Berkeley Technology Law Journal

Volume 17 | Issue 1 Article 27

January 2002

Constitutional Law - Additional Developments

Berkeley Technology Law Journal

ADDITIONAL DEVELOPMENTS—CONSTITUTIONAL LAW

AMERICAN CIVIL LIBERTIES UNION V. RENO

217 F.3d 162 (3d Cir. 2000)

At issue in this case was whether the Child Online Protection Act ("COPA") violates the First Amendment. Because the statute imposed an impermissible burden on protected speech, the Third Circuit affirmed the district court's decision granting the American Civil Liberties Union preliminary injunction to prevent the enforcement of COPA.

The American Civil Liberties Union ("ACLU") and several world wide web publishers brought action in the United States District Court for the Eastern District of Pennsylvania, challenging COPA's constitutionality and seeking to enjoin its enforcement. The district court entered a preliminary injunction preventing the government from enforcing COPA, holding that it placed too great a burden on protected expression. The court applied a two-part test to determine whether the statute is constitutional: (1) whether the statute is narrowly tailored to meet a compelling state interest, and (2) whether the statute is the least restrictive means to achieve that objective. In applying this test, the court reasoned that the high economic cost of implementing an age verification system and the ineffectiveness of such a system would cause web publishers to cease publishing such material or censor more material than necessary. Furthermore, less restrictive means, such as parental blocking and filtering software, would likely be as effective as COPA.

The Third Circuit upheld this decision. In applying the same test, it based its entire opinion on the constitutionality of the "contemporary community standards" clause to identify material that is harmful to minors in the context of the web. Any statute imposing a content-based restriction on speech is presumptively invalid and subject to strict scrutiny analysis. The court found that COPA creates an impermissible burden because current technology does not permit web publishers to geographically restrict access to their sites, and, consequently, requires them to abide by the most restrictive state's standards. This case was distinguishable, on the facts, from prior, non-web cases because, unlike mail or telephone mediums, the web was not geographically constrained. Defendants in prior non-web cases had the ability to geographically control the distribution of the controversial material, and were therefore not subject to the most restrictive state's standards.

The court distinguished this case from *United States v. Thomas*, 74 F.3d 701 (6th Cir. 1996), in which the Sixth Circuit held that the degree of harm caused by material on the defendant's electronic bulletin board must be judged by the standards of the community in which the disputed material was received. Unlike web publishers, bulletin board operators have control over the geographical distribution of their materials.

The court further determined that the statute was not readily susceptible to a narrow construction that would make it constitutional. The court rejected the government's argument that the "contemporary community standards" language should be interpreted by an "adult" rather than a "geographic" standard, noting that community standards had always been interpreted as a geographic standard. In addition, the court concluded that striking the "contemporary community standards" clause would not salvage COPA's constitutionality because the clause was an integral part of the statute.

The court concluded that granting the preliminary injunction would not violate the public's interest.

CYBERSPACE COMMUNICATIONS, INC. V. ENGLER

142 F. Supp. 2d 827 (E.D. Mich. 2001)

The United States District Court for the Easter District of Michigan considered whether a Michigan state law regulating the dissemination of sexually explicit materials to children violates the First Amendment and/or the Commerce Clause of the United States Constitution. On the First Amendment issue, the court applied a two-part test: (1) whether the statute is necessary to achieve a compelling state interest, and (2) whether the statute is narrowly tailored to achieve that result. The court held that the Act violated the First Amendment by placing undue content-based limitation on speech. Further the court held that because the Commerce Clause precludes the application of a state statute to commerce that occurs outside of a state's borders, Michigan's effort to regulate what information may be transmitted to Michigan's children via the Internet was in violation of the Commerce Clause.

Michigan's 1999 Public Act 33 ("the Act") contained provisions which pertain to dissemination of sexually explicit materials to children over the Internet. Internet companies and the American Civil Liberties Union ("ACLU") brought suit challenging the constitutionality of the Act, seeking to enjoin defendants from enforcing the Act. The district court issued a preliminary injunction on July 29, 1999. This decision was affirmed by the Sixth Circuit and remanded for further proceedings. On remand, the district court granted the plaintiff's motion for summary judgment that permanently enjoined the defendant from enforcing the Act.

The district court based its holding on the Act's undue content-based limitation on speech. The court recognized that the state had a compelling interest to protect minor children from exposure to obscene materials. However, the court found that the defendants failed to demonstrate that less intrusive means would not achieve similar restrictions. The court noted that filters, child-friendly software, or the on/off switch of the computer, all of which are less intrusive, would allow parents to control the information coming into their home via the Internet.

The district court further held that the Act violated the Commerce Clause, which precludes the application of a state statute to commerce occurring outside of a state's borders. The court found that by regulating information transmitted to Michigan's children via the Internet, the Act attempted to control Internet communications that might originate in states and countries outside Michigan. The court denied defendants' request to limit the relief to the challenged provisions of the Act, stating that courts would not "rewrite statutes to create constitutionality."

DENDRITE INTERNATIONAL, INC. V. DOE

342 N.J. Super. 134 (N.J. Super. Ct. App. Div. 2001)

The Superior Court of New Jersey ruled on the issue of whether the First Amendment protects speech in online chat rooms. Applying a case-by-case, multi-step test that analyzes and balances the equities and rights at issue, the court held that all forms of speech, including anonymous speech over the Internet, are protected.

Plaintiff is a publicly traded product and service company for pharmaceutical and consumer packaged goods. In its quarterly report to the Securities and Exchange Commission, plaintiff announced new licensing methods for its newer products. Some commentators viewed this announcement as a way to manipulate its future financial reports and to give the appearance of larger revenues despite no actual revenue increase. Individuals in online stock chat rooms derisively commented about plaintiff's announcement. Defendant placed nine such negative messages about the plaintiff in a Yahoo! chat room. Defendant's postings suggested that the plaintiff intentionally acted in bad faith by giving the appearance of earnings without improving the company. The plaintiff filed suit for defamation and misappropriation of trade secrets. During discovery, the plaintiff moved to obtain the defendant's identity from Yahoo!. The motion judge denied plaintiff's motion. The plaintiff's request for interlocutory appeal was granted.

The Superior Court of New Jersey upheld the motion judge's decision. The court held that the plaintiff must establish a *prima facie* case against the defendant in order to overcome the protection provided to the defendant by the First Amendment. The typical standard to evaluate a discovery request is a generous motion-to-dismiss standard. However, there is a higher burden of proof where the right to free speech is at risk. The plaintiff is required to show that an act giving rise to civil liability actually occurred and the discovery is aimed at revealing the identity of the person who committed the act. The court reasoned that the First Amendment protected all speech, including anonymous speech over the Internet. The court advised that trial courts must carefully balance the need for injured parties to seek redress and the essential right to anonymously participate in online forums.

DVD COPY CONTROL ASSOCIATION V. BUNNER

93 Cal. App. 4th 648 (Cal. App. 6th. 2001)

The Court of Appeal of California, Sixth Appellate District, examined whether the publication of decryption software on the Internet is protected by the First Amendment or violates the Uniform Trade Secrets Act ("UTSA"). The court held that the defendant's use of DeCSS was protected by the First Amendment.

Plaintiff DVD Copy Control Association ("DVDCAA") brought suit against the defendant, claiming that he had violated the UTSA and a click wrap license by using DVD decryption software called DeCSS to play an encrypted DVD on a system not controlled by the DVDCAA's content scrambling system ("CSS"), and by republishing or linking to DeCSS on the Internet. The defendant argued that enjoining him from disclosing DeCSS on the Internet would violate his First Amendment rights because it constituted an unconstitutional prior restraint. The Santa Clara County Superior Court granted DVDCAA a preliminary injunction, holding that CSS, which embodied DVDCCA's trade secret, had been reverse engineered. Since the UTSA allows for reverse engineering, the publication of CSS would only be illegal if the user was subject to the licensing agreement. That issue would not be resolved without discovery, but the balance of hardships favored a preliminary injunction for DVDCAA. The defendant would only have to remove the trade secret information from their websites and would be free to publicly debate the matter until resolved at trial. Without the injunction, however, the plaintiff may lose the trade secret permanently.

Bunner appealed the lower court's decision, claiming that he did not decrypt the software and that the First Amendment protected his publication of the decryption software on the web. He first claimed that he did not decrypt DVDCAA's software because the "master keys" on a CSS-encrypted DVD could be derived exclusively from the DVD itself without recourse to decryption technology. General copying of DVDs was not feasible because removal media did not have the capacity to hold the enormous files necessary for movies. Second, Bunner argued that he republished the DeCSS source code on his website so programmers could improve the code and Linux users could use it to play DVDs. At the time, he had no knowledge that CSS contained trade secrets, and believed that it had been created either independently or through legal reverse engineering. Furthermore, he contended that CSS was no longer a trade secret because it had been previously published on the Internet.

The Fourth Circuit reversed the lower court on two grounds—the UTSA's "improper means" requirement and the First Amendment. The UTSA prohibits appropriation of trade secrets by "improper means." A plaintiff claiming misappropriation has the burden of identifying those trade secrets. While Bunner did not use improper means to obtain DVDCCA's proprietary information, DVDCCA would likely have proven that Bunner knew CSS was a trade secret. However, the court concluded that DeCSS is speech and, therefore, protected by the First Amendment. While source code can be compiled, it retains its fundamentally expressive nature and remains the preferred mode of communication among programmers. The preliminary injunction was overturned, because it unduly restrained free speech.

ELDRED V. RENO

239 F.3d 372 (D.C. Cir. 2001)

The United States Court of Appeals for the District of Columbia Circuit addressed Copyright Clause and First Amendment constitutional challenges to the Copyright Term Extension Act of 1998 ("CTEA"). The Court held that the statutory extension of copyright durations was constitutional.

Plaintiff, corporations, associations and individuals using works in the public domain for vocational and personal uses, filed suit against the Attorney General claiming that CTEA was unconstitutional. The plaintiffs alleged that the extension of copyright protection provided for in CTEA violated their First Amendment freedom of expression rights and conflicted with the Copyright Clause's goal of "promoting the Sciences and Useful Arts." The plaintiffs argued that: (1) the extension of copyright protection by CTEA violates freedom of speech under the First Amendment, (2) CTEA cannot retroactively extend already existing copyright protection because, as the work already exists, it lacks the originality required for the grant of copyright protection, and (3) CTEA violates the constitutional requirement that copyright protection endure for a "limited time." The district court entered judgment on the pleadings in favor of the defendant and dismissed the plaintiffs' claim in its entirety, holding that the extension is permissible since the "limited time" clause is subject to the discretion of Congress.

The D.C. Circuit affirmed the decision of the district court, holding that CTEA does not violate freedom of speech under the First Amendment because copyright protection only covers particular instances of expression and not the ideas expressed therein. Due to exceptions for expression based on the idea/expression dichotomy, the court held that copyrights are categorically immune from challenges under the First Amendment. Plaintiffs lack any cognizable First Amendment right to exploit the copyrighted works of others. Rejecting the plaintiffs' second argument, that existing works are not original for purposes of the extension of copyright protection, the court found that the test for originality only applies when the work is initially created. The fact that a work has copyright protection demonstrates that it fulfilled the originality requirement. Stating that the preamble to the Copyright Clause does not limit the power of Congress to define the duration of copyright protection, the Appellate court also rejected the plaintiffs' third contention. In sum, the Appellate court affirmed the district court's decision that the CTEA is a proper exercise of Congress's power under the Copyright Clause of the Constitution.

On February 19, 2002, the United States Supreme Court granted Plaintiffs' Petition for *Certiorari*.

GUEST V. LEIS

255 F.3d 325 (6th Cir. 2001)

The Sixth Circuit ruled on the protection afforded by the First and Fourth Amendments, the Electronic Communications Privacy Act ("ECPA") and the Privacy Protection Act ("PPA") for preventing the seizure of an entire computer when only a fraction of the information on it is connected to possible illegal activities.

Plaintiffs were users and operators of Internet bulletin board systems. The Regional Electronic Computer Intelligence Task Force ("RECI") downloaded obscene images from the bulletin boards. Based on these images, the RECI obtained search warrants and seized computer equipment associated with the bulletin boards. The plaintiffs brought suit against the RECI, the Sheriff, and the Sheriff's Department for violations of the First and Fourth Amendments, the ECPA and the PPA. The district court granted the defendants' motion for summary judgment on all claims. Plaintiffs appealed.

The Sixth Circuit affirmed the district court's decision. On the Fourth Amendment count, plaintiffs claimed that their expectation of privacy had been violated. The court held that there was no expectation of privacy when a privacy disclaimer is posted or when the information is provided to a third party, nor is there privacy for a delivered e-mail. Plaintiffs also claimed that the defendants exceeded the scope of the warrant. The court held that if the plaintiffs could not show that the defendants accessed files beyond those specified in the warrant, plaintiffs could not show invasion of privacy. Further, the court held that it is reasonable to seize an entire computer because it is difficult to search the computer in a suspect's home.

As to the First Amendment claim, plaintiffs alleged that the defendants unlawfully placed a restraint on their speech because the material in question had not yet been determined obscene in an adversarial proceeding. The court held that evidence for a criminal prosecution that would be preserved (i.e., not destroyed) need not first be determined obscene to avoid violation of First Amendment rights. The court ruled that governmental search with a warrant does not violate the privacy created by the ECPA. Regarding the PPA claim, the court held that when protected materials are co-mingled on a computer with criminal evidence, seizure of the computer is warranted; officials cannot, however, search PPA-protected materials.

KYLLO V. UNITED STATES

533 U.S. 27 (2001)

The Supreme Court decided whether law enforcement's use of thermal imaging on citizens' homes violates their Fourth Amendment rights. The Court held that "[w]here . . . the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant."

A United States Department of the Interior agent suspected defendant Danny Kyllo of growing marijuana in his home. Indoor marijuana growth requires high-intensity lamps that give off significant heat. To investigate the defendant, the agent used a thermal imager to search for heat emanating from the defendant's home. Upon collecting high thermal measurements, the agent used these measurements and additional evidence to secure a warrant to search the defendant's home. The search yielded 100 marijuana plants. The defendant was indicted on one count of manufacturing marijuana. The district court granted the defendant's motion to suppress the evidence from the search, and entered a conditional guilty plea. On appeal, the Ninth Circuit remanded for a hearing on the intrusiveness of thermal imaging. The district court then held that the thermal scan was nonintrusive, and, therefore, permissible, because it cannot penetrate into the structure or reveal intimate details of the home. The Ninth Circuit initially reversed, but the opinion was withdrawn. A subsequent Ninth Circuit panel affirmed the district court. This panel reasoned that the defendant showed no expectation of privacy because he did not conceal the heat escaping from his home, and that the thermal scan did not reveal intimate details of his life.

The defendant appealed. The Supreme Court reversed and held that the thermal imaging was an unlawful search. A Fourth Amendment search occurs when the government violates a subjective expectation of privacy which society recognizes as reasonable, as previously stated by the Court in *Katz v. United States,* 389 U.S. 347 (1967), a case involving the use of an electronic listening device. The Court viewed use of electronic listening devices, thermal imagers and satellite scans as unreasonable searches. When sense-enhancing technology is used to obtain information about the interior of the home that could not otherwise have been obtained without physical intrusion into a constitutionally protected area, and the technology used to search the home is not in general public use, an impermissible search has occurred.

The government argued that it only detected heat radiating off the walls of the house, and that this is different from sound traveling through the walls. The Court rejected this argument, stating that such a distinction is mechanical and would result in permitting searches with more sophisticated technology in the future. The Court further stated that all details of the home are intimate details because of their inaccessibility to government officials. "In the home, our cases show, *all* details are intimate details, because the entire area is held safe from prying government eyes." To consider some details of the home intimate and others not, would result in ambiguity for the courts and for law enforcement officials.

NATIONAL A-1 ADVERTISING, INC. V. NETWORK SOLUTIONS, INC.

121 F. Supp. 2d 156 (D.N.H. 2000)

The United States District Court for the District of New Hampshire ruled on the issue of whether Network Solutions, Inc.'s ("NSI") refusal to register second-level domain names under its "decency policy" violated the plaintiff's First Amendment rights. The court recognized no constitutionally protected right to include particular words or phrases in the space occupied by second-level domain names.

The plaintiff sought to register with NSI a number of domain names that contained allegedly offensive words. NSI refused to register those domain names under its decency policy. The plaintiff brought an action against NSI, seeking a declaration that NSI's refusal to register its proposed domain names violated its First Amendment right to freedom of speech.

The district court granted NSI's motion for summary judgment, and held that NSI's actions did not violate the plaintiff's First Amendment rights. The court noted the First Amendment only "proscribes governmental conduct, not conduct undertaken by private citizens," and that NSI was not a state actor at the time of registration. In its analysis, the court first noted there was no evidence that the government sought to evade its responsibilities by delegating them to private entities such as NSI. Second, there was no evidence that the government imposed any regulatory restrictions on registering second-level domain names. Finally, the court was not persuaded that the relationship between the government and NSI could properly be viewed as "symbiotic."

The court further held that even if NSI qualified as a government actor, it did not violate the plaintiff's First Amendment rights because the space occupied by second-level domain names was not designed, intended, or traditionally employed to act as a forum for speech. The court explained that second-level domain names essentially serve the utilitarian role of identifying computer addresses. "That some people might want to express points of view or attempt to convey a particular message by converting the second-level domain name space into a message-carrying vehicle, does not operate to convert that space into a 'forum' for speech."

BERKELEY TECHNOLOGY LAW JOURNAL
ANNUAL REVIEW OF LAW AND TECHNOLOGY

BUSINESS LAW