ADDITIONAL DEVELOPMENTS—CYBERLAW

PEBBLE BEACH COMPANY V. CADDY

453 F.3d 1151 (9th Cir. 2006)

In *Pebble Beach*, the United States Court of Appeal for the Ninth Circuit affirmed the dismissal of the plaintiff's claim for lack of personal jurisdiction. The court, following the "minimum contacts" test, held that the foreign business owner's "passive" website was insufficient to show a purposeful availing by the defendant of the privilege of conducting activities in California, or the United States as a whole.

Plaintiff Pebble Beach Company, proprietor of a well-known golf course in Monterey County, California, had used the trade name "Pebble Beach" for 50 years and maintains a website at www.pebblebeach.com. Defendant Michael Caddy, a dual citizen of the United States and the United Kingdom, operated a bed-and-breakfast in southern England named "Pebble Beach" and advertises it at www.pebblebeach-uk.com. This site contained information about lodging rates and accommodations, but was "passive" insofar as it lacks interactive features, like a reservation system.

In 2003, Pebble Beach sued Caddy for intentional infringement and dilution of its "Pebble Beach" mark under the Lanham Act and the California Business and Professions Code. The district court dismissed Pebble Beach's claim for lack of personal jurisdiction, and Pebble Beach appealed.

The Ninth Circuit affirmed the district court's dismissal for lack of personal jurisdiction, finding that passive websites like Caddy's were an insufficient basis for asserting personal jurisdiction. Despite state and federal long-arm statutes, Pebble Beach failed to establish that Caddy had "minimum contacts" with either California or the United States by (1) purposefully availing himself of the privilege of conducting activities in California or the United States as a whole; or (2) that he purposefully directed its activities toward one of those two forums.

The court found that Pebble Beach failed to identify any conduct by Caddy that took place in California or in the United States that would invoke the benefits and protections of the laws of the forum. The court also found that Caddy's registration of a domain name or creation of a passive website, which did nothing to encourage residents from the forum state to act, lacked the "something more" required for Caddy to have "expressly aimed" his conduct at California or the United States, regardless of their foreseeable effects.

UNITED STATES V. ZIEGLER

474 F.3d 1184 (9th Cir. 2007)

The US Court of Appeals for the Ninth Circuit held that although the defendant's subjective expectation of privacy in his office and computer was also objectively reasonable, his employer maintained the authority to consent to the search of his workplace environment. The resulting evidence, images of child pornography stored on the computer, copied from the defendant's computer were therefore admissible.

In 2001, the director of a company that served as an internet service provider to Frontline Processing, Inc. ("Frontline"), Ziegler's employer, contacted the FBI with a tip that a Frontline employee had been accessing child pornographic websites from a company computer. The FBI then contacted Softich, Frontline's IT Administrator, who confirmed that such sites had indeed been accessed. Softich told the FBI that Frontline was using a firewall, which allowed constant monitoring of employees' internet activities, and that the employees were aware of this practice. Softich identified Ziegler's computer as the one involved. Softich then told the FBI agent that the IT department had already installed a monitoring device inside the computer.

The parties dispute whether the FBI agent then instructed Softich to copy Zeigler's hard drive, or merely to safeguard the backup copy of the hard drive, which the IT department already had. However, the parties did not dispute that on January 30, 2001, Softich obtained a key to Zeigler's office from Frontline's chief financial officer, opened Ziegler's computer, and made two copies of its hard drive.

In May of 2003, Ziegler was indicted for receipt of child pornography, possession of child pornography and receipt of obscene material. Ziegler filed a pretrial motion to suppress the evidence, claiming that the FBI violated the Fourth Amendment when it directed the Frontline employees to search his computer without first obtaining a warrant. The government countered that Softich had copied the hard drive without any instructions from the agent, and discounted the contradictory accounts of the event as a misunderstanding. The court ruled that this dispute was secondary to the issue of Ziegler's expectation of privacy in his workplace computer.

As the court noted, a legitimate expectation of privacy is established when the claimant can show that he had a subjective expectation, and when such subjective expectation is objectively reasonable. The government did not dispute Ziegler's subjective expectation of privacy and found it to be objectively reasonable for a private employee to retain at least some expectation of privacy in her office. Zeigler's office was not shared with co-workers and had a separate lock, facts supporting his reasonable belief in privacy.

The retrieval of Zeigler's hard-drive was justified by the court as complying with the Fourth Amendment because Zeigler's private employer had retained the right to consent to the search. By receiving permission to conduct the search from the employer's Chief Financial Officer, the search had received valid consent.

YAHOO! INC. V. LA LIGUE CONTRE LE RACISME ET L'ANTISEMITISME

433 F.3d 1199 (9th Cir. 2006), cert. denied, 126 S.Ct. 2332 (2006)

In *Yahoo! Inc. v. La Ligue Contre Le Racisme et L'Antisemitism*, a divided panel of the Ninth Circuit held that the lower court properly exercised personal jurisdiction over two French associations by virtue of their filing and the prosecution of the action in France was an intentional act, expressly aimed at the forum state, causing harm that the associations knew was likely to be suffered in the forum state., but reversed and remanded because the suit was not sufficiently ripe for judicial decision.

Two French associations, La Ligue Contre Le Racisme et L'Antisemitisme ("LICRA") and L'Union des Etudiants Juifs de France ("UEJF"), originally brought an action against Yahoo! Inc. ("Yahoo!") in the Tribunal de Grande Instance de Paris because Yahoo! had presented Nazi objects and memorabilia for sale in violation of French law. The French court issued an order requiring Yahoo! to "dissuade and render impossible any access" to sites or services "that may be construed as constituting an apology for Nazism or a contesting of Nazi crimes" or face a penalty of 100,000 Euro per day per violation.

Yahoo! sought a declaratory judgment in a California federal court that the French court's orders were unenforceable. The district court found that it could exercise personal jurisdiction over the French parties, that the dispute was ripe, and that the French court's orders were unenforcable because they violated the First Amendment. Shortly thereafter, Yahoo! adopted a new policy prohibiting use of auctions or classified advertisements for items "associated with or could be used to promote or glorify groups that are known principally for hateful and violent positions directed at others based on race or similar factors." Yahoo! represented that its new policy was unrelated to the the French court's orders.

In an 8-3 decision, the Ninth Circuit held that *Calder v. Jones*, 465 U.S. 783 (1984) controlled and that personal jurisdiction over the two French associations was proper because their filing an action against Yahoo! in a French court constituted an intentional act expressly aimed at the forum state causing harm that the French associations knew was likely to be suffered in the forum state.

However, a three judge plurality of the panel decided that the case was not ripe for judicial determination. Yahoo!'s voluntary change of policy brought it "in large measure" into compliance with the French court order, rendering penalties highly unlikely. Thus, the Ninth Circuit did not address the lower court's holding with respect to the First Amendment.

SNOW V. DIRECTV, INC.

450 F.3d 1314 (11th Cir. 2006)

The United States Court of Appeal for the Eleventh Circuit held that a website owner failed to state a claim under the Stored Communications Act (SCA) against DirecTV. Although the website expressly forbade access to DirecTV, required users to register, create a password, and agree to additional terms that affirmed the non-association with DirecTV, there was nothing inherent in any of these steps to infer that access to the website by the general public was restricted.

DirecTV, a satellite television provider, was engaged in a nationwide effort against those intercepting and pirating the company's encrypted satellite transmissions using "pirate access devices." One of these actions was against Michael Snow, eventually dismissed without prejudice.

In response to this campagn, Snow created a non-commercial website, http://www.stop-corporate-extortion.com as a "private support group" for "individuals who have been, are being, or will be sued by any Corporate entity." The website's homepage explicitly forbade access to DIRECTV and its agents, and users of the site to register, create a password, and agree to additional terms reaffirming non-association with DirecTV. A person clicking "I Agree to these terms" could enter, view, and participate in the electronic bulletin board.

Snow alleged that employees of DirecTV and two of its law firms accessed the website on numerous occasions in violation of the SCA. The SCA prohibits intentional accessing or exceeding authorization to access an electronic communication while in electronic storage. The United States District Court for the Middle District of Florida dismissed the complaint because the electronic bulletin boards were not "in electronic storage" and, therefore, not protected by the SCA.

The Eleventh Circuit affirmed the district court's determinations to dismiss Snow's claim for lack of personal jurisdiction and failure to state a claim. The lower court found that Snow's electronic bulletin board was not within the scope of electronic communication in electronic storage as contemplated by the SCA. The Eleventh Circuit affirmed on different grounds, finding Snow's website "readily accessible to the general public" and therefore explicitly exempt from the SCA under 18 U.S.C. § 2511(2)(g). Requiring registration, the creation of a password, and clicking "I Agree to these terms" were insufficient restrictions on public access and instead constituted a self-screening process by which non-intended users would voluntarily excuse themselves.

BEYOND SYSTEMS INC. V. KEYNETICS INC.

422 F.Supp.2d 523 (D. Md. 2006)

The United States District Court for the District of Maryland held that Maryland's anti-spam statute—the Maryland Commercial Electronic Mail Act ("MCEMA")—did not violate Dormant Commerce Clause of the Constitution and was not preempted by the federal anti-spam legislation, Controlling the Assault of Non-Solicited Pornography and Marketing Act 15 U.S.C. § 7707 ("CAN-SPAM Act").

Beyond Systems, Inc ("BSI"), a Maryland based ISP, brought suit against Keynetics, Inc., Jeffrey Mulligan, the operator of two websites, and Rackspace Ltd., an ISP that facilitated their actions. The suit alleged that BSI had received over 6,000 unsolicited commercial e-mails on behalf of the defendants, in violation of the MCEMA.

Keynetics, trading under the name ClickBank, operated a website selling digital products from various venders and used a network of online affiliates to drive potential customers to ClickBank's website, primarily through bulk e-mail. The referring affiliate received a commission for any completed sales. Jeffrey Mulligan is the sole proprietor of CBmall, a website similar to ClickBank, though it re-routed all of its customers to ClickBank for actual purchase. Rackspace Ltd., the ISP, provided hosting services for the e-mail sent by Keynetics, Mulligan, and their affiliates.

BSI alleged that the e-mails it received were prohibited by MCEMA and that the defendants had notice of BSI's objections. Keynetics and Rackspace moved for summary judgment on the grounds that the MCEMA imposed an undue burden on interstate commerce in violation of the Dormant Commerce Clause of the Constitution

The court examined the legitimacy of the state's interest and weighed the burden on interstate commerce in light of the local benefit derived from the statute. The court relied upon *Washington v. Heckle*, 24 P.3d 404 (Wash. 2001), in which the Washington Supreme Court upheld the constitutionality of an "essentially identical" Washington anti-spam statute challenge on the same grounds. The court also relied on *MaryCLE, LLC v. First Choice Internet, Inc.*, 890 A.2d 818 (Md. Ct. Spec. App. 2006), which applied the reasoning from *Heckle* to the MCEMA and held it constitutional.

The court also rejected Keynetics' argument that MCEMA was preempted by the CAN-SPAM Act. At least in the situations where an action under MCEMA was against a non-resident defendant, the MCEMA was "in no way inconsistent with CAN-SPAM" because CAN-SPAM did not preempt any "statute, regulation, or rule [which] prohibits falsity or deception in any portion of a commercial electronic mail messages or information attached thereto."

COMMUNICATIONS DECENCY ACT (CDA) IMMUNITY

BARNES V. YAHOO! INC.

No. Civ. 05-926-AA, 2005 WL 3005602 (D. Or., Nov. 8, 2005)

LANDRY-BELLE V. VARIOUS, INC.

No. 05-1526, 2006 WL 1676136 (W.D. La., June 9, 2006)

PRICKETT V. INFOUSA, INC.

No. 4:05-CV-10, 2006 WL 887431 (E.D. Tex., Mar. 30, 2006)

DIMEO V. MAX

433 F. Supp. 2d 523 (E.D. Pa. 2006)

ANTHONY V. YAHOO! INC.

421 F. Supp. 2d 1257 (N.D. Cal. 2006)

DOE V. BATES

No. 5:05-CV-91-DF-CMC, 2006 WL 3813758, (E.D. Texas, Dec. 27, 2006)

Over the past year, courts have clarified and expanded the immunity afforded to interactive computer services under the Communications Decency Act, 47 U.S. § 230(c)(1).

In *Barnes v. Yahoo!, Inc.*, the United States District Court for the District of Oregon granted defendant Yahoo!'s motion to dismiss, ruling that Yahoo! qualified for immunity as an interactive service provider notwithstanding the company's failure to remove a false online profile of Cecilia Barnes after a company representative allegedly assured Barnes that it would do so. Barnes argued that her claims under Oregon tort law relied only on defendant's liability for failing to fulfill its alleged promise and thus were not barred by § 230 immunity. The court rejected this argument; since Barne's ex-boyfriend, not Yahoo!, had created the offensive material, Yahoo! was immune from liability as publisher of the false online profile.

Similar facts in *Landry-Belle v. Various, Inc.* led the United States District Court for the Western District of Louisiana to grant defendant Various, Inc.'s motion to dismiss claims relating to a false and obscene profile of Shelly Landry-Belle posted on an adult-oriented site owned and operated by Various. Even though Landry-Belle believed her ex-boyfriend created the profile with her picture, she claimed Various acted as an information content provider, and thus not afforded § 230(c)(1) immunity. Various created the entry form used to accept the false profile and subsequently added keywords to the profile, categorizing it, and submitting it to search engines. The court held that the "web-

site's role in eliciting the information at issue [does] not deprive the website operator of immunity under the CDA."

The plaintiffs in *Prickett v. infoUSA, Inc.*, in the United States District Court for the Eastern District of Texas, also failed to convince the court that creating an online form with informational prompts sufficed to abrogate the defendants' immunity. The plaintiffs brought tort claims based on infoUSA's listing of their home addresses and phone numbers under the heading "Entertainers—Adult" on both infoUSA's own website and other websites licensing infoUSA's database of business listings, including Yahoo! Local and Yahoo! Yellow Pages. The court ruled in favor of defendants infoUSA, dismissing a motion for summary judgment. After rejecting the informational prompts argument, the court went on to hold that a defendant retains immunity under the CDA even if it later provides content to a third party, like a search engine. The court held that even though infoUSA's new business listing entry form contained an assurance that it "call[ed] every [new] business to verify" each listing, § 230(c)(1) immunity could not be lost due to a failure in verifying anonymous third party's entry of plaintiffs' contact information along with false, damaging information. Citing *Barnes*, the court found that to hold infoUSA liable for its failure to verify the listing would be "treating it as a publisher," a claim necessarily barred by § 230(c)(1).

In *Dimeo v. Max*, plaintiff Anthony Dimeo, III filed a complaint against Tucker Max for defamatory remarks about Dimeo posted on defendant's website, a gossip and entertainment site. The site's message boards included harsh comments about Dimeo from anonymous individuals which had been edited and selectively posted by Max. Despite criticizing the site as coarse and vulgar, the United States District Court for the Eastern District of Pennsylvania granted Max's motion for summary judgment with regard to § 230 immunity. First, the court classified Max's site as an interactive computer service providing a "service" that "enables computer access" by multiple users to a server. Second, the court ruled that Max's editorial control had not risen to the level of an information content provider's "development of information," therefore being insufficient to void § 230(c)(1) immunity.

The United States District Court for the Northern District of California in *Anthony v. Yahoo!, Inc.* found that § 230 did not immunize Yahoo! from fraud and negligent misrepresentation claims regarding the defendant's online dating services. Plaintiff Robert Anthony claimed Yahoo! created and forwarded false or expired user profiles to misrepresent the number of eligible singles using the service, thereby coaxing non-members to join and current members to renew the service. Yahoo!'s role in creating misrepresentative marketing communications with expired profiles, as well as the plaintiff's unopposed contention that Yahoo! created false profiles could not garner § 230 immunity.

In *Doe v. Bates*, the plaintiffs claimed that Yahoo! was liable for harm to their minor son as a result of pornographic photographs of him posted in a Yahoo! e-group. The United States District Court for the Eastern District of Texas granted Yahoo!'s motion to dismiss adopting the report and recommendations of the magistrate judge.

The magistrate judge found that Yahoo! met the requirements of § 230(c)(1) immunity because it had not participated in the creation of the content at issue (the photos) and that the plaintiffs' claims as to Yahoo!'s failure to "overs[ee] and intervene" postings on the "Candyman" Yahoo! group (a group centered on sharing hard-core child pornography) necessarily required the content to have been furnished by another content provider, the exact scenario § 230(c)(1) protects. The magistrate also rejected the plaintiffs' assertion that § 230(c)(1) is merely "definitional" and does not itself provide immunity.

The district court also rejected the plaintiffs' contention that there is an exception within § 230 immunity for an intentional violation of criminal law. The plaintiffs asserted that Yahoo! should be liable because it profited from child pornography in violation of 18 U.S.C. § 2252A. The court noted that Congress' intention to immunize providers of interactive computer services was not dependant on how they earned their revenue, and that the immunity was created to protect service providers like Yahoo! from just such liability because of the practical impossibility of monitoring and restricting every Yahoo! group or posting hosted by Yahoo!.

COMPUTER FRAUD AND ABUSE ACT

NILFISK-ADVANCE, INC. V. MITCHELL

2006 WL 827073 (W.D.Ark.)

NEXANS WIRES S.A. V. SARK-USA, INC.

166 Fed.Appx. 559 (2d. Cir. 2006)

These two recent decisions concern the scope of Computer Fraud and Abuse Act (CFAA) and the definition of losses under the Act.

In *Nexan-Wires v. Sark-USA* the United States Court of Appeal for the Second Circuit rejected plaintiffs' CFAA claims for the loss of revenue resulting from the defendant's alleged misappropriation of the plaintiff's protected files because that loss was not caused by the "interruption of service," and was not related to any type of "computer investigation or repair." In contrast, in *Nilfsk-Advance, Inc. v. Mitchell*, the United States District Court for the Western District of Arkansas ruled that the defendant's conduct fell within the CFAA when he accessed the plaintiff's computer with the intention to misappropriate confidential information, even though the defendant was authorized to access the computer.

In *Nexans Wires S.A. v. Sark-USA, Inc*, the Second Circuit addressed the question of what constitutes losses sufficient to state a claim under the CFAA. The plaintiff, a manufacturer of silver-plated copper wire, alleged that individuals employed by distribution affiliates accessed and downloaded the plaintiff's proprietary information. These employees subsequently resigned, and with the help of other named defendants and the downloaded information, formed Sark-USA to compete with plaintiff. Plaintiff brought suit under the CFAA and state law against Sark-USA, Inc. The defendants moved for summary judgment, which the United States District Court for the Southern District of New York denied.

According to § 1030(a)(5)(B)(I) of the CFAA, a plaintiff must have suffered a loss of at least $5,000 in order to state a claim for relief. The CFAA defines a loss as "any remedial costs of investigating the computer for damage, remedying the damage and any costs incurred because the computer cannot function while or until repairs are made." The CFAA only allows plaintiff to include lost revenue when it is lost "because of an interruption of service." The plaintiff in *Nexans Wires* claimed to have met the statutory $5,000 requirement because it (a) lost "profits of at least $10 million," and (b) spent $8,000 in travel expenses when it sent its executives from Germany to New York to investigate the loss of data.

The Second Circuit agreed with the district court that CFAA distinguished "loss of revenue" from "incurred costs," and that the former is only recoverable when it is related to an "interruption of service." The district court rejected the plaintiff's claim for lost revenue because it was undisputed that no interruption of service occurred, and therefore, the losses were not within the scope of CFAA. The district court also rejected the plaintiff's second claim for damages because the travel expenses were related to investigating business losses unrelated to actual computers or computer services.

In *Nilfisk-Advance, Inc. v. Mitchell*, the United States District Court for the Western District of Arkansas ruled on whether an employee violated the CFAA by transmitting company files containing confidential information and trade secrets to his personal computer after having resigned, but prior to actually completing work with the company. Having indicated his intent to leave the company, defendant project engineer Mitchell e-mailed numerous zip files of proprietary and confidential information to his personal e-mail account. He was terminated a week later, and subsequently refused to let Nilfisk inspect his personal computer.

Claiming that Mitchel had exceeded his authorization and intentionally caused damage to plaintiff by transferring files stored on his office computer to his personal e-mail account, Nilfisk brought suit under the CFAA. Nilfisk further alleged that while Mitchell did have the authority to access his computer at work, the transmission of files for the purpose of misappropriation exceeded that authorization. Even though Mitchell had authorization to access the files, the court found the Mitchell's conduct sufficiently excessive to deny Mitchell's motion to dismiss the CFAA claim.

BERKELEY TECHNOLOGY LAW JOURNAL
ANNUAL REVIEW OF LAW AND TECHNOLOGY

CONSTITUTIONAL LAW