ADDITIONAL DEVELOPMENTS—CYBERLAW

IN RE DOUBLECLICK PRIVACY LITIGATION

154 F. Supp. 2d 497 (S.D.N.Y. 2001)

The United States District Court for the Southern District of New York ruled on whether Internet cookies violate Title II of the Electronic Communications Privacy Act ("ECPA"), the Federal Wiretap Act, and the Computer Fraud and Abuse Act. The court held that the plaintiff had failed to adequately plead violations of each of the above statutes.

Doubleclick acts as an intermediary, helping advertisers place ads on web sites. Doubleclick uses "cookies" to collect information from users, tracking web usage and submission information. As a user navigates a participating web site or submits information, this usage information is added to Doubleclick's cookie and is sent to Doubleclick's computers. Doubleclick processes this information to determine the appropriate advertisement to display as a "banner" ad on the web page. Plaintiffs brought a class action suit under three federal law claims and four state law claims. The federal claims were under Title II of the ECPA, the Federal Wiretap Act, and the Computer Fraud and Abuse Act. On defendants' motion to dismiss on the pleadings, the district court found for the defendants. As a result, the state claims, under common law and New York law, were not considered by the district court.

Title II of the ECPA prohibits unauthorized access to information (e.g., "hacking"). It provides an exception for conduct authorized by a user of the service, regarding communication of or intended for that user. Doubleclick argued that its conduct fell under this exception. The court held that the exception was not an affirmative defense. Thus, Doubleclick did not have the burden of proving its actions fell within the exception. Next, the court held that the websites that posted the ads were the "users" referred to in the exception. Finally, the court held that the website's authorization of Doubleclick's access and the information posted by individual users to web sites was information "intended for" the websites. Thus, the court held that there was no issue for the court to decide under the ECPA claim.

Doubleclick also claimed that its conduct fell within the exception to the Federal Wiretap Act, which provides that intercepting an electronic communication is lawful unless done for the purpose of committing a criminal or tortious act. The court held that in determining the purpose of a defendant's action, it was not enough to prove that the act was tortious. The plaintiff must also show that the act was done with tortious purpose. Since the plaintiffs did not plead that Doubleclick acted with tortious purpose, the court held there were no issues remaining to be tried under this act.

The Computer Fraud and Abuse Act provides relief for those who suffer damage or loss as a result of unauthorized access to computer information. The statute defines "damage" as a loss of at least $5,000 during any one year. Plaintiffs argued that the statute defined "loss" differently from "damage," and that they should not be subject to the $5,000 limitation. The court held that "loss" was not intended as an exception to the $5,000 limit, and, therefore, that the plaintiff did not plead damages that were entitled to relief.

KONOP V. HAWAIIAN AIRLINES, INC.

236 F.3d 1035 (9th Cir. 2001)

The Ninth Circuit ruled on whether an employer's intrusion into an employee's private website violates the Electronic Communications Privacy Act ("ECPA"). Deciding that accessing messages in transit and accessing stored messages were legally indistinguishable activities, the court held that the employer's action could constitute a violation of the ECPA.

Plaintiff was a pilot working for defendant. Plaintiff maintained a website that criticized his employer. The website was available only to employees, and not to managers or union representatives. The vice president of defendant company used the names of two employee pilots to access the plaintiff's website. Thereafter, the plaintiff was placed on medical suspension. Plaintiff brought suit alleging tort claims, retaliatory suspension, federal labor claims, and federal wiretap claims under the ECPA and Stored Communications Act. The district court dismissed all but the retaliatory suspension claim on summary judgment. The district court ruled for the defendant on the suspension claim after a bench trial. Plaintiff appealed the grant of summary judgment on the wiretap and labor claims and final judgment of retaliation claim.

On the wiretap claim, the Ninth Circuit held that the plaintiff had raised a material question of fact and summary judgment should not have been granted. Under the ECPA, which amended the Federal Wiretap Act, there is no difference between intercepting messages in transit and accessing communications in storage. Further, private messages should not be differently protected simply because they are transmitted by different modes of communication (i.e., voicemail versus e-mail). The court held that exceptions to the ECPA do not apply because the website was not publicly available and was accessed using the account of an employee that was not party to the communication.

On the labor claim, the defendant asserted that there was a lack of jurisdiction, that the plaintiff forfeited his right to protection, and that the claims lacked sufficient evidentiary support. However, the court held that statutory provisions are properly triable in federal court, and that the postings on the protected site raised a triable issue as to whether the plaintiff was participating in a protected activity.

NETWORK SOLUTIONS, INC. V. UMBRO INTERNATIONAL, INC.

259 Va. 759 (S. Ct. 2000)

The Virginia Supreme Court heard the issue of whether a domain name is a form of property that is subject to garnishment. The court, by a vote of five to two, did not sanction the garnishment of Network Solutions, Inc.'s services under the present Virginia garnishment statutes, although domain names are being bought and sold in today's marketplace.

Umbro International, Inc. ("Umbro") obtained a default judgment against the registrant of the Internet domain name www.umbro.com, a Canadian corporation that was the judgment debtor. It went on to obtain a *writ of facias* and institute garnishment proceeding against the judgment debtor. In the garnishment summons, Umbro named Network Solutions, Inc. ("NSI") as the garnishee and sought to garnish thirty-eight Internet domain names that the judgment debtor had registered with NSI. NSI opposed the motion and garnishment on the grounds that the judgment debtor's domain name registration agreements with NSI were contracts for services, and, thus, not subject to garnishment. The lower court ruled that the domain names were "valuable intangible property subjected to garnishment", and ordered NSI to deposit control of all the judgment debtor's domain name registrations into the court's registry for sale by the sheriff's office.

Reversing the lower court's decision, the Virginia Supreme Court dodged the question of whether a domain name was a form of intellectual property, and held that domain names are not subject to garnishment under Virginia state law. Under Virginia Code section 8.01-511, a garnishment summons may be issued with respect to "a liability on any person other than the judgment debtor . . . ." The court held that a domain name registered by NSI was not a liability within the meaning of this statute, explaining that a domain name registration resulted from a contract between the registrar and registrant to use a unique domain name for a specific period of time. A contract for services cannot be a liability as the term is used in the statute. Therefore, it cannot be garnished. The court further reasoned that allowing the garnishment of NSI's services would open the door to garnishment of "practically any service."

In his dissent, Justice Compton disagreed that the right to use a domain name was a contract for services. Rather, Justice Compton found that domain name was a form of intangible personal property, and, therefore, that the judgment debtor, by virtue of the domain name registration agreement with NSI, had a current possessory interest in the property. Justice Compton would thus affirm the judgment of the lower court and hold the domain names subject to garnishment.

UNITED STATES V. COHEN

260 F.3d 68 (2d. Cir. 2001)

The Second Circuit ruled on the issue of whether Internet gambling from a foreign country violated the law as an illegal transmission of bets in foreign commerce, a transmission of communication entitling recipient to receive money as a result of bets, and providing information assisting betting. The court held that the defendant violated 18 U.S.C. § 1084 and that the safe harbor provision contained in 18 U.S.C. § 1084(b) did not apply to the defendant.

The defendant operated a sports-betting service from Antigua. Gamblers would send money to Antigua and communicate by telephone or the Internet to place bets. The defendant was arrested for illegal transmission in foreign commerce of bets or wagers under 18 U.S.C. § 1084(a)(1), transmission of communication entitling recipient to receive money as a result of bets under 18 U.S.C. § 1084(a)(2), and providing information assisting betting under 18 U.S.C. § 1084(a)(3). The defendant was convicted and appealed. The following six issues were on appeal: (1) whether the Government was required to prove a "corrupt motive" in connection with the conspiracy in this case; (2) whether the district court properly instructed the jury to disregard the safe harbor provision contained in section 1084(b); (3) whether Cohen "knowingly" violated section 1084; (4) whether the rule of lenity requires a reversal of Cohen's convictions; (5) whether the district court constructively amended Cohen's indictment in giving its jury instructions; and (6) whether the district court abused its discretion by denying Cohen's request to depose a foreign witness.

The Second Circuit upheld the conviction in its entirety. The defendant argued that corrupt motive was a necessary element for conviction. The court disagreed, reasoning that ignorance of the law is no excuse, and that all that was required for a conviction under these laws was that the defendant knowingly committed the illegal acts. The defendant then argued that certain actions fell within a safe harbor provision for permissible communications. The court found that defendant's conduct did not fit under any safe harbor provision, principally because gambling was illegal in the locations in which the gamblers placed their bets. Defendant also lost on arguments of lenity, improper amendment of charges, and failure to grant a motion to depose a foreign witness.