also recognized. The Court tried to strike that balance in *Cox Broadcasting Corp. v. Cohn*, 420 U.S. 469 (1975), and subsequent cases involving restrictions on truthful publication of private information. Because we must decide where this case fits within that balance, we begin our analysis by reviewing those decisions.

In *Cox Broadcasting*, the Supreme Court ruled that the First Amendment prohibits a lawsuit against a television station for broadcasting a rape victim's name when the station learned her identity from a publicly available court record. The Court reasoned that "the interests in privacy fade when the information involved already appears on the public record." The Court observed that "[b]y placing the information in the public domain on official court records, the State must

---

[1] Virginia argues that Ostergren could redact several digits from each SSN and still express her message. But the First Amendment protects Ostergren's freedom to decide how her message should be communicated. *Cohen v. California*, 403 U.S. 15, 24 (1971). Furthermore, partial redaction would diminish the documents' shock value and make Ostergren less credible because people could not tell whether she or Virginia did the partial redaction.

be presumed to have concluded that the public interest was thereby being served." The Court also discussed the importance of truthful reporting about public records and expressed reluctance to create a doctrine that "would invite timidity and self-censorship and very likely lead to the suppression of many items that should be made available to the public." The Court concluded:

> At the very least, the First and Fourteenth Amendments will not allow exposing the press to liability for truthfully publishing information released to the public in official court records. Once true information is disclosed in public court documents open to public inspection, the press cannot be sanctioned for publishing it.

The Court explained that "[i]f there are privacy interests to be protected in judicial proceedings, the States must respond by means which avoid public documentation or other exposure of private information."

Although *Cox Broadcasting* avoided deciding whether truthful publication may ever be punished, subsequent cases helped to clarify the relevant inquiry. In *Oklahoma Publishing Co. v. District Court*, 430 U.S. 308 (1977), the Supreme Court held that a trial court could not bar newspapers from publishing a juvenile offender's name learned during a court proceeding open to the public. In *Landmark Communications, Inc. v. Virginia*, 435 U.S. 829 (1978), the Court held that Virginia could not punish a newspaper for publishing correct information that had been leaked about confidential proceedings by the Virginia Judicial Inquiry and Review Commission. The Court reasoned that Virginia's interests in preserving respect for courts and protecting individual judges' reputations did not justify prohibiting speech that "clearly served those interests in public scrutiny and discussion of governmental affairs which the First Amendment was adopted to protect."

The Supreme Court later articulated a constitutional standard based upon these decisions. In *Smith v. Daily Mail Publishing Co*., 443 U.S. 97 (1979), the Court observed that *Cox Broadcasting, Oklahoma Publishing*, and *Landmark Communications* "all suggest strongly that if a newspaper lawfully obtains truthful information about a matter of public significance then state officials may not constitutionally punish publication of the information, absent a need to further a state interest of the highest order."

After this flurry of decisions, the Supreme Court applied the *Daily Mail* standard roughly a decade later in another case about a rape victim. In *The Florida Star v. B.J.F*., 491 U.S. 524 (1989), the appellee B.J.F. reported to local police that she had been robbed and sexually assaulted. Despite its internal policy against revealing names of rape victims, the police department inadvertently placed a police report containing B.J.F.'s name in its press room. After a reporter copied the police report verbatim, an area newspaper published an article containing B.J.F.'s full name. She sued for money damages, claiming the newspaper had been per se negligent. The jury awarded damages and a Florida appellate court affirmed.

The Supreme Court reversed. Before applying the *Daily Mail* standard regarding truthful publication of lawfully obtained information, the Court noted three underlying considerations that justified this analytical approach. First, that the standard covers only lawfully obtained information means that the government retains ample means of protecting interests that might be threatened by publication. This consideration has additional implications when the government

itself initially holds the information:

> To the extent sensitive information is in the government's custody, it has even greater power to forestall or mitigate the injury caused by its release. The government may classify certain information, establish and enforce procedures ensuring its redacted release, and extend a damages remedy against the government or its officials where the government's mishandling of sensitive information leads to its dissemination. Where information is entrusted to the government, a less drastic means than punishing truthful publication almost always exists for guarding against the dissemination of private facts.

Second, "punishing the press for its dissemination of information which is already publicly available is relatively unlikely to advance the interests in the service of which the State seeks to act." The Court added that "where the government has made certain information publicly available, it is highly anomalous to sanction persons other than the source of its release." Third, "'timidity and self-censorship' . . . may result from allowing the media to be punished for publishing certain truthful information." Having reiterated these considerations, the Court endorsed the *Daily Mail* standard: "We hold . . . that where a newspaper publishes truthful information which it has lawfully obtained, punishment may lawfully be imposed, if at all, only when narrowly tailored to a state interest of the highest order."

Applying this standard, the Supreme Court found that the newspaper truthfully published lawfully obtained information about a matter of public significance. The Court also found that punishing the newspaper was not narrowly tailored to Florida's interest in preserving rape victims' privacy because the police department itself could have initially withheld the sensitive information. That the department's disclosure was actually inadvertent was immaterial. The Court concluded: "Where, as here, the government has failed to police itself in disseminating information, it is clear that the imposition of damages against the press for its subsequent publication can hardly be said to be a narrowly tailored means of safeguarding anonymity."

Notably, *Cox Broadcasting* and its progeny avoided deciding the ultimate question of whether truthful publication could ever be prohibited. Each decision resolved this ongoing conflict between privacy and the First Amendment "only as it arose in a discrete factual context."

Those decisions nonetheless make clear that Ostergren's constitutional challenge must be evaluated using the *Daily Mail* standard.[2] Accordingly, Virginia may enforce section 59.1-443.2 against Ostergren for publishing lawfully obtained, truthful information about a matter of public significance "only when narrowly tailored to a state interest of the highest order." Virginia concedes that Ostergren lawfully obtained and truthfully published the Virginia land records that she posted online. Moreover, this information plainly concerns "a matter of public significance" because displaying the contents of public records and criticizing Virginia's release of private information convey political messages that concern the public. Therefore, the only remaining

---

[2] Counsel for the Attorney General conceded during oral argument that, under this standard, Ostergren's advocacy website cannot be distinguished from a television station or newspaper.

issues are (1) whether Virginia has asserted a state interest of the highest order and (2) whether enforcing section 59.1-443.2 against Ostergren would be narrowly tailored to that interest.

1.

Virginia asserts that its interest in protecting privacy by limiting SSNs' public disclosure constitutes "a state interest of the highest order." Before discussing this issue, we address the proper analytical framework for determining what constitutes a state interest of the highest order.

In deciding what constitutes a state interest of the highest order, courts cannot be bound by "the State's view and its conduct." Furthermore, Supreme Court precedent applying the *Daily Mail* standard makes clear that objective criteria can be considered when deciding what constitutes a state interest of the highest order.

We find it helpful to place our inquiry in historical context by discussing the genesis of modern privacy concerns surrounding SSNs. The Social Security Administration created SSNs in 1936 merely to track individuals' earnings and eligibility for Social Security benefits. They soon became used for other purposes, however, because SSNs provide unique permanent identification for almost every person. Countless state and federal agencies adopted the SSN. For example, Congress authorized the Internal Revenue Service to begin using the SSN for taxpayer identification in 1961. Private organizations, especially financial institutions, also started using the SSN for account identification and other purposes.

Public concern about information privacy, however, soon increased. In 1973, the Department of Health, Education, and Welfare published an influential report warning about "an increasing tendency for the Social Security number to be used as if it were an SUI [standard universal identifier]." Congress responded by enacting the Privacy Act of 1974 which prohibits government agencies from denying rights, privileges, or benefits because a person withholds his SSN. By enacting this statute, "Congress sought to curtail the expanding use of social security numbers by federal and local agencies and, by so doing, to eliminate the threat to individual privacy and confidentiality of information posed by common numerical identifiers."

Since then, usage of SSNs by federal and local agencies, financial institutions, and other organizations has become nearly ubiquitous. The SSN has become a crucial piece of information allowing the creation or modification of myriad personal accounts. Unfortunately, for that reason, SSNs can easily be used to commit identity theft. One therefore has a considerable privacy interest in keeping his SSN confidential.

We previously considered this privacy interest in *Greidinger v. Davis*, 988 F.2d 1344 (4th Cir. 1993):

> Since the passage of the Privacy Act, an individual's concern over his SSN's confidentiality and misuse has become significantly more compelling. For example, armed with one's SSN, an unscrupulous individual could obtain a person's welfare benefits or Social Security benefits, order new checks at a new address on that person's checking account, obtain credit cards, or even obtain the person's paycheck.

On average, victims of identity theft lose about $ 17,000 and must spend over $ 1,000 and 600 hours of personal time cleaning up their credit reports.

Reflecting these concerns, Congress and all 50 States have passed laws regulating SSN collection and disclosure. Although not dispositive, these practices indicate a broad consensus that SSNs' public disclosure should be strictly curtailed.

Given the serious privacy concerns and potential harm stemming from SSN dissemination, Virginia's asserted interest in protecting individual privacy by limiting SSNs' public disclosure may certainly constitute "a state interest of the highest order." We need not ultimately decide that question, however, because our holding below regarding narrow-tailoring suffices to resolve the constitutional challenge.

2.

We next consider whether enforcing section 59.1-443.2 against Ostergren would be narrowly tailored to Virginia's asserted interest in preserving individual privacy. Supreme Court precedent imposes a stringent standard regarding narrow-tailoring. *Cox Broadcasting* and its progeny indicate that punishing truthful publication of private information will almost never be narrowly tailored to safeguard privacy when the government itself released that information to the press. Even where disclosure to the press was accidental, *Florida Star* indicates that the press cannot be prevented from publishing the private information.

In both *Cox Broadcasting* and *Florida Star*, the government disclosed private information to the press and thereafter sought to prevent media outlets from truthfully publishing that information. This case appears similar in that Virginia likewise disclosed public records containing private information to Ostergren and now seeks to prevent her from publishing them online. Because Virginia "failed to police itself in disseminating information," *Cox Broadcasting* and *Florida Star* suggest that preventing Ostergren from publishing those records could almost never be narrowly tailored. According to their stringent standard, Ostergren could never be prohibited from publicizing SSN-containing Virginia land records she already lawfully obtained (including those posted on her website), and Virginia would need to redact all original land records available from courthouses (not merely digital copies available through secure remote access) before Ostergren could be prohibited from publishing SSN-containing Virginia land records she might later obtain.

Despite apparent similarities, however, the instant case also differs from *Cox Broadcasting* and *Florida Star* in two critical respects that impact our narrow-tailoring analysis. First, this case implicates a different conception of privacy--one predicated upon control of personal information rather than secrecy. Second, Virginia's knowledge about and practical control over the private information here differs significantly from *Cox Broadcasting* and *Florida Star*. Given these differences, this case requires a more nuanced analysis. We consider each difference separately below and then discuss the proper narrow-tailoring analysis.

Cox Broadcasting and *Florida Star* involved a particular conception of privacy whereby "private" matters are those one would prefer to keep hidden from other people because disclosure would be embarrassing or compromising. Under this conception, one's privacy interest hinges upon whether information has been kept secret, and protecting privacy involves ensuring that people can keep personal matters secret or hidden from public scrutiny. Because this conception of privacy presupposes secrecy, personal matters that have been publicly disclosed can no longer

be considered private.

The instant case involves a different conception of privacy not predicated upon secrecy. *Cox Broadcasting* and *Florida Star* addressed the privacy concern that disclosing certain personal matters (information one had hoped to keep secret) might cause embarrassment or reputational damage. But people do not feel embarrassed when asked to provide their SSN; nor do they fear that their reputation will suffer when others find out that number. People worry only about how their SSN will be used--more specifically, about whether some unscrupulous person will steal their identity. Accordingly, this case involves a particular conception of privacy whereby one does not mind publicity itself but nonetheless would prefer to control how personal information will be used or handled. Under this conception, privacy does not hinge upon secrecy but instead involves "the individual's *control* of information concerning his or her person."

This difference affects our narrow-tailoring analysis because *Cox Broadcasting's* holding stemmed from the conception of privacy predicated upon secrecy. The Supreme Court concluded that "the interests in privacy fade when the information involved already appears on the public record." This makes sense where privacy hinges upon secrecy because publicly accessible information could not be considered private anymore. But the reasoning makes noticeably less sense where privacy hinges upon control. Whereas emotional distress resulting from disclosure occurs only once when one discovers the publicity, publicly accessible SSNs could be misused repeatedly over time until they become less easily accessed. Furthermore, because SSNs are more easily accessed online than in bound original land records, people worried about preventing identity theft would have a considerable privacy interest against "giv[ing] further publicity."

The instant case also differs in another respect from *Cox Broadcasting* and *Florida Star* regarding narrow-tailoring. There, the Supreme Court held that punishing truthful publication of private information was not narrowly tailored because the government could have initially refused to disclose that information to the press. This rationale assumes that the government could have easily prevented initial disclosure. That assumption does not fully apply in this case.

Both *Cox Broadcasting* and *Florida Star* involved situations in which a government employee created the document containing sensitive information that was later disclosed. Thus, initial disclosure could have been avoided by not recording the information or sealing the document from the outset. This appeal presents a different situation. For the most part, private attorneys (rather than the government) were responsible for creating real estate documents containing people's SSNs and then submitting those documents for recording. The clerk of court could have inspected these documents before recording them and redacted any SSNs, but even this solution differs from *Cox Broadcasting* and *Florida Star*, where the government did not have to search for the sensitive information needing redaction. Given that every year hundreds of thousands of documents are submitted for recording in Virginia, inspecting each one would have been no small undertaking. Most importantly, however, attorneys began filing documents containing SSNs long before Virginia could have been expected to comprehend the current threat of identity theft. For this reason, we find inapplicable *Cox Broadcasting's* observation that "[b]y placing the information in the public domain on official court records, the State must be presumed to have concluded that the public interest was thereby being served."

Virginia currently prohibits attorneys from submitting real estate documents for recording that contain unredacted SSNs. Given the historical circumstances, however, clerks of court still possess millions of land records, over three percent of which probably contain unredacted SSNs. Inspecting all these records to find and redact SSNs would be far more burdensome than sealing indictments and police reports revealing rape victims' identities. Moreover, clerks cannot place original land records under seal while completing such redaction because people must verify who owns what during real estate transactions. Furthermore, regarding land records available through secure remote access, the parties agree that running software used for redacting SSNs costs about four cents per page and has a one to five percent error rate. Virginia thus faces considerable obstacles in avoiding initial disclosure that *Cox Broadcasting* and *Florida Star* did not have to consider. Such realities must factor into our narrow-tailoring analysis.

The factual differences between this case and *Cox Broadcasting* and *Florida Star* suggest the need for a more nuanced analytical approach to the narrow-tailoring requirement. The Supreme Court's recognition of different conceptions of privacy--one focused upon secrecy and incompatible with any disclosure, the other focused upon control and consistent with limited disclosure--and the unrealistic challenge of preserving total secrecy in this situation strongly suggest that Virginia should have more latitude to limit disclosure of land records containing unredacted SSNs than *Cox Broadcasting* and *Florida Star* allowed for protecting rape victims' anonymity. Specifically, the Court's First Amendment jurisprudence does not necessarily require that Virginia redact SSNs from all original land records maintained in courthouse archives before Ostergren may be prevented from publishing them online. Ostergren's website supports this conclusion by recognizing the critical difference between original land records available from courthouses and digital land records available through secure remote access:

> Once records are recorded at the courthouse, they become public and anyone can get them. But shouldn't we all have to drive to the Courthouse to see them? Yes, but sadly that is not the case anymore. Legislators have kowtowed to special interests and in VA, they voted specifically to allow these records online.

This certainly does not mean, however, that enforcing section 59.1-443.2 against Ostergren would be constitutional. We cannot conclude that prohibiting Ostergren from posting public records online would be narrowly tailored to protecting individual privacy when Virginia currently makes those same records available through secure remote access without having redacted SSNs. The record reflects that 15 clerks of court have not finished redacting SSNs from their land records, which are nonetheless available online. Under *Cox Broadcasting* and its progeny, the First Amendment does not allow Virginia to punish Ostergren for posting its land records online without redacting SSNs when numerous clerks are doing precisely that. Virginia could curtail SSNs' public disclosure much more narrowly by directing clerks not to make land records available through secure remote access until after SSNs have been redacted.

In summary, Virginia's failure to redact SSNs before placing land records online means that barring Ostergren's protected speech would not be narrowly tailored to Virginia's interest in protecting individual privacy. For this reason, we hold that enforcing section 59.1-443.2 against Ostergren for the land records posted on her website would violate the First Amendment.

JOHN DOE v. 2THEMART.COM INC.
140 F. Supp. 2d 1088 (W.D. Wash. 2001)

OPINION and ORDER by THOMAS S. ZILLY, United States District Judge

This matter comes before the Court on the motion of J. Doe (Doe) to proceed under a pseudonym and to quash a subpoena issued by 2TheMart.com (TMRT) to a local internet service provider, Silicon Investor/InfoSpace, Inc. (InfoSpace). The motion raises important First Amendment issues regarding Doe's right to speak anonymously on the Internet and to proceed in this Court using a pseudonym in order to protect that right.

FACTUAL BACKGROUND

There is a federal court lawsuit pending in the Central District of California in which the shareholders of TMRT have brought a shareholder derivative class action against the company and its officers and directors alleging fraud on the market. In that litigation, the defendants have asserted as an affirmative defense that no act or omission by the defendants caused the plaintiffs' injury. By subpoena, TMRT seeks to obtain the identity of twenty-three speakers who have participated anonymously on Internet message boards operated by InfoSpace. That subpoena is the subject of the present motion to quash.

InfoSpace is a Seattle based Internet company that operates a website called "Silicon Investor." The Silicon Investor site contains a series of electronic bulletin boards, and some of these bulletin boards are devoted to specific publically traded companies. InfoSpace users can freely post and exchange messages on these boards. Many do so using Internet pseudonyms, the often fanciful names that people choose for themselves when interacting on the Internet. By using a pseudonym, a person who posts or responds to a message on an Internet bulletin board maintains anonymity.

One of the Internet bulletin boards on the Silicon Investor website is specifically devoted to TMRT. According to the brief filed on behalf of J. Doe, "to date, almost 1500 messages have been posted on the TMRT board, covering an enormous variety of topics and posters. Investors and members of the public discuss the latest news about the company, what new businesses it may develop, the strengths and weaknesses of the company's operations, and what its managers and its employees might do better."

Some of the messages posted on the TMRT site have been less than flattering to the company. In fact, some have been downright nasty. For example, a user calling himself "Truthseeker" posted a message stating "TMRT is a Ponzi scam that Charles Ponzi would be proud of. . . . The company's CEO, Magliarditi, has defrauded employees in the past. The company's other large shareholder, Rebeil, defrauded customers in the past." Another poster named "Cuemaster" indicated that "they were dumped by their accountants ... these guys are friggin liars ... why haven't they told the public this yet??? Liars and criminals!!!!!" Another user, not identified in the exhibits, wrote "Lying, cheating, thieving, stealing, lowlife criminals!!!!" Other postings advised TMRT investors to sell their stock. "Look out below!!!! This stock has had it ... get short or sell your position now while you still can." "They [TMRT] are not building anything, except extensions on their homes...bail out now."

TMRT, the defendant in the California lawsuit, issued the present subpoena to InfoSpace pursuant to Fed.R.Civ.P. 45(a)(2). The subpoena seeks, among other things, "all identifying information and documents, including, but not limited to, computerized or computer stored records and logs, electronic mail (E-mail), and postings on your online message boards," concerning a list of twenty-three InfoSpace users, including Truthseeker, Cuemaster, and the current J. Doe, who used the pseudonym NoGuano. These users have posted messages on the TMRT bulletin board or have communicated via the Internet with users who have posted such messages. The subpoena would require InfoSpace to disclose the subscriber information for these twenty-three users, thereby stripping them of their Internet anonymity.

InfoSpace notified these users by e-mail that it had received the subpoena, and gave them time to file a motion to quash. One such user who used the Internet pseudonym NoGuano now seeks to quash the subpoena. NoGuano alleges that enforcement of the subpoena would violate his or her First Amendment right to speak anonymously.

DISCUSSION

The Internet represents a revolutionary advance in communication technology. It has been suggested that the Internet may be the "greatest innovation in speech since the invention of the printing press[.]" It allows people from all over the world to exchange ideas and information freely and in "real-time." Through the use of the Internet, "any person with a phone line can become a town crier with a voice that resonates farther than it could from any soapbox."

The rapid growth of Internet communication and Internet commerce has raised novel and complex legal issues and has challenged existing legal doctrine in many areas. This motion raises important and challenging questions of: (1) what is the scope of an individual's First Amendment right to speak anonymously on the Internet, and (2) what showing must be made by a private party seeking to discover the identity of anonymous Internet users through the enforcement of a civil subpoena?

A. The anonymity of Internet speech is protected by the First Amendment.

The right to the freedom of speech is enshrined in the First Amendment to the United States Constitution. This limitation on governmental interference with free speech applies directly to the federal government, and has been imposed on the states via the Fourteenth Amendment. A court order, even when issued at the request of a private party in a civil lawsuit, constitutes state action and as such is subject to constitutional limitations. For this reason, numerous cases have discussed the limitations on the subpoena power when that power is invoked in such a manner that it impacts First Amendment rights. See, e.g., *NAACP v. Alabama ex rel. Patterson*, 357 U.S. 449, 461 (1958) (discussing the First Amendment implications of a civil subpoena to disclose the membership list for the NAACP).

First Amendment protections extend to speech via the Internet. A component of the First Amendment is the right to speak with anonymity. This component of free speech is well established. See, e.g., *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 357 (1995) (overturning an Ohio law that prohibited the distribution of campaign literature that did not contain the name and address of the person issuing the literature, holding that "under our

Constitution, anonymous pamphleteering is not a pernicious, fraudulent practice, but an honorable tradition of advocacy and dissent. Anonymity is a shield from the tyranny of the majority."); *Talley v. California*, 362 U.S. 60, 65 (1960).

The right to speak anonymously was of fundamental importance to the establishment of our Constitution. Throughout the revolutionary and early federal period in American history, anonymous speech and the use of pseudonyms were powerful tools of political debate. The Federalist Papers (authored by Madison, Hamilton, and Jay) were written anonymously under the name "Publius." The anti-federalists responded with anonymous articles of their own, authored by "Cato" and "Brutus," among others. Anonymous speech is a great tradition that is woven into the fabric of this nation's history.

The right to speak anonymously extends to speech via the Internet. Internet anonymity facilitates the rich, diverse, and far ranging exchange of ideas. The "ability to speak one's mind" on the Internet "without the burden of the other party knowing all the facts about one's identity can foster open communication and robust debate." People who have committed no wrongdoing should be free to participate in online forums without fear that their identity will be exposed under the authority of the court.

When speech touches on matters of public political life, such as debate over the qualifications of candidates, discussion of governmental or political affairs, discussion of political campaigns, and advocacy of controversial points of view, such speech has been described as the "core" or "essence" of the First Amendment. Governmental restrictions on such speech are entitled to "exacting scrutiny," and are upheld only where they are "narrowly tailored to serve an overriding state interest." However, even non-core speech is entitled to First Amendment protection. "First Amendment protections are not confined to 'the exposition of ideas[.]'" Unlike the speech at issue in *McIntyre* and *Talley*, the speech here is not entitled to "exacting scrutiny," but to normal strict scrutiny analysis.

B. Applicable legal standard.

The free exchange of ideas on the Internet is driven in large part by the ability of Internet users to communicate anonymously. If Internet users could be stripped of anonymity by a civil subpoena enforced under the liberal rules of civil discovery, this would have a significant chilling effect on Internet communications and thus on basic First Amendment rights. Therefore, discovery requests seeking to identify anonymous Internet users must be subjected to careful scrutiny by the courts.

"Unmeritorious attempts to unmask the identities of online speakers have a chilling effect on" Internet speech. The "potential chilling effect imposed by the unmasking of anonymous speakers would diminish if litigants first were required to make a showing of need for the information." "Requiring such a showing would allow [the Internet] to thrive as a forum for speakers to express their views on topics of public concern." InfoSpace and NoGuano have accordingly urged this Court to "adopt a balancing test requiring litigants to demonstrate that their need for identity information outweighs anonymous online speakers' First Amendment rights."

In the context of a civil subpoena issued pursuant to Fed.R.Civ.P. 45, this Court must determine when and under what circumstances a civil litigant will be permitted to obtain the

identity of persons who have exercised their First Amendment right to speak anonymously. There is little in the way of persuasive authority to assist this Court. However, courts that have addressed related issues have used balancing tests to decide when to protect an individual's First Amendment rights.

In *Columbia Ins. Co. v. Seescandy.com*, 185 F.R.D. 573 (N.D. Cal. 1999), the plaintiff was unable to identify the defendants when filing the complaint. That complaint named J. Doe defendants, and alleged, *inter alia*, the infringement of a registered trademark when those defendants registered the "Seescandy.com" domain name. The J. Doe defendants had engaged in the allegedly tortious conduct entirely online, and anonymously. The court considered whether to allow discovery to uncover the identity of the defendants so that they might be properly served and subject to the jurisdiction of the court. The court recognized the defendant's "legitimate and valuable right to participate in online forums anonymously or pseudonymously."

Accordingly, the court ruled that four limiting principals would apply to such discovery. The court required that the plaintiff identify the individual with some specificity so the court could determine if they were truly an entity amenable to suit, and that the plaintiff identify all previous steps taken to locate the defendant, justifying the failure to properly serve. The *Seescandy.com* court imposed two other requirements that have relevance. First, the plaintiff was required to show that the case would withstand a motion to dismiss, "to prevent abuse of this extraordinary application of the discovery process and to insure that plaintiff has standing." Second, the plaintiff was required to file a discovery request justifying the need for the information requested. Therefore, the court required the plaintiff to demonstrate that the suit, and the resulting discovery sought, was not frivolous, and to demonstrate the need for the information.

Similarly, in *In re Subpoena Duces Tecum to America Online, Inc.*, 52 Va. Cir. 26 (2000), the court reviewed a subpoena seeking the identity of certain J. Doe defendants who had allegedly made defamatory statements and disclosed confidential information online. The Virginia court recognized the First Amendment right to Internet anonymity, and held that an Internet service provider could assert that right on behalf of its users. The court applied a two part test determining whether the subpoena would be enforced. First, the court must be convinced by the pleadings and evidence submitted that "the party requesting the subpoena has a legitimate, good faith basis to contend that it may be the victim of conduct actionable in the jurisdiction where the suit was filed." Second, "the subpoenaed identity information [must be] *centrally needed to advance that claim*." In that particular case, because the court concluded that the plaintiff had met these requirements, the discovery was allowed.

The courts in *Seescandy.com* and *America Online* applied similar factors. Both required a showing of, at least, a good faith basis for bringing the lawsuit, and both required some showing of the compelling need for the discovery sought. In both cases, the need for the information was especially great because the information sought concerned J. Doe *defendants*. Without the identifying information, the litigation against those defendants could not have continued.

The standard for disclosing the identity of a non-party *witness* must be higher than that articulated in *Seescandy.com* and *America Online.* When the anonymous Internet user is not a party to the case, the litigation can go forward without the disclosure of their identity. Therefore, non-party disclosure is only appropriate in the exceptional case where the compelling need for

the discovery sought outweighs the First Amendment rights of the anonymous speaker.

Accordingly, this Court adopts the following standard for evaluating a civil subpoena that seeks the identity of an anonymous Internet user who is not a party to the underlying litigation. The Court will consider four factors in determining whether the subpoena should issue. These are whether: (1) the subpoena was issued in good faith and not for any improper purpose, (2) the information sought relates to a core claim or defense, (3) the identifying information is directly and materially relevant to that claim or defense, and (4) information sufficient to establish or to disprove that claim or defense is unavailable from any other source.[1]

This test provides a flexible framework for balancing the First Amendment rights of anonymous speakers with the right of civil litigants to protect their interests through the litigation discovery process. The Court shall give weight to each of these factors as the court determines is appropriate under the circumstances of each case. This Court is mindful that it is imposing a high burden. "But the First Amendment requires us to be vigilant in making [these] judgments, to guard against undue hindrances to political conversations and the exchange of ideas."

C. Analysis of the present motion.

In the present case, TMRT seeks information it says will validate its defense that "changes in [TMRT] stock prices were *not* caused by the Defendants but by the illegal actions of individuals who manipulated the [TMRT] stock price using the Silicon Investor message boards." This Court must evaluate TMRT's need for the information in light of the four factors outlined above.

1. Was the subpoena brought in good faith?

This Court does not conclude that this subpoena was brought in bad faith or for an improper purpose. TMRT and its officers and directors are defending against a shareholder derivative class action lawsuit. They have asserted numerous affirmative defenses, one of which alleges that the defendants did not cause the drop in TMRT's stock value. TMRT could reasonably believe that the posted messages are relevant to this defense.

However, as originally issued the subpoena was extremely broad. The subpoena would have required the disclosure of personal e-mails and other personal information that has no relevance to the lawsuit. This disregard for the privacy and the First Amendment rights of the online users, while not demonstrating bad faith *per se*, weighs against TMRT in balancing the interests here.

2. Does the information sought relate to a core claim or defense?

Only when the identifying information is needed to advance core claims or defenses can it be

---

[1] This Court is aware that many civil subpoenas seeking the identifying information of Internet users may be complied with, and the identifying information disclosed, without notice to the Internet users themselves. This is because some Internet service providers do not notify their users when such a civil subpoena is received. The standard set forth in this Order may guide Internet service providers in determining whether to challenge a specific subpoena on behalf of their users. However, this will provide little solace to Internet users whose Internet service company does not provide them notice when a subpoena is received.

sufficiently material to compromise First Amendment rights. If the information relates only to a secondary claim or to one of numerous affirmative defenses, then the primary substance of the case can go forward without disturbing the First Amendment rights of the anonymous Internet users.

The information sought by TMRT does not relate to a core defense. Here, the information relates to only one of twenty-seven affirmative defenses raised by the defendant, the defense that "no act or omission of any of the Defendants was the cause in fact or the proximate cause of any injury or damage to the plaintiffs." This is a generalized assertion of the lack of causation. Defendants have asserted numerous other affirmative defenses that go more "to the heart of the matter," such as the lack of material misstatements by the defendants, actual disclosure of material facts by the defendants, and the business judgment defense.[2] Therefore, this factor also weighs in favor of quashing the subpoena.

3. Is the identifying information directly and materially relevant to a core claim or defense?

Even when the claim or defense for which the information is sought is deemed core to the case, the identity of the Internet users must also be materially relevant to that claim or defense. Under the Federal Rules of Civil Procedure discovery is normally very broad, requiring disclosure of any relevant information that "appears reasonably calculated to lead to the discovery of admissible evidence." But when First Amendment rights are at stake, a higher threshold of relevancy must be imposed. Only when the information sought is directly and materially relevant to a core claim or defense can the need for the information outweigh the First Amendment right to speak anonymously.

TMRT has failed to demonstrate that the identity of the Internet users is directly and materially relevant to a core defense. These Internet users are not parties to the case and have not been named as defendants as to any claim, cross-claim or third-party claim. Therefore, unlike in *Seescandy.com* and *America Online, Inc.*, their identity is not needed to allow the litigation to proceed.

According to the pleadings, the Internet user known as NoGuano has never posted messages on Silicon Investor's TMRT message board. At oral argument, TMRT's counsel conceded this point but stated that NoGuano's information was sought because he had "communicated" via the Internet with Silicon Investor posters such as Truthseeker. Given that NoGuano admittedly posted no public statements on the TMRT site, there is no basis to conclude that the identity of NoGuano and others similarly situated is directly and materially relevant to TMRT's defense.

As to the Internet users such as Truthseeker and Cuemaster who posted messages on the TMRT bulletin board, TMRT has failed to demonstrate that their identities are directly and materially relevant to a core defense. TMRT argues that the Internet postings caused a drop in TMRT's stock price. However, what was said in these postings is a matter of public record, and the identity of the anonymous posters had no effect on investors. If these messages did influence

---

[2] Many of TMRT's affirmative defenses might be viewed by this Court as "non-core," including comparative fault, estoppel, laches, and unclean hands.

the stock price, they did so without *anyone* knowing the identity of the speakers.

TMRT speculates that the users of the InfoSpace website may have been engaged in stock manipulation in violation of federal securities law. TMRT indicates that it intends to compare the names of the InfoSpace users with the names of individuals who traded TMRT stock during the same period to determine whether any illegal stock manipulation occurred. However, TMRT's innuendos of stock manipulation do not suffice to overcome the First Amendment rights of the Internet users. Those rights cannot be nullified by an unsupported allegation of wrongdoing raised by the party seeking the information.

4. Is information sufficient to establish TMRT's defense available from any other source?

TMRT has failed to demonstrate that the information it needs to establish its defense is unavailable from any other source. The chat room messages are archived. TMRT obtained copies of these messages and submitted them to this Court. TMRT can therefore demonstrate what was said, when it was said, and can compare the timing of those statements with fluctuations in the TMRT stock price. The messages are available for use at trial, and TMRT can support its defense without encroaching on the First Amendment rights of the Internet users.

CONCLUSION

The Internet is a truly democratic forum for communication. It allows for the free exchange of ideas at an unprecedented speed and scale. For this reason, the constitutional rights of Internet users, including the right to speak anonymously, must be carefully safeguarded.

Courts should impose a high threshold on subpoena requests that encroach on this right. In order to enforce a civil subpoena seeking the identifying information of a non-party individual who has communicated anonymously over the Internet, the party seeking the information must demonstrate, by a clear showing on the record, that four requirements are met: (1) the subpoena seeking the information was issued in good faith and not for any improper purpose, (2) the information sought relates to a core claim or defense, (3) the identifying information is directly and materially relevant to that claim or defense, and (4) information sufficient to establish or to disprove that claim or defense is unavailable from any other source.

The Court has weighed these factors in light of the facts. TMRT has failed to demonstrate that the identify of these Internet users is directly and materially relevant to a core defense in the underlying securities litigation. Accordingly, Doe's motion to quash the subpoena is GRANTED.

SOLERS, INC. v. JOHN DOE

977 A.2d 941 (D.C. App. 2009)

FISHER, *Associate Judge*:

Appellant Solers, Inc. "is a for-profit Virginia corporation. [Its] work principally consists of developing software and other technology for agencies within the Department of Defense." Appellee SIIA describes itself as "the principal trade association for the software and digital content industry" and explains that "[o]ne of [its] chief missions is to protect the intellectual property of member companies by fighting the software piracy."

In order "[t]o fulfill its mission, SIIA [has] developed anti-piracy programs. "SIIA's enforcement program enables sources with knowledge of software piracy to report anonymously to SIIA via telephone or the Internet about companies [committing piracy] . . . ." Through this program, John Doe reported that Solers was engaged in copyright infringement.

On May 18, 2005, Solers filed a complaint against Doe. The following day Solers issued a subpoena to SIIA, seeking production of all documents related to the identity of Doe, Doe's initial report and his ensuing correspondence with SIIA, and "[a]ll documents . . . believed to be 'evidence'" of Solers' alleged copyright infringement. SIIA, which is not a party to the underlying suit, filed a motion to quash.

This appeal presents us with issues of first impression -- whether the First Amendment protects the anonymity of someone such as Doe, and, if so, under what circumstances a plaintiff such as Solers may invoke court processes to learn Doe's identity and have its day in court. In our analysis we will consider the differing standards employed by other jurisdictions.

The tension between a speaker's desire for anonymity and the right of the plaintiff to protect his reputation or property arises in a variety of contexts, including defamation, copyright infringement, harassment, and malicious gossip. Because the interests at stake will vary, a trial court may need to modify the test we adopt depending on the type of injury alleged. In other words, one size does not necessarily fit all. Here we are faced with a claim of defamation, and we therefore formulate a general framework to fairly accommodate the reputational interests of the plaintiff and the First Amendment rights of the anonymous defendant.

Courts have applied a variety of tests to grapple with the question of when it is appropriate to force a third party to reveal the identity of a defendant charged with defamation. One of the standards most easily satisfied requires only that the court be convinced that the party seeking the subpoena "has a legitimate, good faith basis to contend that it may be the victim of [actionable] conduct . . . ." In our view, the "good faith test" insufficiently protects a defendant's anonymity: "Plaintiffs can often initially plead sufficient facts to meet the good faith test . . . even if the defamation claim is not very strong, or worse, if they do not intend to pursue the defamation action to a final decision." The good faith test and the similarly lax motion to dismiss test may needlessly strip defendants of anonymity in situations where there is no substantial evidence of wrongdoing, effectively giving little or no First Amendment protection to that anonymity.

Toward the other end of the spectrum is the test articulated by the New Jersey Superior Court in *Dendrite International, Inc. v. Doe No. 3*, 775 A.2d 756, 760-61 (N.J. Super. Ct. App. Div. 2001), which requires plaintiffs to "produce sufficient evidence supporting each element of its cause of action, on a prima facie basis," after which the court would "balance the defendant's First Amendment right of anonymous free speech against the strength of the prima facie case presented and the necessity for the disclosure . . . to allow the plaintiff to properly proceed."

The Supreme Court of Delaware adopted a modified version of the *Dendrite* test in *Doe v. Cahill*, 884 A.2d 451 (Del. 2005), holding "that before a defamation plaintiff can obtain the identity of an anonymous defendant through the compulsory discovery process he must support his defamation claim with facts sufficient to defeat a summary judgment motion." "In other words," "the defamation plaintiff, as the party bearing the burden of proof at trial, must introduce

evidence creating a genuine issue of material fact for all elements of a defamation claim *within the plaintiff's control*." In addition, "to the extent reasonably practicable under the circumstances, the plaintiff must undertake efforts to notify the anonymous poster that he is the subject of a subpoena [and] withhold action to afford the anonymous defendant a reasonable opportunity to file and serve opposition to the discovery request." The important feature of *Dendrite* and *Cahill* is to emphasize that the plaintiff must do more than simply plead his case.

A Test for the District of Columbia

Procedural labels such as prima facie or "summary judgment" may prove misleading, but the test we now adopt closely resembles the "summary judgment" standard articulated in *Cahill*. When presented with a motion to quash (or to enforce) a subpoena which seeks the identity of an anonymous defendant, the court should: (1) ensure that the plaintiff has adequately pleaded the elements of the defamation claim, (2) require reasonable efforts to notify the anonymous defendant that the complaint has been filed and the subpoena has been served, (3) delay further action for a reasonable time to allow the defendant an opportunity to file a motion to quash, (4) require the plaintiff to proffer evidence creating a genuine issue of material fact on each element of the claim that is *within its control*, and (5) determine that the information sought is important to enable the plaintiff to proceed with his lawsuit. We do not require a separate balancing test at the end of the analysis, nor do we require a showing that the plaintiff has exhausted alternative sources for learning the information. This brief summary of our test must be read in context of the discussion that follows.

Before enforcing a subpoena seeking the identity of an anonymous user of the internet, the court must first determine whether the plaintiff has adequately pleaded each element of his claim. This is only the first step, however. If the complaint is adequate, the court then must ensure that reasonable efforts are made to notify the defendant that the subpoena has been served. Many courts have required the plaintiff to provide this notice, usually by posting it in the same manner in which the allegedly defamatory statement was published. Nevertheless, it often will be simpler and more effective to require the recipient of the subpoena (who likely knows the identity of the anonymous defendant, or at least knows how to contact him) to provide such notice. Once suitable efforts have been made to notify the defendant, the court should delay action to allow him a reasonable opportunity to file a motion to quash the subpoena. "A court should not consider impacting a speaker's First Amendment rights without affording the speaker an opportunity to respond to the discovery request."

The plaintiff next is required to proffer evidence to show that it has a viable claim of defamation. This evidence must be sufficient to create a genuine issue of material fact with respect to all the elements of the defamation claim within the plaintiff's control, "in other words, all elements not dependent upon knowing the identity of the anonymous speaker." An important part of this process is to set forth as precisely as possible the statements by the anonymous defendant that are alleged to be defamatory.

The court should also ensure that the information sought is important to the litigation. This portion of the test is easily satisfied when the anonymous speaker is the defendant and the litigation cannot proceed without serving him with process. We do not, in these circumstances,

require a showing that the plaintiff has exhausted alternative sources for learning the information. When the other elements of the test have been satisfied, we see little point in requiring the plaintiff to travel more circuitous trails in search of Doe's identity.

SIIA protests that enforcement of subpoenas like this one will have a chilling effect on reporting of software piracy: "Because few would-be Internet communicators seeking to report potential software piracy would risk the financial and other burdens of defending a lawsuit, that speech likely would disappear." The test we have adopted takes this concern into account. As the previous discussion should make clear, we do not take lightly a person's decision to speak anonymously. But that is not an absolute right, and SIIA's website alerted John Doe that SIIA might be required to disclose his identity. We do not question the importance of combating software piracy, but that is only one of the interests we must balance.

Solers argues that it is unfair to require production of evidence at this early stage of the proceedings. It is important to emphasize in response that we do not expect Solers to demonstrate that it is entitled to judgment in its favor. Rather, Solers merely must show that it has a viable claim of defamation -- that there is a genuine issue of material fact on each element of the claim that does not depend on knowing the defendant's identity. Moreover, this is a test for deciding whether to enforce or quash the subpoena. If the court decides to quash, it will have to determine after a separate inquiry whether to prolong the litigation or to dismiss the complaint for failure to prosecute.

Recognizing Solers' dilemma, the trial court may choose to allow some discovery before deciding whether to order disclosures that will reveal the identity of Doe. Here, for example, Solers does not know the exact statements made by John Doe. It might be useful as a preliminary step to order SIIA to disclose those statements, if that can be done without revealing Doe's identity. Or, perhaps, the court could allow limited discovery to determine whether the court may exercise personal jurisdiction over Doe. The court need not decide at the very outset of the litigation whether to compel SIIA to disclose the identity of John Doe.

It should be obvious that a key issue on remand will be determining what types of evidence the court reasonably may expect Solers to proffer without knowing the identity of John Doe. Applying this aspect of the test will require sensitivity to the unique circumstances of each case. Nevertheless, in this context, a plaintiff must do more than simply plead his case. We therefore vacate the judgment of the Superior Court and remand this case to give Solers an opportunity to present *evidence* supporting its claim of defamation.

UNIVERSAL CITY STUDIOS, INC. v. CORLEY

273 F.3d 429 (2d Cir. 2001)

JON O. NEWMAN, Circuit Judge

When the Framers of the First Amendment prohibited Congress from making any law "abridging the freedom of speech," they were not thinking about computers, computer programs, or the Internet. But neither were they thinking about radio, television, or movies. Just as the inventions at the beginning and middle of the 20th century presented new First Amendment

issues, so does the cyber revolution at the end of that century. This appeal raises significant First Amendment issues concerning one aspect of computer technology--encryption to protect materials in digital form from unauthorized access. The appeal challenges the constitutionality of the Digital Millennium Copyright Act ("DMCA"), 17 U.S.C. § 1201 *et seq.* (Supp. V 1999) and the validity of an injunction entered to enforce the DMCA.

Defendant-Appellant Eric C. Corley and his company, 2600 Enterprises, Inc., appeal from the final judgment of the United States District Court for the Southern District of New York (Lewis A. Kaplan, District Judge) enjoining them from various actions concerning a decryption program known as "DeCSS." The injunction primarily bars the Appellants from posting DeCSS on their web site and from knowingly linking their web site to any other web site on which DeCSS is posted. We affirm.

Introduction

This appeal concerns the anti-trafficking provisions of the DMCA, which Congress enacted in 1998 to strengthen copyright protection in the digital age. Fearful that the ease with which pirates could copy and distribute a copyrightable work in digital form was overwhelming the capacity of conventional copyright enforcement to find and enjoin unlawfully copied material, Congress sought to combat copyright piracy in its earlier stages, before the work was even copied. The DMCA therefore backed with legal sanctions the efforts of copyright owners to protect their works from piracy behind digital walls such as encryption codes or password protections. In so doing, Congress targeted not only those pirates who would *circumvent* these digital walls (the "anti-circumvention provisions," contained in 17 U.S.C. § 1201 (a)(1)), but also anyone who would *traffic* in a technology primarily designed to circumvent a digital wall (the "anti-trafficking provisions," contained in 17 U.S.C. § 1201 (a)(2), (b)(1)).

Corley publishes a print magazine and maintains an affiliated web site geared towards "hackers." The so-called hacker community includes serious computer-science scholars conducting research on protection techniques, computer buffs intrigued by the challenge of trying to circumvent access-limiting devices or perhaps hoping to promote security by exposing flaws in protection techniques, mischief-makers interested in disrupting computer operations, and thieves, including copyright infringers who want to acquire copyrighted material (for personal use or resale) without paying for it.

In November 1999, Corley posted a copy of the decryption computer program "DeCSS" on his web site. DeCSS is designed to circumvent "CSS," the encryption technology that motion picture studios place on DVDs to prevent the unauthorized viewing and copying of motion pictures. Corley also posted on his web site links to other sites where DeCSS could be found.

Plaintiffs-Appellees are eight motion picture studios that brought an action seeking injunctive relief against Corley under the DMCA. any other web site containing DeCSS. The District Court rejected Corley's constitutional attacks on the statute and the injunction.

Corley renews his constitutional challenges on appeal. Specifically, he argues primarily that: the DMCA as applied to his dissemination of DeCSS violates the First Amendment because

computer code is "speech" entitled to full First Amendment protection and the DMCA fails to survive the exacting scrutiny accorded statutes that regulate speech.

Background

The movie studios were reluctant to release movies in digital form until they were confident they had in place adequate safeguards against piracy of their copyrighted movies. The studios took several steps to minimize the piracy threat. First, they settled on the DVD as the standard digital medium for home distribution of movies. The studios then sought an encryption scheme to protect movies on DVDs. They enlisted the help of members of the consumer electronics and computer industries, who in mid-1996 developed the Content Scramble System ("CSS"). CSS is an encryption scheme that employs an algorithm configured by a set of "keys" to encrypt a DVD's contents. The algorithm is a type of mathematical formula for transforming the contents of the movie file into gibberish; the "keys" are in actuality strings of 0's and 1's that serve as values for the mathematical formula. Decryption in the case of CSS requires a set of "player keys" contained in compliant DVD players, as well as an understanding of the CSS encryption algorithm. Without the player keys and the algorithm, a DVD player cannot access the contents of a DVD. With the player keys and the algorithm, a DVD player can display the movie on a television or a computer screen, but does not give a viewer the ability to use the copy function of the computer to copy the movie or to manipulate the digital content of the DVD.

The studios developed a licensing scheme for distributing the technology to manufacturers of DVD players. In exchange for the licenses, manufacturers were obliged to keep the player keys confidential. Manufacturers were also required to prevent the transmission of "CSS data" from a DVD drive to any "internal recording device," including, presumably, a computer hard drive.

With encryption technology and licensing agreements in hand, the studios began releasing movies on DVDs in 1997. In 1998, the studios secured added protection against DVD piracy when Congress passed the DMCA, which prohibits the development or use of technology designed to circumvent a technological protection measure, such as CSS. The pertinent provisions of the DMCA are examined in greater detail below.

In September 1999, Jon Johansen, a Norwegian teenager, collaborating with two unidentified individuals, reverse-engineered a licensed DVD player designed to operate on the Microsoft operating system, and culled from it the player keys and other information necessary to decrypt CSS. The record suggests that Johansen was trying to develop a DVD player operable on Linux, an alternative operating system that did not support any licensed DVD players at that time. In order to accomplish this task, Johansen wrote a decryption program executable on Microsoft's operating system. That program was called, appropriately enough, "DeCSS."

If a user runs the DeCSS program with a DVD in the computer's disk drive, DeCSS will decrypt the DVD's CSS protection, allowing the user to copy the DVD's files and place the copy on the user's hard drive. The result is a very large computer file that can be played on a non-CSS-compliant player and copied, manipulated, and transferred just like any other computer file. DeCSS comes complete with a fairly user-friendly interface that helps the user select from

among the DVD's files and assign the decrypted file a location on the user's hard drive. The quality of the resulting decrypted movie is "virtually identical" to that of the encrypted movie on the DVD. And the file produced by DeCSS, while large, can be compressed to a manageable size by compression software. This compressed file can be copied onto a DVD, or transferred over the Internet (with some patience).

While there may be alternative means of extracting a non-encrypted, copyable movie from a DVD--for example, by copying the movie along with its encryption "bit-by-bit," or "ripping" a DVD by siphoning movie file data after CSS has already been decrypted by a licensed player--DeCSS is the superior means of acquiring easily copyable movies. We acknowledge the complexity and the rapidly changing nature of the technology involved, but it is clear that the Defendants have presented no evidence to refute any of these findings by the District Court.

Johansen posted the executable object code, but not the source code, for DeCSS on his web site. The distinction between source code and object code is relevant to this case, so a brief explanation is warranted. A computer responds to electrical charges, the presence or absence of which is represented by strings of 1's and 0's. Strictly speaking, "object code" consists of those 1's and 0's. While some people can read and program in object code, "it would be inconvenient, inefficient and, for most people, probably impossible to do so." Computer languages have been written to facilitate program writing and reading. A program in such a computer language--BASIC, C, and Java are examples--is said to be written in "source code." Source code has the benefit of being much easier to read (by people) than object code, but as a general matter, it must be translated back to object code before it can be read by a computer. This task is usually performed by a program called a compiler. Since computer languages range in complexity, object code can be placed on one end of a spectrum, and different kinds of source code can be arrayed across the spectrum according to the ease with which they are read and understood by humans. Within months of its appearance in executable form on Johansen's web site, DeCSS was widely available on the Internet, in both object code and various forms of source code.

In November 1999, Corley wrote and placed on his web site, 2600.com, an article about the DeCSS phenomenon. His web site is an auxiliary to the print magazine, *2600: The Hacker Quarterly*, which Corley has been publishing since 1984. While the magazine and the web site cover some issues of general interest to computer users--such as threats to online privacy--the focus of the publications is on the vulnerability of computer security systems, and more specifically, how to exploit that vulnerability in order to circumvent the security systems.

Corley's article about DeCSS detailed how CSS was cracked, and described the movie industry's efforts to shut down web sites posting DeCSS. It also explained that DeCSS could be used to copy DVDs. At the end of the article, the Defendants posted copies of the object and source code of DeCSS. In Corley's words, he added the code to the story because "in a journalistic world, . . . you have to show your evidence . . . and particularly in the magazine that I work for, people want to see specifically what it is that we are referring to," including "what evidence . . . we have" that there is in fact technology that circumvents CSS. Writing about DeCSS without including the DeCSS code would have been, to Corley, "analogous to printing a

story about a picture and not printing the picture." Corley also added to the article links that he explained would take the reader to other web sites where DeCSS could be found.

2600.com was only one of hundreds of web sites that began posting DeCSS near the end of 1999. The movie industry tried to stem the tide by sending cease-and-desist letters to these sites. These efforts met with only partial success. In January 2000, the studios filed this lawsuit.

Constitutional Challenges Based on the First Amendment

A. Applicable Principles

1. Code as Speech

Communication does not lose constitutional protection as "speech" simply because it is expressed in the language of computer code. Mathematical formulae and musical scores are written in "code," *i.e.*, symbolic notations not comprehensible to the uninitiated, and yet both are covered by the First Amendment. If someone chose to write a novel entirely in computer object code by using strings of 1's and 0's for each letter of each word, the resulting work would be no different for constitutional purposes than if it had been written in English. The "object code" version would be incomprehensible to readers outside the programming community (and tedious to read even for most within the community), but it would be no more incomprehensible than a work written in Sanskrit for those unversed in that language. The undisputed evidence reveals that even pure object code can be, and often is, read and understood by experienced programmers. And source code (in any of its various levels of complexity) can be read by many more. Ultimately, however, the ease with which a work is comprehended is irrelevant to the constitutional inquiry. If computer code is distinguishable from conventional speech for First Amendment purposes, it is not because it is written in an obscure language.

2. Computer Programs as Speech

Of course, computer code is not likely to be the language in which a work of literature is written. Instead, it is primarily the language for programs executable by a computer. These programs are essentially instructions to a computer. In general, programs may give instructions either to perform a task or series of tasks when initiated by a single (or double) click of a mouse or, once a program is operational ("launched"), to manipulate data that the user enters into the computer. Whether computer code that gives a computer instructions is "speech" within the meaning of the First Amendment requires consideration of the scope of the Constitution's protection of speech.

Even dry information, devoid of advocacy, political relevance, or artistic expression, has been accorded First Amendment protection. Thus, for example, courts have subjected to First Amendment scrutiny restrictions on the dissemination of technical scientific information, scientific research, and attempts to regulate the publication of instructions.

Computer programs are not exempted from the category of First Amendment speech simply because their instructions require use of a computer. A recipe is no less "speech" because it calls for the use of an oven, and a musical score is no less "speech" because it specifies performance

on an electric guitar. Arguably distinguishing computer programs from conventional language instructions is the fact that programs are executable on a computer. But the fact that a program has the capacity to direct the functioning of a computer does not mean that it lacks the additional capacity to convey information, and it is the conveying of information that renders instructions "speech" for purposes of the First Amendment. The information conveyed by most "instructions" is how to perform a task.

Instructions such as computer code, which are intended to be executable by a computer, will often convey information capable of comprehension and assessment by a human being. A programmer reading a program learns information about instructing a computer, and might use this information to improve personal programming skills and perhaps the craft of programming. Moreover, programmers communicating ideas to one another almost inevitably communicate in code, much as musicians use notes. Limiting First Amendment protection of programmers to descriptions of computer code (but not the code itself) would impede discourse among computer scholars, just as limiting protection for musicians to descriptions of musical scores (but not sequences of notes) would impede their exchange of ideas and expression. Instructions that communicate information comprehensible to a human qualify as speech whether the instructions are designed for execution by a computer or a human (or both).

For all of these reasons, we join the other courts that have concluded that computer code, and computer programs constructed from code, can merit First Amendment protection.

3. The Scope of First Amendment Protection for Computer Code

Having concluded that computer code conveying information is "speech" within the meaning of the First Amendment, we next consider, to a limited extent, the scope of the protection that code enjoys. As the District Court recognized, the scope of protection for speech generally depends on whether the restriction is imposed because of the content of the speech. Content-based restrictions are permissible only if they serve compelling state interests and do so by the least restrictive means available. A content-neutral restriction is permissible if it serves a substantial governmental interest, the interest is unrelated to the suppression of free expression, and the regulation is narrowly tailored, which "in this context requires . . . that the means chosen do not 'burden substantially more speech than is necessary to further the government's legitimate interests.'" *Turner Broadcasting System, Inc. v. FCC*, 512 U.S. 622, 662 (1994).

"Government regulation of expressive activity is 'content neutral' if it is justified without reference to the content of regulated speech." The government's purpose is the controlling consideration. A regulation that serves purposes unrelated to the content of expression is deemed neutral, even if it has an incidental effect on some speakers or messages but not others." The Supreme Court's approach to determining content-neutrality appears to be applicable whether what is regulated is expression (regulation of volume of music), conduct, or any "activity" that can be said to combine speech and non-speech elements.

To determine whether regulation of computer code is content-neutral, the initial inquiry must be whether the regulated activity is "sufficiently imbued with elements of communication to fall

within the scope of the First . . . Amendment." Computer code, as we have noted, often conveys information comprehensible to human beings, even as it also directs a computer to perform various functions. Once a speech component is identified, the inquiry then proceeds to whether the regulation is "justified without reference to the content of regulated speech."

The Appellants vigorously reject the idea that computer code can be regulated according to any different standard than that applicable to pure speech, *i.e.*, speech that lacks a nonspeech component. Although recognizing that code is a series of instructions to a computer, they argue that code is no different, for First Amendment purposes, than blueprints that instruct an engineer or recipes that instruct a cook. We disagree. Unlike a blueprint or a recipe, which cannot yield any functional result without human comprehension of its content, human decision-making, and human action, computer code can instantly cause a computer to accomplish tasks and instantly render the results of those tasks available throughout the world via the Internet. The only human action required to achieve these results can be as limited and instantaneous as a single click of a mouse. These realities of what code is and what its normal functions are require a First Amendment analysis that treats code as combining nonspeech and speech elements, *i.e.*, functional and expressive elements.

We recognize, as did Judge Kaplan, that the functional capability of computer code cannot yield a result until a human being decides to insert the disk containing the code into a computer and causes it to perform its function (or programs a computer to cause the code to perform its function). Nevertheless, this momentary intercession of human action does not diminish the nonspeech component of code, nor render code entirely speech, like a blueprint or a recipe. Judge Kaplan cogently explained why this is especially so with respect to decryption code:

> Once a decryption program like DeCSS is written, it quickly can be sent all over the world. Every recipient is capable not only of decrypting and perfectly copying plaintiffs' copyrighted DVDs, but also of retransmitting perfect copies of DeCSS and thus enabling every recipient to do the same. They likewise are capable of transmitting perfect copies of the decrypted DVD.
>
> These considerations drastically alter consideration of the causal link between dissemination of computer programs such as this and their illicit use. Here, dissemination itself of means of circumventing access controls to copyrighted works threatens to produce virtually unstoppable infringement of copyright. In consequence, the causal link between the dissemination of circumvention computer programs and their improper use is sufficiently close to warrant selection of a level of constitutional scrutiny based on the programs' functionality.

The functionality of computer code properly affects the scope of its First Amendment protection.

4. The Scope of First Amendment Protection for Decryption Code

In considering the scope of First Amendment protection for a decryption program like DeCSS, we must recognize that the essential purpose of encryption code is to prevent

unauthorized access. Owners of all property rights are entitled to prohibit access to their property by unauthorized persons. Homeowners can install locks on the doors of their houses. Custodians of valuables can place them in safes. Stores can attach to products security devices that will activate alarms if the products are taken away without purchase. These and similar security devices can be circumvented. Burglars can use skeleton keys to open door locks. Thieves can obtain the combinations to safes. Product security devices can be neutralized.

Our case concerns a security device, CSS computer code, that prevents access by unauthorized persons to DVD movies. The CSS code is embedded in the DVD movie. Access to the movie cannot be obtained unless a person has a device, a licensed DVD player, equipped with computer code capable of decrypting the CSS encryption code. In its basic function, CSS is like a lock on a homeowner's door, a combination of a safe, or a security device attached to a store's products.

DeCSS is computer code that can decrypt CSS. In its basic function, it is like a skeleton key that can open a locked door, a combination that can open a safe, or a device that can neutralize the security device attached to a store's products. DeCSS enables anyone to gain access to a DVD movie without using a DVD player.

The initial use of DeCSS to gain access to a DVD movie creates no loss to movie producers because the initial user must purchase the DVD. However, once the DVD is purchased, DeCSS enables the initial user to copy the movie in digital form and transmit it instantly in virtually limitless quantity, thereby depriving the movie producer of sales. The advent of the Internet creates the potential for instantaneous worldwide distribution of the copied material.

At first glance, one might think that Congress has as much authority to regulate the distribution of computer code to decrypt DVD movies as it has to regulate distribution of skeleton keys, combinations to safes, or devices to neutralize store product security devices. However, despite the evident legitimacy of protection against unauthorized access to DVD movies, regulation of decryption code like DeCSS is challenged in this case because DeCSS differs from a skeleton key in one important respect: it not only is capable of performing the function of unlocking the encrypted DVD movie, it also is a form of communication, albeit written in a language not understood by the general public. As a communication, the DeCSS code has a claim to being "speech," and as "speech," it has a claim to being protected by the First Amendment. But just as the realities of what any computer code can accomplish must inform the scope of its constitutional protection, so the capacity of a decryption program like DeCSS to accomplish unauthorized--indeed, unlawful--access to materials in which the Plaintiffs have intellectual property rights must inform and limit the scope of its First Amendment protection.

With all of the foregoing considerations in mind, we next consider the Appellants' First Amendment challenge to the DMCA as applied in the specific prohibitions that have been imposed by the District Court's injunction.

B. First Amendment Challenge

The District Court's injunction applies the DMCA to the Defendants by imposing two types

of prohibition. The first prohibits posting DeCSS or any other technology for circumventing CSS on any web site. The second prohibits knowingly linking any web site to any other web site containing DeCSS. The validity of the prohibitions must be considered separately.

1. Posting

The initial issue is whether the posting prohibition is content-neutral, since this classification determines the applicable constitutional standard. The Appellants contend that the anti-trafficking provisions of the DMCA and their application by means of the posting prohibition of the injunction are content-based. They argue that the provisions "specifically target . . . scientific expression based on the particular topic addressed by that expression--namely, techniques for circumventing CSS." We disagree. The Appellants' argument fails to recognize that the target of the posting provisions of the injunction--DeCSS--has both a nonspeech and a speech component, and that the DMCA, as applied to Appellants, and the posting prohibition target only the nonspeech component. Neither the DMCA nor the posting prohibition is concerned with whatever capacity DeCSS might have for conveying information to a human being, and that capacity is what arguably creates a speech component of the decryption code. The DMCA and the posting prohibition are applied to DeCSS solely because of its capacity to instruct a computer to decrypt CSS. That functional capability is not speech within the meaning of the First Amendment. This type of regulation is therefore content-neutral, just as would be a restriction on trafficking in skeleton keys identified because of their capacity to unlock jail cells, even though some of the keys happened to bear a slogan or other legend that qualified as a speech component.

As a content-neutral regulation with an incidental effect on a speech component, the regulation must serve a substantial governmental interest, the interest must be unrelated to the suppression of free expression, and the incidental restriction on speech must not burden substantially more speech than is necessary to further that interest. *Turner Broadcasting*, 512 U.S. at 662. The Government's interest in preventing unauthorized access to encrypted copyrighted material is substantial, and the regulation of DeCSS by the posting prohibition plainly serves that interest. Moreover, that interest is unrelated to the suppression of expression. The injunction regulates the posting of DeCSS, regardless of whether DeCSS code contains any information comprehensible by human beings that would qualify as speech. Whether the incidental regulation on speech burdens substantially more speech than necessary to further the interest in preventing unauthorized access to copyrighted materials requires some elaboration.

Posting DeCSS on the Appellants' web site makes it instantly available at the click of a mouse to any person in the world with access to the Internet, and such person can then instantly transmit DeCSS to anyone else with Internet access. Although the prohibition on posting prevents the Appellants from conveying to others the speech component of DeCSS, the Appellants have not suggested any technique for barring them from making this instantaneous worldwide distribution of a decryption code that makes a lesser restriction on the code's speech component. It is true that the Government has alternative means of prohibiting unauthorized access to copyrighted materials. For example, it can create criminal and civil liability for those who gain unauthorized access, and thus it can be argued that the restriction on posting DeCSS is

not absolutely necessary. But a content-neutral regulation need not employ the least restrictive means of accomplishing the governmental objective. It need only avoid burdening "substantially more speech than is necessary to further the government's legitimate interests." The prohibition on the Defendants' posting of DeCSS satisfies that standard.

2. Linking

A hyperlink is a cross-reference appearing on one web page that, when activated by the point-and-click of a mouse, brings onto the computer screen another web page. With a hyperlink on a web page, the linked web site is just one click away.[1]

In applying the DMCA to linking (via hyperlinks), Judge Kaplan recognized that a hyperlink has both a speech and a nonspeech component. It conveys information, the Internet address of the linked web page, and has the functional capacity to bring the content of the linked page to the user's computer screen. He ruled that application of the DMCA to the Defendants' linking to web sites containing DeCSS is content-neutral because it is justified without regard to the speech component of the hyperlink. The prohibition applies whether or not the hyperlink contains any information, comprehensible to a human being, as to the Internet address of the web page being accessed. The linking prohibition is justified solely by the functional capability of the hyperlink.

Applying the requirements for content-neutral regulation, Judge Kaplan then ruled that the DMCA, as applied to the Defendants' linking, served substantial governmental interests and was unrelated to the suppression of free expression. We agree. He then carefully considered the "closer call," as to whether a linking prohibition would satisfy the narrow tailoring requirement. In an especially carefully considered portion of his opinion, he observed that strict liability for linking to web sites containing DeCSS would risk two impairments of free expression. Web site operators would be inhibited from displaying links to various web pages for fear that a linked page might contain DeCSS, and a prohibition on linking to a web site containing DeCSS would curtail access to whatever other information was contained at the accessed site.

To avoid applying the DMCA in a manner that would "burden substantially more speech than is necessary to further the government's legitimate interests," Judge Kaplan required clear and convincing evidence

> that those responsible for the link (a) know at the relevant time that the offending material is on the linked-to site, (b) know that it is circumvention technology that may not lawfully be offered, and (c) create or maintain the link for the purpose of disseminating that technology.

He then found that the evidence satisfied his three-part test by his required standard of proof.

In response to our post-argument request for the parties' views on various issues, including

---

[1] "Linking" not accomplished by a hyperlink would simply involve the posting of the URL of another web page. A "link" of this sort is sometimes called an "inactive link." With an inactive link, the linked web page would be only four clicks away.

Judge Kaplan's test for a linking prohibition, the Appellants replied that his test was deficient for not requiring proof of intent to cause, or aid or abet, harm, and that the only valid test for a linking prohibition would be one that could validly apply to the publication in a print medium of an address for obtaining prohibited material.

We see no need on this appeal to determine whether a test as rigorous as Judge Kaplan's is required. It suffices to reject the Appellants' contention that an intent to cause harm is required and that linking can be enjoined only under circumstances applicable to a print medium. As they have throughout their arguments, the Appellants ignore the functional capacity of decryption computer code and hyperlinks to facilitate instantaneous unauthorized access to copyrighted materials by anyone anywhere in the world. Under the circumstances, the injunction's linking prohibition validly regulates the Appellants' opportunity instantly to enable anyone anywhere to gain unauthorized access to copyrighted movies on DVDs.

At oral argument, we asked the Government whether its undoubted power to punish the distribution of obscene materials would permit an injunction prohibiting a newspaper from printing addresses of bookstore locations carrying such materials. In a properly cautious response, the Government stated that the answer would depend on the circumstances of the publication. The Appellants' supplemental papers enthusiastically embraced the arguable analogy between printing bookstore addresses and displaying on a web page links to web sites at which DeCSS may be accessed. They confidently asserted that publication of bookstore locations carrying obscene material cannot be enjoined consistent with the First Amendment, and that a prohibition against linking to web sites containing DeCSS is similarly invalid.

Like many analogies posited to illuminate legal issues, the bookstore analogy is helpful primarily in identifying characteristics that *distinguish* it from the context of the pending dispute. If a bookstore proprietor is knowingly selling obscene materials, the evil of distributing such materials can be prevented by injunctive relief against the unlawful distribution (and similar distribution by others can be deterred by punishment of the distributor). And if others publish the location of the bookstore, preventive relief against a distributor can be effective before any significant distribution of the prohibited materials has occurred. The digital world, however, creates a very different problem. If obscene materials are posted on one web site and other sites post hyperlinks to the first site, the materials are available for instantaneous worldwide distribution before any preventive measures can be effectively taken.

This reality obliges courts considering First Amendment claims in the context of the pending case to choose between two unattractive alternatives: either tolerate some impairment of communication in order to permit Congress to prohibit decryption that may lawfully be prevented, or tolerate some decryption in order to avoid some impairment of communication.

In facing this choice, we are mindful that it is not for us to resolve the issues of public policy implicated by the choice we have identified. Those issues are for Congress. Our task is to determine whether the legislative solution adopted by Congress, as applied to the Appellants, is consistent with the limitations of the First Amendment, and we are satisfied that it is.