ASPEN PUBLISHERS

The Computer & Internet Lawyer

Volume 28 ▲ Number 1 ▲ JANUARY 2011

Ronald L. Johnston, Arnold & Porter, LLP Editor-in-Chief*

Cloud Computing: Recent Cases and Anticipating New Types of Claims

By Mark H. Wittow

Cases relevant to cloud computing arise in a variety of areas of law, as cloud computing is a type of business activity distinct from a unique legal area. Like any area of business activity, particularly those involving computers and digital distribution, cloud-computing-related transactions have and will generate a variety of potential cases:[1]

1. Commercial disputes focused on contract law and business torts;
2. Intellectual property law cases including potential patent, trademark, and copyright infringement, and trade secret misappropriation claims;
3. Claims grounded in privacy, computer fraud, and electronic communication laws that include a private right of action; and
4. Cybercrime cases brought by state and federal prosecutors.

Mark H. Wittow is a partner in the Seattle office of K&L Gates. His work focuses on intellectual property and technology transactions and litigation, including the acquisition, development, marketing, and distribution of computer-related technologies, media content, and other types of technology, intellectual property, and electronic commerce issues. He is the current chair of the ABA Intellectual Property Law section's Information Technology Division and former co-chair of its Software, Online Trademarks, and Databases committees. The author thanks K&L Gates Law Librarian Warner Miller for his assistance in updating this article for publication in *The Computer and Internet Lawyer.*

Recent Cases

Cartoon Network v. CSC Holdings,[2] also known as the *Cablevision* case (the dba of CSC Holdings), addressed cloud-based digital television services, specifically whether a television cable service's operation of a remote storage digital video recorder (RS-DVR) system and the related serving of content constituted copyright infringement. The Second Circuit held that Cablevision did not directly infringe copyrights by offering its RS-DVR system to consumers. Cablevision's RS-DVR system allowed its customers to store recorded television shows on a central server rather than on a hard drive in the customer's home. The operation of the system involved the

Wolters Kluwer
Law & Business

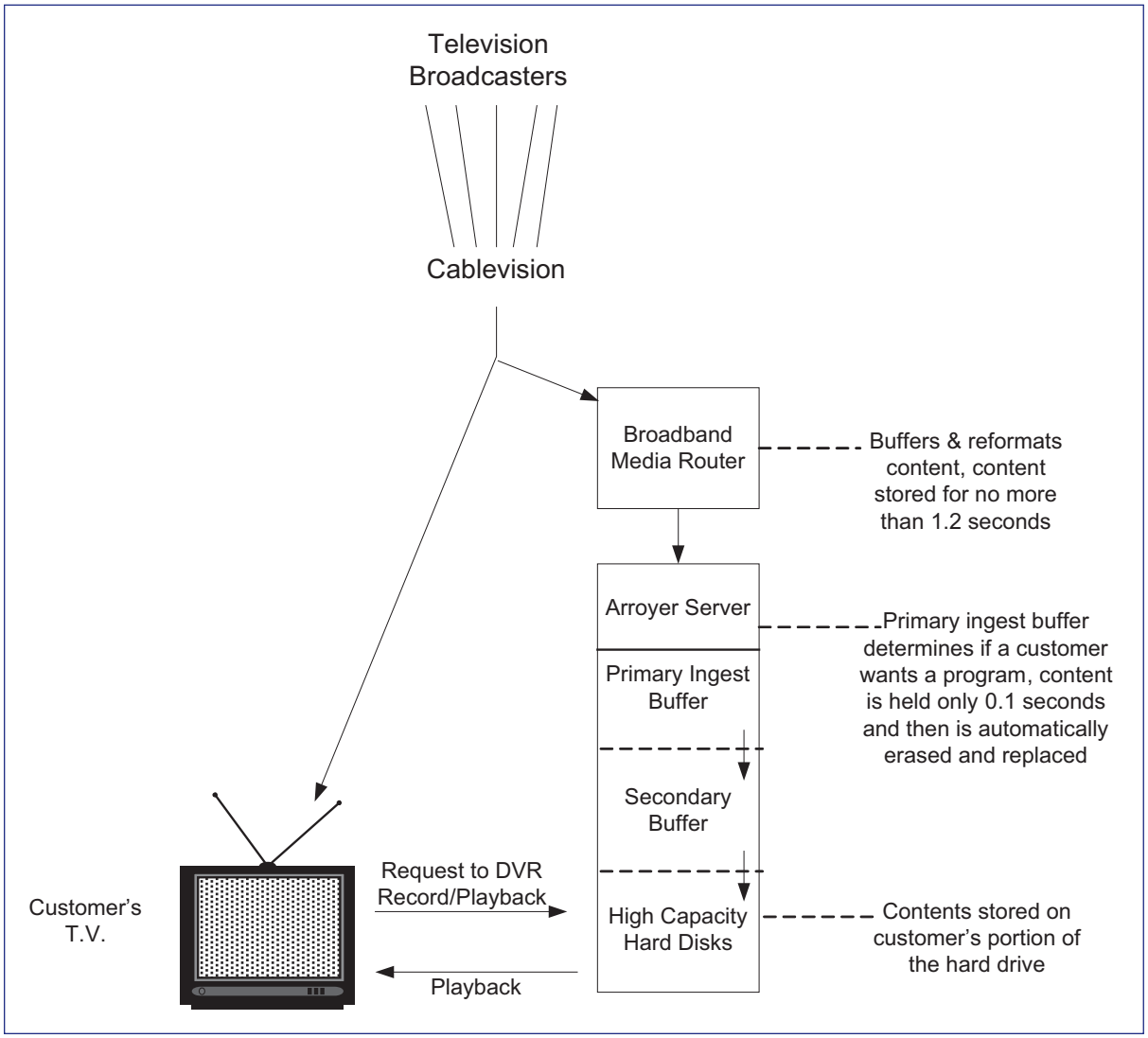
creation of primary ingest buffer copies in system RAM (random access memory) of no more than 1.2 seconds of a work for a period of 0.1 seconds. Cablevision took the content from one stream of programming, after the split, and stored it one small piece at a time in the primary ingest buffer.

A graphic representation of the RS-DVR system appears in Figure 1.

The content providers argued that, in buffering the data that made up a work, Cablevision infringed because it reproduced the work "in copies." Section 101 defines "copies" as "material objects . . . , in which a work is fixed by any method now known or later developed, and from which the work can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device." Section 101 provides that a work is "'fixed" in a tangible medium of expression when its embodiment in a copy . . . , by or under the authority of the author, is sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for a period of more than transitory duration." A work consisting of sounds, images, or both that are being transmitted is "fixed" if a fixation of the work is being made simultaneously with its transmission.

Based on Copyright Act definitions, RAM reproductions are generally considered to be "fixed" and thus constitute "copies" that are within the scope of the copyright owner's reproduction right. The definition of "fixed" leaves open the possibility, however, that certain RAM reproductions that exist for only a "period of . . . transitory duration" are not copies. The statute does

Figure 1: The RS-DVR System



not define "transitory duration" directly. Because permanence is not required for fixation, "transitory" must denote something shorter than "temporary." "Transitory" must also denote something less than "ephemeral," as that term is used in the Copyright Act, since the Copyright Act confirms that "ephemeral recordings" are fixed by providing a specific exemption for "ephemeral recordings" lasting up to six months.[3]

Here, the copy was in a buffer for only 1.2 seconds before being overwritten. The Second Circuit concluded that it was not fixed, so not a "copy." The Second Circuit held that the acts of buffering in the operation of buffering in the RS-DVR did not create copies as the Copyright Act defines that term.

After the RS-DVR subscriber selects a program to record, and that program airs, an unauthorized copy of the television program—a copyrighted work—resides on Cablevision's server. To determine if Cablevision was directly liable for making this copy, the Second Circuit examined who made the copy. If the copy was made by Cablevision then it would be liable for direct infringement.

The Second Circuit concluded that some element of volition or causation was required to impose direct liability. Mere ownership of the machine performing the copying was not sufficient. Cablevision designed, housed, and maintained a system to produce copies, but the customer was the one who pressed the button and activated the machine to do the copying. Copies were automatically made on the customer's command.

The Second Circuit also examined whether Cablevision transmitted a performance of the work to the public. The RS-DVR playback did result in a transmission of a performance of the work—the transmission from the server to the consumer's television. But the Second Circuit held that this transmission did not involve a transmission of a performance "to the public." For the Second Circuit, the key question was: Who was the potential audience of the transmission? The RS-DVR system made transmissions to only one subscriber at a time, using a copy made at the request of that subscriber. The Second Circuit concluded that, because each RS-DVR playback transmission was made to a single subscriber, using a single unique copy produced by that subscriber, the transmission was not a performance to the public and therefore did not infringe any right of public performance of the copyright owner.

The US Supreme Court sought the views of the Solicitor General on the question of whether it should hear the case. The Supreme Court denied the *certiorari* petition after the Solicitor General recommended that the Court not hear the case, in part because the technology-related issues had not had time to develop and partly because of the unique posture of the case in which the parties by stipulation excluded contributory infringement and fair use arguments.

Cloud-based distribution services also continue to be the subject of various copyright infringement claims in cases interpreting (1) the US Supreme Court's 2005 decision in *MGM Studios, Inc. v. Grokster Ltd*,[4] (2) whether "making available" for distribution constitutes distribution under the Copyright Act, (3) the safe harbor provisions of the 1998 Digital Millennium Copyright Act,[5] and (4) the safe harbor provisions of the Communications Decency Act.[6]

The prevailing view in US courts is that making available, standing alone, does not equal distribution, but there is no definitive decision on the question.

In *Arista Records, LLC v. Usenet.com, Inc.*,[7] the District Court for the Southern District of New York granted summary judgment to plaintiff record companies[8] on claims for (1) direct copyright infringement of the exclusive right of distribution under 17 U.S.C. § 106(3); (2) inducement of infringement; (3) contributory infringement; and (4) vicarious infringement by Usenet.com, Inc. (UCI).

UCI created an online bulletin board system on which subscribers posted files and downloaded files posted by others for storage on their personal computers. While technically different in format conversions, UCI's service created an experience like peer-to-peer file-sharing networks, including Napster. UCI offered access to its service based on monthly fees and agreement to UCI's terms of use (TOU). One TOU prohibited the unauthorized upload of copyrighted content. The record companies objected to UCI's activities as the unauthorized distribution of copyrighted works.

Copyright infringement plaintiffs must establish ownership of a valid copyright and unauthorized copying or a violation of one of the other exclusive rights provided under the Copyright Act. Here, it was undisputed that the record companies owned valid copyrights to music files on UCI's service and had not authorized their distribution or reproduction via this service. The remaining question was whether UCI's service directly distributed the record companies' works.[9]

The record companies contended that UCI's transmittal of files in response to subscribers' requests constituted a "distribution." UCI cited the *Cablevision* case, arguing that direct infringement requires volitional

conduct and that, when a service is a mere "passive conduit" for user-requested works, it cannot be liable. The record companies argued that *Cablevision* was limited to the exclusive rights of reproduction and public performance and that no volitional conduct was required when addressing infringement based on unauthorized distribution. Rejecting this argument, the district court found that the volitional conduct requirement applies to all exclusive rights under the Copyright Act.

The question then became whether UCI engaged in volitional conduct. UCI argued that its service was like a common carrier delivering user-requested files automatically without its active involvement. UCI, however, was aware that music files were among the most popular on its service and took measures to increase their retention time. Moreover, UCI took active steps to remove other content types (including pornography) and to block certain users. Those actions transformed UCI from a passive provider of a forum to an active participant in copyright infringement. Accordingly, the court found volitional conduct and granted summary judgment on the issue of direct infringement of the exclusive right of distribution.

The record companies also brought inducement of infringement, contributory infringement, and vicarious infringement claims. All three require a threshold showing of direct infringement by a third party, which was found based on subscribers' downloads of the record companies' copyrighted works, thereby creating unauthorized copies on their computers.

One who distributes a device with the object of promoting its use to infringe a copyright is liable for the resulting infringement by third parties. Here, UCI employees acknowledged the use of the service to download copyrighted works. UCI sought to attract users of other file-sharing services, such as Napster and Kazaa, and pursued infringement-minded users through its use of Web site metatags embedding words such as "warez" (slang for pirated content) to ensure that searches for illegal content returned UCI's Web site. Further, UCI's Web site advertised its infringing uses, encouraging users to "[d]ownload thousands of FREE CD quality music files!" UCI employees provided technical assistance to help users download copyrighted content and provided Web site tutorials on how to download content, using infringing works as examples. UCI touted that file transmissions could not be monitored so users could conduct infringing activities anonymously. The court found UCI's failure to limit infringement under such circumstances strong evidence of intent to foster copyright infringement. UCI employees' statements demonstrated that UCI knew that its service was used to obtain copyrighted material. UCI caused or contributed to infringement by creating promotional materials that emphasized the availability of copyrighted content and by operating servers that stored and distributed the content.[10]

Another cloud-computing-related issue is whether merely making a file available (in the cloud) for distribution, via a peer-to-peer file sharing network or otherwise, constitutes distribution for purposes of determining Copyright Act infringement liability. The prevailing view in US courts is that making available, standing alone, does not equal distribution, but there is no definitive decision on the question.[11]

The DMCA safe harbor provision insulates online service providers from infringement liability if they adhere to certain guidelines and promptly block access to allegedly infringing material (or take down such material from their systems) upon notification of infringement. Under § 512(c), a service provider will not be liable for copyright infringement resulting from activity by a user if the service provider lacks knowledge of the infringing activity, does not receive a financial benefit directly attributable to the infringement and acts expeditiously to remove or block access to the infringing content once notice is given. Additionally, service providers must adopt, inform users of, and implement a policy that terminates the accounts of users who are repeat infringers and must not interfere with "standard technical measures" that a copyright owner uses to protect its work from infringement.

The applicability of the DMCA safe harbor for online publishers of third-party content is one of the key issues in the Viacom-Google litigation regarding Google's YouTube video service, currently pending before the Southern District of New York. That court recently granted summary judgment to Google and YouTube, holding that they were entitled to the DMCA § 512(c) safe harbor because they had insufficient notice of particular infringements. The court noted that general knowledge of ubiquitous infringements did impose a duty on a service provider to search for and remove infringing material.[12] The decision addressed a number of issues related to the application of the DMCA safe harbor provisions.

The standard for the use of the DMCA safe harbor by cloud computing services also was addressed in several other recent court decisions, such as *Perfect 10 Inc. v. CCBill LLC,*[13] (service provider's responsibility to block repeat offenders); *UMG Recordings, Inc. v. Veoh Networks, Inc.,*[14] (DMCA safe harbor protects service provider that merely reformats third-party content); and *Io Group v. Veoh Networks, Inc.,*[15] (DMCA safe harbor protects video service provider that followed take-down procedures and automatically reformatted third-party content).[16]

In *Nemet Chevrolet, Ltd. v. ConsumerAffairs.com, Inc.,*[17] the court relied on § 230 of the Communications Decency Act to affirm dismissal of a defamation lawsuit against a Web site that collected and disseminated consumer complaints. The court held that, to avoid dismissal at the complaint stage, a plaintiff's complaint against an online service provider must allege with specific detail why § 230 immunity does not bar the claim, that is, how the online service provider itself participated in the actual creation or development of the allegedly unlawful content.[18]

Computer Fraud and Abuse Act and Related Claims Regarding Web Sites

Claims regarding the unauthorized "scraping" (automated collection) of information from the cloud have been successfully asserted, at least initially, based on the Computer Fraud and Abuse Act (CFAA, 18 U.S.C. § 1030) or trespass theories. CFAA is triggered when someone accesses a computer used in or affecting interstate commerce "without authorization" or when that person "exceeded authorized access."[19] In a recently decided case, *Craigslist, Inc. v. Naturemarket, Inc.*,[20] Craigslist won a $1.3 million judgment against a seller of software that enabled automatic posting of listings to Craigslist and scraped email addresses from the Craigslist Web site on a variety of causes of action including CFAA.

In *Barclays Capital, Inc. v. Theflyonthewall.com*,[21] the court held that a financial services firm could use the hot news doctrine to block a competing publisher from re-distributing the recommendations in investment reports. The court determined that the provision of attribution for the source of the information did not absolve the defendant from liability.

Privacy Rights

The US Supreme Court recently decided *City of Ontario v. Quon*[22] and addressed whether a search of text messages transmitted on a police pager was reasonable. The City of Ontario provided pagers to SWAT team police officers. After Sgt. Quon exceeded his allowed usage, the City acquired transcripts from the pager service provider via subpoena and discovered that Quon had used the pager for personal purposes, including sexually explicit messages. Quon sued, claiming an unlawful search in violation of the Fourth Amendment.

The trial court found that officers had a reasonable expectation of privacy in the text messages and that liability should hinge on whether the police chief's intent was to uncover misconduct rather than to discover the efficacy of the usage limit. A jury decided that the police chief's intent had to do with the usage, so the defendants were absolved of liability. The Ninth Circuit reversed, holding that the search was unreasonable as a matter of law, so the police chief's intent never should have gone to trial.

The US Supreme Court reversed and held that the search was reasonable, as the search was motivated by a legitimate work-related purpose, reasonably related to the objectives of the search, and not excessively intrusive. The Supreme Court noted that it would not have been reasonable for Quon to assume that his text messages were immune from scrutiny. The Court assumed for purposes of its analysis, but did not actually decide, that Quon had a reasonable expectation of privacy in the text messages.

Personal Information

In *Party City Corp. v. Superior Court of San Diego County*,[23] the California Court of Appeal held that zip codes are not protected personal identification information, rejecting a class action suit that relied on California's Song-Beverly Credit Card Act of 1971. The court, referring to the terms of the Health Information Technology for Economic and Clinical Health (HITECH) Act, found that five-digit zip codes are group, not individual, identifiers because thousands of people have the same zip code.

Courts have split on the question of what is necessary to have standing to pursue claims in database security breach cases. Many courts have held that a mere risk of future identity theft is not enough to confer standing.[24] Others have found that standing to pursue claims did exist in such cases.[25]

In *In re Hannaford Bros. Co. Customer Data Breach Sec. Litig.*,[26] the court dismissed all but one of the class action lawsuits filed by victims of a data breach. The court allowed claims from consumers who had suffered a direct loss to the consumers' account and dismissed claims by consumers who had the fraudulent charges reversed or had no fraudulent charges.

In *Ruiz v. Gap, Inc.*,[27] the court dismissed a plaintiff's claim for negligence based on the risk of future identity theft, but noted that a plaintiff did have standing to assert a claim when the plaintiff's personal information was stolen, along with unencrypted personal information for 750,000 other job applicants, from a laptop owned by a job-application processing vendor.

Similarly, in *Allison v. Aetna, Inc.*,[28] an employee applicant whose information was contained in a breached employment application database lacked standing to pursue negligence, breach-of-contract, and invasion-of-privacy claims because the individual could not establish any actual likelihood that identity theft risk existed.

New Types of Claims

In 2009, the Identity Theft Resource Center analyzed 498 publicly reported data security breaches affecting 222 million total records including:

- "Data on the move," such as lost laptops;
- Accidental exposure;
- Insider theft;
- Losses involving subcontractor; and
- Hacking.

On February 22, 2010, the FTC issued a news release stating that the FTC had notified almost 100 entities that personal information about their employees, students, or customers had been exposed via peer-to-peer file-sharing Web sites, creating risks of identity theft and fraud. As a result of these types of security breaches, and the increasing use of cloud services for a variety of tasks, we can expect to see the following types of claims in coming years:

- Liability of cloud service providers for inadequate security; damages from hacker attacks, loss of user data;
- Liability of cloud service providers for data mining;
- Liability under securities laws for improper dissemination of investment information on social networking Web sites;
- Liability in Europe for breach or disclosure in violation of national laws implementing EU Data Protection Directive 95/46/EC;
- Fourth Amendment; suppression of evidence obtained from cloud service providers without proper authorization; and
- Facilitation of censorship or surveillance by cloud computing service providers (*e.g.*, proposed under Global Online Freedom Act/H.R. 2271)).

The following is a list of pending cases that illustrates new types of claims concerning cloud computing services that will arise as a result of the exposure of personal data or other information held in the cloud:

- Electronic Privacy Information Center (EPIC) Complaint and Request for Injunction, Request for Investigation and for Other Relief—In the Matter of Google, Inc., and Cloud Computing Services, filed March 17, 2009 before the US Federal Trade Commission (pending).[29]
- Classmates Online, Inc., class action litigation alleging deceptive practices and violation of ECPA for change of privacy policy allowing expanded searches of provided personal data (tentative settlement pending hearing).[30]
- Netflix, Inc., class action litigation for failure to protect allegedly anonymized rental data and to comply with privacy and data security policy protections for data shared with researchers (settlement approved).[31]
- Facebook "Beacon" class action litigation, concerning Facebook's Beacon program, designed to allow users to share information with selected friends about actions taken on affiliated, third-party Web sites. Plaintiffs claimed inadequate notice or choice about how Facebook and its affiliates collected information about Web-browsing activity before publication on Facebook (settlement pending).[32]
- Google "Buzz" class action litigation, alleging violations of ECPA, Stored Communications Act, and various other claims regarding unauthorized publication of Gmail subscriber contact lists, and related FTC investigation (settlement pending).[33]
- Class action lawsuit alleging that Google shares user personal information contained in search queries with third parties and thereby violates various federal and state laws.[34] Lifelock, Inc., settlement with FTC and state attorneys general regarding false claims about its identity theft and data security services (settlement announced Mar, 9, 2010).

With respect to potential Fourth Amendment issues arising from the use of cloud computing services, in *State v. Bellar,*[35] the dissenting opinion states:

> [A] defendant's privacy rights in the information stored in his personal computer is retained even if the information is copied and stored on a medium owned by someone else.
>
> ⋆⋆⋆
>
> Nor are a person's privacy rights in electronically stored personal information lost because that data is retained in a medium owned by another. Again, in a practical sense, our social norms are evolving

away from the storage of personal data on computer hard drives to retention of that information in the "cloud," on servers owned by internet service providers. … I suspect that most citizens would regard that data as no less confidential or private because it was stored on a server owned by someone else.

★★★

Our precedents suggest that the existence of a protected privacy interest in private information is not determined by ownership of the storage medium for that information. … The existence or not of a protected privacy interest was not determined by who owned the servers and other devices on which the information was stored.

★★★

Because of the different nature of the privacy interests protected under the federal and state constitutions, consideration of analogous Fourth Amendment cases is helpful but not instructive. In that area of law as well, the ownership of the storage medium does not determine whether a privacy interest exists in the stored data.

Notes

1. Cloud-computing businesses, like more terrestrial businesses, will have disputes involving corporate and securities issues, employees, product liability, negligence, and the like.
2. Cartoon Network v. CSC Holdings, 536 F.3d 121 (2d Cir. 2008*), cert. denied*, 129 U.S. 2890 (2009).
3. 17 U.S.C. § 112.
4. MGM Studios, Inc. v. Grokster Ltd, 545 U.S. 913 (2005).
5. 17 U.S.C. § 512.
6. 47 U.S.C. § 230.
7. Arista Records, LLC v. Usenet.com, Inc., 633 F. Supp. 2d 124 (S.D.N.Y. 2009).
8. The record companies included Arista Records LLC, Atlantic Recording Corp., BMG Music, Capitol Records, LLC, Caroline Records, Inc., Elektra Entertainment Group Inc., Interscope Records, Laface Records LLC, Maverick Recording Company, Sony BMG Music Entertainment, UMG Records, Inc., Virgin Records America, Inc., Warner Bros. Records, Inc., and Zomba Recording LLC.
9. *See* 17 U.S.C. § 106(3).
10. *See also* Arista Records LLC v. Lime Group LLC, No. 06-5936, 2010 WL 2291485 (S.D.N.Y. May 25, 2010).
11. *See, e.g.,* Perfect 10, Inc. v. Amazon, 508 F.3d 1146, 1162-1163 (9th Cir. 2007); Capitol Records, Inc. v. Thomas, 579 F. Supp. 2d 1210 (D. Minn. 2008); London-Sire Records, Inc. v. Doe, 542 F. Supp. 2d 153, (D. Mass. 2008) (evaluating discovery requests); Atlantic Recording Corp. v. Howell, 554 F. Supp. 2d 976, 981-982 (D. Ariz. 2008) (denying motion for summary judgment); Atlantic Recording Corp. v. Brennan, 534 F. Supp. 2d 278 (D. Conn. 2008) (denying default judgment motion). *But see* Elektra Entertainment Group, Inc. v. Barker, 551 F. Supp. 2d 234, (S.D.N.Y. 2008).
12. Viacom Int'l Inc. v. YouTube Inc., Nos. 07-2103, 07-3582, 2010 WL 2532404 (S.D.N.Y. June 23, 2010).
13. Perfect 10 Inc. v. CCBill LLC, 488 F.3d 1102 (9th Cir. 2007).
14. UMG Recordings, Inc. v. Veoh Networks, Inc., 2008 WL 5423841 (C.D. Cal. 2008).
15. Io Group v. Veoh Networks, Inc., 586 F. Supp. 2d 1132 (N.D. Cal. 2008).
16. *See also* Perfect 10, Inc. v. Google, Inc., No. 04-9484 (C.D. Cal. July 26, 2010) (order granting Google's motion for partial summary judgment of entitlement to safe harbor with respect to certain of its Web-based applications).
17. Nemet Chevrolet, Ltd. v. ConsumerAffairs.com, Inc., 591 F.3d 250 (4th Cir. 2009).
18. *See also* Barnes v. Yahoo! Inc., 565 F.3d 560 (9th Cir. 2009) (online message board entitled to CDA § 230 immunity for failure to remove abusive posts, even if failure was negligent; contract-based promissory estoppel claim permitted to proceed); Fair Housing Council of San Fernando Valley v. Roommates.com, 521 F.3d 1157 (9th Cir. 2008) (roommate matching Web site that developed and specifically required users to respond to questions about housing preferences not eligible for CDA § 230 immunity for Fair Housing Act claims); Chicago Lawyers' Committee for Civil Rights v. Craigslist Inc., 519 F.3d 666 (7th Cir. 2008) (publisher of discriminatory housing ads entitled to CDA § 230 immunity); Doe v. MySpace, Inc., 528 F.3d 413 (5th Cir. 2008) (CDA § 230 immunity for negligent failure to protect underage users from child predators).
19. *See* Register.com v. Verio, Inc., 356 F.3d 393 (2d Cir. 2004); EF Cultural Travel BV v. Zefer Corp., 318 F.3d 58 (1st Cir. 2003); EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577 (1st Cir. 2001); Southwest Airlines Co. v. Farechase, Inc., 318 F. Supp. 2d 435 (N.D. Tex. 2004); Ticketmaster Corp. v. Tickets.com, 2003 WL 214006289 (C.D. Cal. 2003); eBay v. Bidder's Edge Inc., 100 F. Supp. 2d (N.D. Cal. 2000); Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121 (W.D. Wash. 2000); *see also* Creative Computing v. GetLoaded.com LLC, 386 F.3d 930 (9th Cir. 2004); Pacific Aerospace & Electronics, Inc. v. Taylor, 293 F. Supp. 2d 1188 (E.D. Wash. 2003). *But see* Bell Aerospace Servs. v. US Aero Servs., Inc., 690 F. Supp. 2d 1267 (M.D. Ala. 2010) (no violation of CFAA by employees who took information from company to start competing venture, as computer access was authorized).
20. Craigslist, Inc. v. Naturemarket, Inc., 694 F. Supp. 2d 1039 (N.D. Cal. 2010).
21. Barclays Capital, Inc. v. Theflyonthewall.com, 700 F. Supp. 2d 310 (S.D.N.Y 2010).
22. City of Ontario v. Quon, 130 S. Ct. 2619 (2010).
23. Party City Corp. v. Superior Court of San Diego County, 86 Cal. Rptr. 3d 721 (2008).

24. *See, e.g.,* Randolph v. ING Life Ins. And Annuity Co., 486 F. Supp. 2d 1 (D.D.C. 2007); Key v. DSW, Inc., 454 F. Supp. 2d 684 (S.D. Ohio 2006).
25. *See, e.g.,* Pisciotta v. Old National Bancorp., 499 F.3d 629 (7th Cir. 2007); Caudle v. Towers, Perrin, Forster & Crosby, Inc., 580 F. Supp. 2d 273 (S.D.N.Y. 2008); Am. Fed. of Gov't Employees v. Hawley, 543 F. Supp. 2d 44 (D.D.C. 2008).
26. In re Hannaford Bros. Co. Customer Data Breach Sec. Litig., 613 F. Supp. 2d 108 (D. Me. 2009).
27. Ruiz v. Gap, Inc., 622 F. Supp. 2d 908 (N.D. Cal. 2009).
28. Allison v. Aetna, Inc., No. 09-2560 (E.D. Pa. Mar. 8, 2010).
29. The Electronic Privacy Information Center's Web site suggests that the FTC has taken no specific action on EPIC's complaint. Almost a year after the filing of EPIC's complaint, EPIC submitted comments to the FTC for consideration at one of the agency's "privacy roundtables." *See http://epic.org/privacy/ftc/EPIC_FTC_Comment.pdf.* In its comments to the FTC, EPIC noted the FTC's assurance that it was conducting an "investigation on Cloud Computing services" but EPIC also complained that the FTC had, to date, failed "to take any meaningful actions" on the issues raised by its Complaint.
30. In re: Classmates.com Consolidated Litigation, No. 09-45, U.S.D.C. W.D. Wash. (filed Jan. 13, 2009).
31. Valdez-Marquez v. Netflix, Inc., No. 09-5903, U.S.D.C., N.D. Cal. (filed Dec. 17, 2009; settlement approved Mar. 2010).
32. Lane v. Facebook, Inc., No. 08-3845, U.S.D.C. N.D. Cal. (filed Aug. 12, 2008), and McCall v. Facebook, Inc., No. 10-16380 (9th Cir. filed June 23, 2010).
33. In re Google Buzz Privacy Litigation, No. 10-672, U.S.D.C. N.D. Cal. (filed Feb. 17, 2010); a number of related cases were consolidated under this caption. A settlement in the Google Buzz litigation was announced on November 2, 2010.
34. Gaos v. Google, Inc., No. 10-0480 (N.D. Calif. filed Oct. 25, 2010).
35. State v. Bellar, 217 P.3d 1094 (Or. App. 2009) (dissenting opinion of J. Sercombe).