JOURNAL OF INTERNET LAW
VOLUME 14
NUMBER 1
ASPEN PUBLISHERS
JULY 2010
EDITED BY DLA PIPER

Cloud Computing: Emerging Legal Issues for Access to Data, Anywhere, Anytime

By Mark H. Wittow and Daniel J. Buller

Working with the "cloud" has become a normal part of everyday life, for both business and pleasure. From legal research to word processing, file storage and movie viewing, computer users are able to take advantage of the cloud for a variety of tasks. Some functions may be practical and mundane, such as, for example, publishing and sharing vacation photos or chatting with friends and family. Other uses may be extremely sensitive and highly technical, such as storing and securing personal information for millions of credit card subscribers or health records for insureds. Cloud computing has become increasingly common among both businesses and individuals, and the cloud, which is essentially a metaphor for the Internet,[1] is being used in increasingly innovative ways. Generally, "cloud computing" occurs when an Internet connection delivers hardware power and software functionality to users regardless of where they are or which computer they are using. Because users merely are using the Internet to obtain their data and computing power, they are

Continued on page 5

Mark H. Wittow is a partner in the Seattle office of K&L Gates. His work focuses on intellectual property, technology transactions, and litigation. He is the current chair of the ABA-Intellectual Property Law Section Information Technology Division He can be reached at mark.wittow@klgates.com. Daniel J. Buller is a third-year student at the Kansas University School of Law; he will graduate in May 2011. Before attending law school, he worked for seven years in information technology at High Touch, Inc., a software development company in Wichita, KS. He can be reached at dbuller@ku.edu.

IN THIS ISSUE

Wolters Kluwer
Law & Business

ASPEN PUBLISHERS

JOURNAL OF INTERNET LAW

EDITORIAL OFFICES

400 Hamilton Avenue
Palo Alto, CA 94301
(650) 328-6561

76 Ninth Avenue
New York, NY 10011
(212) 771-0600

JOURNAL OF INTERNET LAW (ISSN# 1094-2904) is published monthly by Aspen Publishers, 76 Ninth Avenue, New York, NY 10011. Telephone: 212-771-0600. One year subscription (12 issues) price: $515. Single issue price: $49. To subscribe, call 1-800-638-8437. For customer service, call 1-800-234-1660. **Purchasing reprints:** For customized article reprints, please contact *Wright's Reprints* at 1-877-652-5295 or go to the *Wright's Reprints* website at *www.wrightsreprints.com* Postmaster: Send address changes to JOURNAL OF INTERNET LAW, Aspen Publishers, 7201 McKinney Circle, Frederick, MD 21704.

Cloud Computing: Emerging Legal Issues Continued from page 1

less tethered to their offices, homes, and even their physical computer systems than ever before.

Traditionally, using hardware and software resources required on-site computing power and disk storage space, as well as the technical human expertise necessary to implement, maintain, and secure those resources. Complicated and expensive upgrade procedures were necessary to take advantage of new developments and features available for software applications. In addition, the upgraded software (and hardware) often required upgrading licenses and increasing backup and recovery capabilities to reduce the downtime that users would experience should a software or hardware failure occur. Local administrators with specialized, technical skill-sets were historically responsible for application and hardware maintenance. In addition, the "traditional model" often involved managing a large hardware infrastructure with disparate operating systems and applications that required individual backups, monitoring, and software updates. Disaster recovery preparation entailed allocating redundant hardware, which correspondingly increased the amount of space that was physically required to support the additional equipment (the hardware footprint). The traditional computing model required companies (and individuals) to make a significant financial commitment to set up software and hardware resources, and these were frequently difficult to expand when the needs of users changed.

The limitations of the traditional model were mitigated to an extent by hardware innovations such as designing servers with vastly increased computing power to fit into a very small space. The consolidation of physical servers by system virtualization and centralized disk storage also helped lessen some of the expenses of the traditional model. With virtualization, one physical system provides the computing power for multiple virtual servers. The physical server dynamically allocates its actual resources, as the virtual servers require them. For example, the servers providing corporate email and calendaring are on the same physical system (co-tenants) as the servers that provide file and data storage. When the email system has a spike in activity, the physical server is able to borrow resources from the data storage system so that end users do not experience a drag on performance. Through such innovations, the "cloud" was born.

While experts differ on a precise definition of "cloud computing,"[2] it generally involves a subscription-based service that satisfies computing and storage needs from a virtually unlimited hardware and communication infrastructure, which is managed by a third-party provider. Cloud computing allows for rapid increases in capacity or capability without the need to invest in additional infrastructure, personnel, or software licensing. As one CEO of a cloud computing provider put it, "[a]s a customer, you don't know where the resources are, and for the most part, you don't care. What's really important is the capability to access your application anywhere, move it freely and easily, and inexpensively add resources."[3]

Mobility and convenience are major factors in the rapid adoption of cloud computing. According to the Pew Internet and American Life Project, approximately 69 percent of US Internet users make use of webmail services, online data storage (*e.g.*, for pictures, videos, personal files, etc.), or software programs (*e.g.*, word processors or spreadsheets) whose functionality is located on the Web.[4] A majority of these users say that ease and convenience of use are major reasons that they use the cloud for handling these functions. Forty-one percent of cloud users say that the ability to access their data from any computer is the principal reason for their choice to use the cloud.[5]

The increasing popularity of Internet notebooks, or "netbooks," underscores the importance of mobility to the modern computer user. Netbooks are typically low-cost, lightweight laptop computers with reduced hardware capacity and processing power that are primarily designed to provide the user with access to the Internet.[6] Netbooks provide users with vast resources because the cloud is fully accessible without requiring users to make a substantial investment in local hardware. The virtually unlimited resources available in the cloud make the local system's limited hardware capabilities irrelevant.

Cloud computing offers companies the ability to expand their resources in real time as customer demand for product increases. For example, Animoto, a software provider that converts personal photos into music videos, developed a Facebook application that took the company from 25,000 users to 250,000 users in three days. At its peak, Animoto was signing up

20,000 new users per hour. It launched the service with five virtual servers and, by the end of the three days, had expanded to 3,500 servers. Animoto's ability to scale-up at such an incredible rate was accomplished by using a cloud provider that was able to add resources as demand for product increased.[7] Mobility, ease-of-access, and the ability to inexpensively scale system resources save users time and money. But the benefits that the cloud provides come at a cost. Despite the ease and flexibility that cloud computing provides to users, users should wonder precisely how their data being stored on the Web are kept and used by the cloud service providers. A great advantage to the traditional model is that the users had control over their data and could implement whatever safeguards they thought necessary to retain control. In contrast, cloud users neither possess nor control their data. Sixty-three percent of cloud users say that they would be very concerned if the cloud provider kept a copy of files that users wanted to delete.[8] Ninety percent of users would be very concerned if their data were to be sold to others by the cloud provider.[9]

Cloud users have no access to the physical hardware providing their storage and processor resources. The concerns under the traditional model that caused users to invest in redundant hardware and disparate backup and recovery solutions do not disappear simply by choosing to use the cloud. The users are merely trusting that the cloud service providers are taking the risks of data loss and security seriously. The users' expectations of security and reliability and the lack of direct control that the users have over the hardware providing the data and processing power present particularly challenging problems for the cloud computing model. Users expect cloud service providers to minimize single points of failure and encrypt data. In the end, the convenience, reduced upfront costs, and impressive scalability offered by the cloud computing model will have to be balanced against the users' expectations of data control, data flow, and disaster recovery requirements.

EMERGING LEGAL ISSUES

Cloud computing and storage infrastructures are vastly more powerful than ever before because governments, businesses, and individuals are developing them at an increasingly rapid pace. The uses for which these infrastructures are put in place are diverse, ranging from lucrative and mission-critical business functions to sensitive information and expressive content. Existing laws and governance models have not always been able to keep pace with these developments. As a result, the potential for legal disputes is considerable.

Privacy concerns are on the rise. Thirty-five percent of Internet users feel that their privacy has been invaded or violated due to information that they provided via the Internet.[10]

With privacy concerns in mind, the Electronic Privacy Information Center (EPIC) recently filed a complaint with the Federal Trade Commission (FTC) regarding the cloud computing services offered by Google, Inc.[11] EPIC alleged that Google does not adequately safeguard the confidential information that it obtains from its users and requested that the FTC open an investigation into Google's Cloud Computing Services. The complaint went on to suggest that the FTC enjoin Google from offering any service for which inadequate protections of privacy and security of users' data are found to exist. The complaint isolated several cloud-based services offered by Google, including webmail (Gmail),[12] online document storage and editing (Google Docs),[13] integrated desktop and Internet search (Google Desktop),[14] online photo storage (Picasa Web Albums),[15] and scheduling programs (Google Calendar).[16] The customer data residing on a Google server are critical to the architecture of each of these services.[17] According to the complaint, Google misrepresents the privacy and security of its users' data. For example, it assures users of Google Docs that their data are secure and private unless the user specifically publishes them to the Web or invites collaborators. However, Google's terms of service explicitly disavow any warranty or any liability for harm that might result from Google's negligence to protect the privacy and security of user data.

EPIC's complaint pointed out several known flaws with Google's cloud-based services. These include disclosure of documents to users who lacked permission to view them; security flaws in Google's webmail service that exposed usernames and passwords to theft; the exposure of Google users' personal data to malicious Internet sites; and, finally, flaws that could allow malicious sites to gain full control over users' systems. In addition, the complaint pointed out the inherent risks posed by users who transfer their applications

and data files onto a centralized server, namely, the relinquishment of users' control over their own data. The harm caused, in each of these instances, was reasonably avoidable by the adoption of "commonsense security practices, including the storage of personal data in encrypted form, rather than in clear text."[18] As a result, the complaint alleges, Google's inadequate security measures are an unfair business practice and a deceptive trade practice.[19]

User privacy rights are fundamental to EPIC's complaint. The need for clear and consistent communication of policies, practices, and capabilities is necessary for adequately meeting user expectations. Data protection practices, such as encryption—how it is used and who is employing it—are also at the heart of the complaint against Google. As the services offered by cloud providers become more sophisticated, so too should their policies and practices related to privacy and security. The privacy concerns intrinsic in the services that Google offers are serious challenges to both cloud users and providers, but they can be mitigated.

Privacy concerns also have been raised in the context of the pending *Authors Guild v. Google* book search settlement, which creates a cloud-based database of searchable books.[20] In the context of the pending consideration of that settlement, groups such as the Electronic Frontier Foundation and the American Civil Liberties Union of Northern California have requested that Google keep Web search data only for a relatively short period. Google has indicated that it will not disclose personal information, but it hasn't agreed to limits on its use of the data or the time period for holding the data and has not offered any concrete restrictions against disclosure at this stage.

From the perspective of the licensor, the terms of the software license agreement (SLA) should fit the service being offered to limit liability. For example, it is natural for a webmail service, such as Gmail, to store the names and email addresses of its users and their contacts, and there should be adequate security measures to protect this information. However, even though Google's security measures may be adequate to protect the data that users choose to store through Gmail, the licensor may not want to be responsible for storing such information. If a cloud provider does not *need* certain private information, then they could limit their liability by not gathering and storing it.

The SLAs of cloud-based applications and services generally are non-negotiable and much more favorable to the provider than to the end user. For example, Google's license agreement for its "Chrome" Web browser initially gave the company "a perpetual, irrevocable, worldwide, royalty-free, and non-exclusive license to reproduce, adapt, modify, translate, publish, publicly perform, publicly display and distribute any Content which you submit, post or display on or through" the Web browser.[21] The SLA also included a clause that allowed Google to "make such Content available to other companies, organizations or individuals with whom Google has relationships for the provision of syndicated services, and to use such Content in connection with the provision of those services."[22] A debate quickly emerged among users regarding the copyright implications of the Chrome SLA. Google then acted to amend the most objectionable language.[23] As the Chrome incident illustrates, users may need to pay close attention to the language of any SLA to which they are agreeing.

Other issues in cloud computing SLAs should be examined as well. Users should be sure to have a clear understanding of how to terminate their relationship with a given cloud provider while minimizing disruption. For example, there should be a realistic migration plan in place that assures business continuity and secures access to data following the dissolution of the users' relationship with the provider.

Some user concerns regarding the portability and security of cloud-based data and communications among clouds may be addressed in industry standards organizations.[24] Among the organizations participating in that effort are the Object Management Group (OMG), the Distributed Management Task Force (DMTF), the Open Grid Forum (OGF), the Storage Networking Industry Association (SNIA), Open Cloud Consortium (OCC), the Cloud Security Alliance (CSA), and the Standards Development Organization Collaboration on Networked Resources Management (SCRM) working group. The work of those groups is at an early stage, and it is too soon to tell whether standards efforts will be successful in resolving some or all of these issues.

Cloud computing also presents some unique copyright issues. In the *Cartoon Network* case, the Second Circuit recently considered the use of cloud-based technology to deliver cable television programs.[25] TV content providers sued Cablevision, a cable

TV company, which had developed a remote storage digital video recorder (RS-DVR) that allowed Cablevision's customers to preselect programs to record that would later be available for the customers to view on demand. The difference between Cablevision's RS-DVR service and traditional DVRs is that the content was stored in and transmitted over the cloud.[26]

The *Cartoon Network* case required the parties and the court to make subtle distinctions over terms that took on new meanings in light of the fact that data were being processed, stored, and transmitted from within the cloud. The court eventually decided that it did not amount to copyright infringement for Cablevision to house and maintain the hardware that enabled end users to record and watch content on demand. The court held that the streamed buffer copies generated by Cablevision in responding to user requests, being highly transitory in nature, were not sufficiently "fixed" to qualify as copies under copyright law.

Cablevision's particular use of cloud-based technology was important for the court's decision. For example, Cablevision's RS-DVR system stored a unique copy of each program that its customers chose to record and that content was available only to that individual subscriber.[27] However, the court was careful to point out that its decision does not:

> permit content delivery networks to avoid all copyright liability by making copies of each item of content and associating one unique copy with each subscriber to the network, or by giving their subscribers the capacity to make their own individual copies. We do not address whether such a network operator would be able to escape any other form of copyright liability, such as liability for unauthorized reproductions or liability for contributory infringement.[28]

Although the *Cablevision* decision explicitly avoided the issue, secondary liability for copyright infringement remains an issue for cloud computing providers. Peer-to-peer file-sharing networks, which are cloud computing, continue to be popular and remain the subject of litigation, as evidenced by the *Napster*, *Grokster*, *Aimster*, and *Usenet* cases that have made their way to the various federal circuits.[29] In a very recent decision, *Arista Records LLC v. Lime Group, LLC*,[30] Judge Kimba Wood granted partial summary judgment to the plaintiffs, 13 major record companies, against LimeWire for the operation of its Gnutella peer-to-peer file-sharing network. The court granted summary judgment on the inducement of copyright infringement claim because LimeWire engaged in purposeful conduct that fostered infringement, specifically finding that LimeWire intended to encourage infringement, was aware of substantial infringement by users, deliberately sought to attract infringing users, enabled and assisted users to commit infringement, depended on the infringing use for the success of its business, and failed to mitigate infringing activities. With respect to contributory infringement, the court denied summary judgment because it found that there was a fact issue as to whether LimeWire was capable of substantial non-infringing uses. However, the court noted that LimeWire faced a strong contributory infringement case because LimeWire materially contributed to users' infringement by designing, distributing, supporting, and maintaining the program and network in a manner that fostered and encouraged infringement.

A related cloud computing issue is whether merely making a file (content) 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 content available, without more, does not equal distribution, but there is no definitive decision on the question.[31]

Another issue impacting cloud computing is what claims may be made to stop the unauthorized "scraping" (automated collection) of information from the cloud. Claims have been successfully asserted, at least initially, based on the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030, trespass, and even "hot news" theories. The CFAA is triggered when someone accesses a computer used in or affecting interstate commerce "without authorization" or when that person "exceeded authorized access."[32] In a recent decision, *Craigslist, Inc. v. Naturemarket, Inc.*,[33] 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*,[34] 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.

NEW TYPES OF CLAIMS

The Identity Theft Resource Center recently noted that at least 498 publicly reported data security breaches affecting 222 million total records occurred in 2009, with the breaches including (1) "data on the move," such as lost laptops, (2) accidental exposure; (3) insider theft, (4) losses involving subcontractor, and (5) hacking. In 2008, 26 percent of all consumer complaints received by the FTC were related to identity theft.[35] 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. More recently, the FTC noted that it has filed 27 enforcement actions challenging companies' data security practices, typically including allegations that the challenged company failed to take reasonable and appropriate steps to secure personal information collected from customers, such as failing to encrypt personal information or lack of adequate access controls and filters on outbound data.

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, including damages from hacker attacks, loss of user data;
- Liability of cloud service providers for data mining, if actual damages can be shown;
- 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 claims for suppression of evidence obtained from cloud service providers without proper authorization; and
- Facilitation of censorship or surveillance by cloud computing service providers (*e.g.*, as contemplated under the proposed Global Online Freedom Act/H.R. 2271).

The following currently pending cases (and the EPIC complaint regarding Google discussed earlier) illustrate the 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.

- 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 (pending);
- 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 pending);
- 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);
- Google "Buzz" class action litigation alleging violations of ECPA, the Stored Communications Act, and various other claims regarding unauthorized publication of Gmail subscriber contact lists and related FTC investigation (pending); and
- Lifelock, Inc. settlement with FTC and state attorneys general regarding false claims about its identity theft and data security services (announced Mar. 9, 2010).

In general, new types of claims are likely to arise as privacy law develops to address the data protection issues raised by cloud computing. If Congress is unable to enact national legislation, the states will continue to fill in the gaps, leading to a variety of standards and potential claims.

In conclusion, cloud computing offers rich opportunities and incredible potential that can meet

the needs of users like never before; however, privacy and security concerns, legal uncertainties, and the need to understand traditional terms in new ways are emerging as considerable challenges to abandoning traditional infrastructures. The rights and legal liability for both users and cloud service providers will continue to be determined as companies and individuals use the cloud for their computing needs. Ultimately, users will choose the model that makes the most sense given their needs, which may end up being a hybrid of cloud computing and the traditional model.

NOTES

1. Cloud Computing, *http://en.wikipedia.org/w/index.php?title=Cloud_computing&oldid=293407339* (last visited May 30, 2009).
2. J. Nicholas Hoover, "Interop: Oracle Predicts Cloud Confusion to Continue," InformationWeek, Sept. 17, 2008, *http://www.informationweek.com/news/services/hosted_apps/showArticle.jhtml?articleID=210602225*.
3. *Id.*
4. ""PewResearch.org,t, 2008, available at *http://pewresearch.org/pubs/948/cloud-computing-gains-in-currency*.
5. *Id.*
6. Microsoft Encarta Online Encyclopedia, Personal Computer (2009), *http://encarta.msn.com/encnet/refpages/RefArticle.aspx?refid=761557220&pn=2*.
7. Animoto's Facebook Scale-up, *http://blog.rightscale.com/2008/04/23/animoto-facebook-scale-up/ (Apr. 23, 2008)*.
8. Cloud Computing Gains in Currency, *supra* n.4.
9. *Id.*
10. Behavioral Advertising Survey, TRUSTe (Mar. 4, 2009), available at *http://www.truste.org/about/press_release/03_04_09.php*.
11. *See* EPIC Complaint Before the Federal Trade Commission, *In re* Google, Inc., and Cloud Computing Services (Mar. 19, 2009), available at *http://epic.org/privacy/cloudcomputing/google/ftc031709.pdf*.
12. Gmail, *http://mail.google.com* (last visited May 16, 2009).
13. Google Docs, *http://docs.google.com* (last visited May 16, 2009).
14. Google Desktop, *http://desktop.google.com* (last visited May 16, 2009).
15. Picasa Web Albums, *http://picasaweb.google.com* (last visited May 16, 2009).
16. Google Calendar, *http://www.google.com/calendar* (last visited May 16, 2009).
17. EPIC Complaint, *supra* n.11.
18. *Id.*
19. *Id.*
20. *See* "Google Deal with Publishers Raises Privacy Concerns," NPR, *http://www.npr.org/templates/story/story.php?storyId=111797207* (accessed Aug. 14, 2009).
21. "Google Amends Chrome License Agreement After Objections," PCWorld(Sept. 3, 2008), available at *http://www.pcworld.com/businesscenter/article/150637/google_amends_chrome_license_agreement_after_objections.html*.
22. *Id.*
23. *Id.*
24. *See* Press Release, "Cloud-Standards.org, Major Standards Development Organizations Collaborate to Further Adoption of Cloud Standards," *http://cloud-standards.org/wiki/index.php?title=Press_Release* (accessed Aug. 14, 2009).
25. Cartoon Network v. CSC Holdings, Inc., 536 F.3d 121 (2d Cir. 2008), *cert. denied*, 2009 WL 1835220 (June 29, 2009).
26. 536 F.3d at 124.
27. 536 F.3d at 139.
28. . 536 F.3d at 139-140.
29. *See, e.g.,* Metro-Goldwyn-Mayer Studios, Inc., v. Grokster, Ltd. 545 U.S. 913 (2005); Arista Records, LLC v. Usenet.com, Inc., 2009 WL 1873589 (S.D.N.Y. 2009).
30. Arista Records LLC v. Lime Group, LLC, Case No. 06-CV-5936 (S.D.N.Y. May 12, 2010).
31. *See, e.g.,* Perfect 10, Inc. v. Amazon, 508 F.3d 1146, 1162-1163 (9th Cir. 2007); Capital 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).
32. *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 Services v. U.S. Aero Services, Inc., Case No. 1-09CV141 (M.D. Ala. Mar. 5, 2010) (no violation of CFAA by employees who took information from company to start competing venture, as computer access was authorized).
33. Craigslist, Inc. v. Naturemarket, Inc., Case No. C-08-05065-PJH (N.D. Cal. Mar. 5, 2010).
34. Barclays Capital, Inc. v. Theflyonthewall.com,Case No. 06-4908 (S.D.N.Y Mar. 18, 2010).
35. Fed. Trade Comm'n, FTC Releases List of Top Consumer Fraud Complaints in 2008 (Feb. 26, 2009), available at *http://www.ftc.gov/opa/2009/02/2008cmpts.shtm* (the list, contained in the publication *Consumer Sentinel Network Data Book for January-December 2008*, showed that identity theft is the number one consumer complaint).