Spring 2013

TECHNOLOGY LAW IN THE DIGITAL AGE: CURRENT DEVELOPMENTS

Richard Raysman

TECHNOLOGY LAW IN THE DIGITAL AGE: CURRENT DEVELOPMENTS

Richard Raysman[*]

I. INTRODUCTION

The secure establishment, in business and personal use, of the Internet and other modes of accessing information in digital form has raised novel and complex legal issues for today's technology and intellectual property lawyers. The fast pace of this "information highway" stands in stark contrast to the traditional landscape of commercial transactional and intellectual property law. Many existing laws were not designed to deal with a technology that disseminates information at the speed, with the convenience, and to the mass audience now possible in the modern information age. Just as the number of Internet and wireless device users continues to multiply, the number of legal issues of first impression continues to make technology law an exciting and engaging area of practice.

The information technology industry is constantly changing, and its evolution continues apace. New data and media formats, new applications and services, and new methods to access and store data are constantly introduced into the business and consumer markets. It is not only important for the technology law attorney to keep abreast of these changes, but also of the changes in the law. As such, this article provides a concise resource of some of the latest legal developments in technology law, data security and privacy, and e-commerce and licensing.[1]

II. SOCIAL NETWORKS AND ONLINE ADVERTISING

In recent years, online social network websites have received a fair amount of media coverage. The attention has not only concerned their rapid growth and enormous popularity, but also, and perhaps more importantly, has focused on the novel privacy issues that have emerged vis-à-vis the websites and their members, as well as what party should be responsible for the posting of offensive or infringing content or for offsite harms that result from social network interactions.

Broadly speaking, an online social network is a structure that allows its members to share personal information and enables personal contacts through a website or other Internet portal. Member pages of "core" social network websites usually contain information and audio and visual content of a personal nature, though such information may vary widely among individual users. Other interactive websites that allow for the viewing and sharing of media or bring together a community of like-minded users often contain social networking features. Often, this data includes the age, gender and personal interests and hobbies of the individual and is shared with others whom the member determines to be "friends."

---

[*] Partner at Holland & Knight LLP. B.S., MIT (1968); J.D., Brooklyn Law School (1973).

[1] For a more thorough discussion and consideration of these issues, please refer to *Computer Law: Drafting and Negotiating Forms and Agreements*, co-authored by Richard Raysman and Peter Brown (Law Journal Press 1984-2012), *Intellectual Property Licensing: Forms and Analysis* (Law Journal Press 1999-2012), co-authored by Richard Raysman, Edward A. Pisacreta, Kenneth A. Adler and Seth H. Ostrow, and *Emerging Technologies and the Law: Forms & Analysis* (Law Journal Press 1994-2012), co-authored by Richard Raysman, Peter Brown, Jeffrey D. Neuburger and William E. Bandon, III. For a compendium of recent articles and alerts that discuss technology law issues in greater depth, please visit www.hklaw.com and the Digital Technology & E-Commerce Blog.

In some instances, the social network websites themselves have used this data in connection with marketers, albeit in different ways. In turn, this "sharing" has not only stoked the resentment of some social networking members and privacy advocates, but also has drawn the attention of the Federal Trade Commission (FTC), particularly with respect to online behavioral advertising. The FTC defines online behavioral advertising as the tracking of consumers' online activities in order to deliver tailored advertising. The agency notes that in many cases, the information collected is not personally identifiable in the traditional sense – that is, the information does not include the consumer's name, physical address, or similar identifier – rather, businesses generally use "cookies" to track consumers' activities and associate those activities with a particular computer or device.

In response, the FTC staff and industry groups, among others, have released best practices guides for this nascent advertising model. Indeed, with the proliferation of social networking websites and the marketing opportunities of behavioral advertising, it is likely that existing privacy issues will continue to emerge as the online public and the websites themselves determine when disclosure of personal information or online activities runs counter to users' expectations, industry principles, and emerging law.

In December 2010, the FTC issued a preliminary staff report to address the privacy issues associated with new technologies and business models. The report outlined a proposed framework to guide policymakers and other stakeholders regarding the best practices for consumer privacy. Generally speaking, the proposed framework called on companies to build privacy protections into their business operations, offer simplified choice mechanisms that give consumers more meaningful control, and increase the transparency of their data practices. In its Final Report in March 2012, the Commission adopted the staff's preliminary framework with certain clarifications and revisions.[2] The FTC recommends that Congress consider baseline privacy legislation and the industry implement the Report's final privacy framework through individual company initiatives and enforceable self-regulation. To the extent the Report's framework goes beyond existing legal requirements, it is not intended to serve as a template for enforcement actions. Echoing the preliminary report, the FTC prompts companies to: (1) adopt a "privacy by design" approach by building privacy protections into their everyday business practices, including providing reasonable security for consumer data, collecting only the data needed for a specific business purpose, retaining data only as long as necessary to fulfill that purpose, safely disposing of data no longer being used, and implementing reasonable procedures to promote data accuracy; (2) offer a simplified choice for businesses and consumers and give consumers the ability to make decisions about their data at a relevant time and context, including through a Do Not Track mechanism; and (3) make information collection and use practices transparent.

The Final Report clarifies at least three important principles from the preliminary report. First, the FTC addressed concerns about undue burden on small business. The Final Report's privacy framework applies to "all commercial entities that collect or use consumer data that can be 'reasonably linked' to a specific consumer, computer, or other device, unless the entity collects only

[2] *See* FTC REP., PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (Mar. 2012), *available at* http://www.ftc.gov/os/2012/03/120326privacyreport.pdf. *See also* U.S. DEP'T OF COMMERCE, INTERNET POLICY TASK FORCE, COMMERCIAL DATA PRIVACY AND INNOVATION IN THE INTERNET ECONOMY: A DYNAMIC POLICY FRAMEWORK (Dec. 2010) (stating that diminished trust in data privacy may impede innovative and productive uses of new technologies, such as cloud computing systems, and stressed the need to enlist the expertise of the private technology sector and consult existing best practices to create voluntary codes of conduct that promote informed consent and safeguard consumer information).

non-sensitive data from fewer than 5,000 consumers per year and does not share the data with third parties." Notably, the framework applies in all commercial contexts, both online and offline. As to the definition of "reasonably linked," the Final Report clarifies that data is not "reasonably linkable" to the extent that a company: (1) takes reasonable measures to ensure that the data is de-identified; (2) publicly commits not to try to re-identify the data; and (3) contractually prohibits downstream recipients from trying to re-identify the data. Second, the FTC revised its approach to how companies should provide consumers with privacy choices. The preliminary report had set forth a list of five categories of "commonly accepted" information collection practices for which companies need not provide consumers with choice (product fulfillment, internal operations, fraud prevention, legal compliance and public purpose, and first-party marketing). Under the Final Report, the Commission set forth a modified approach that focuses on the context of the consumer's interaction with the business. Under this approach, companies would not need to provide choice before collecting and using consumers' data for "practices that are consistent with the context of the transaction, consistent with the company's relationship with the consumer, or as required or specifically authorized by law." Although many of the "commonly accepted practices" previously identified in the preliminary report would generally meet this standard, there may be exceptions. For data collection practices requiring choice, the agency stated that companies should offer the choice at a time and in a context in which the consumer is making a decision about his or her data. Moreover, the Report stated that companies should obtain affirmative express consent before (1) using consumer data in a materially different manner than claimed when the data was collected; or (2) collecting sensitive data for certain purposes. Third, the FTC recommends that Congress consider enacting targeted legislation to provide greater transparency for, and control over, the practices of information brokers. The agency also called on Congress to enact legislation addressing data security.

Last, the Final Report announced that the agency would focus its future policymaking efforts on five main privacy items: (1) *Do Not Track*: The FTC summarized current industry efforts on this front, but stressed that it would continue to work with these groups to complete implementation of an easy-to use, persistent, and effective Do Not Track system; (2) *Mobile Privacy*: The Report calls on mobile service companies to establish standards that address data collection, transfer, use, and disposal, particularly for location data; (3) *Data Brokers*: To address the issue of transparency and consumer control over data brokers' collection and use of consumer information, the FTC stated that it supports targeted legislation that would provide consumers with access to information about them held by a data broker. The agency also advocated the creation of a centralized website where data brokers could detail the access rights and other choices regarding consumer data; (4) *Large Platform Providers*: The Report reemphasizes that large platforms (e.g., ISPs, operating systems, browsers, and social media) that seek to comprehensively track consumers' online activities raise heightened privacy concerns; and (5) *Promoting Enforceable Self-Regulatory Codes*: The FTC will continue to facilitate the development of industry-specific codes of conduct and will use the FTC Act to take action against companies that engage in unfair or deceptive practices, including the failure to abide by self-regulatory programs they join.

In January 2010, the Financial Industry Regulatory Authority (FINRA), the independent regulator for securities firms doing business in the United States, issued Regulatory Notice 10-06, a guidance to securities firms and brokers regarding the use of social networking websites for business

purposes.[3] Among its key provisions: (1) *Recordkeeping Responsibilities*: "Every firm that intends to communicate, or permit its associated persons to communicate, through social media websites must first ensure that it can retain records of those communications" as required by law; (2) *Suitability Responsibilities*: Regarding recommendations of specific investment products, the Notice urges firms to adopt specific policies, namely, prohibiting recommendations through social media websites without approval of a registered principal, or in the alternative, maintaining a database of recommendations previously approved by a registered principal that can be accessed by personnel; (3) *Interactive Forums*: Real-time interactive communications from a blog or social network page do not require such approval from a principal prior to posting, yet would require that the firm have in place adequate supervisory procedures to minimize compliance risks, such as lexicon-based or random reviews of such interactive electronic communications; (4) *Social Media Restrictions*: Generally speaking, the Notice requires firms to adopt procedures to ensure that personnel using social media websites are adequately supervised and trained; (5) *Third-Party Content*: FINRA does not deem third-party posts as a firm's public communication subject to approval, content, and filing requirements. However, the FINRA Notice states that third-party content might be ascribed to the firm if the firm is "entangled" with the preparation of the content or has "adopted" or implicitly or explicitly endorsed the third-party content.

In July 2009, leading industry associations developed a set of consumer protection principles for online behavioral advertising, meant to correspond with the FTC Staff Report on the issue.[4] The industry's Self-Regulatory Program is broken down into seven principles, which propose that participating organizations and websites, among other things, clearly disclose data collection and use practices with links and disclosures on the Web page where the advertisement appears; permit consumers to choose whether or not their data will be collected, used, or transferred to another entity for behavioral advertising purposes; prohibit service providers from collecting data for behavioral advertising purposes without affirmative consumer consent; adopt reasonable security practices and limit data retention; obtain consent when making material changes to its data collection practices that results in more data collection; and make special considerations for sensitive data, including not collecting financial account numbers, Social Security numbers, pharmaceutical prescriptions, or medical records for behavioral advertising purposes without consumer consent.

The Working Party, an independent European advisory body on data protection and privacy, issued an Opinion informing social network websites on how they can work to comply with the EU data protection law, including the 1995 Data Protection Directive (95/46/EC) (Directive).[5] The Opinion notes that social network website providers and, in many cases, third party application providers, are data controllers under the Directive because they provide the means for the processing of user data and undertake the basic service of user management (e.g. registration and deletion of accounts). The Opinion makes clear that websites should maintain appropriate technical safeguards to prevent unauthorized access of users' information and make available to users easy-to-use default

[3] FINRA REGULATORY NOTICE 10-6, SOCIAL MEDIA WEBSITES: (Jan. 2010), *available at* http://www.finra.org/web/groups/industry/@ip/@reg/@notice/documents/notices/p120779.pdf.

[4] AM. ASS'N OF ADVER. AGENCIES ET AL., SELF REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING (2009), *available at* http://www.iab.net/media/file/ven-principles-07-01-09.pdf.

[5] Article 29 Data Protection Working Party, Opinion 5/2009 on online social networking (June 12, 2009), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf.

settings to restrict access to users' personal information beyond their desired contacts. Regarding the use of information, the Opinion states that websites should inform users of the different purposes for which they process personal data, including using members' data for marketing functions, the sharing of data with third-parties and the use of users' sensitive data. The Opinion also states that personal data of users should be removed as soon as their accounts are deleted and that inactive accounts should no longer be visible to the outside world.

In *Facebook, Inc. v. Power Ventures, Inc.*, the Northern District of California looked at whether a social network profile aggregating service may be liable for copyright infringement for gaining consent from users to make copies of their social network profile pages and then "scraping" the data from the social network for use on its own website.[6] The court denied the defendant's motion to dismiss, rejecting the defendant's argument that no infringement was possible because the profile user pages were not protected by copyright and the social network website did not hold any rights to user content. The court conceded that the defendant correctly asserted that the social network website did not have a copyright on the user content the defendant sought, but found that if the defendant first had to make a copy of a user's entire profile page in order to collect that user content, such action might violate the website's terms of use, citing *Ticketmaster L.L.C. v. RMG Techs, Inc.*[7] The court also refused to dismiss the "indirect" copyright infringement claims, finding that the defendant's inducement of users to exceed their authorized usage and thereby allow the defendant to make copies of their profile pages may support a contributory claim. The court also let stand the social network's Digital Millennium Copyright Act (DMCA) claims for the defendant's automated activities that allegedly circumvented certain anti-scraping technological measures on the website that were designed to protect copyrighted content.

In further proceedings, the court granted the plaintiff's motion for summary judgment on its CAN-SPAM and Computer Fraud and Abuse Act (CFAA) claims.[8] The court rejected the defendant's argument that because Facebook's own servers sent the commercial e-mails at issue, the defendants did not "initiate" the e-mails as a matter of law. The court found that although Facebook servers did automatically send the emails at the instruction of the defendant's software, it was clear that the defendants' actions – in creating a friend referral promotion with monetary incentives, importing users' friends to the guest list, and authoring the e-mail text – served to "originate" the e-mails as is required by the CAN-SPAM Act. Regarding the CFAA claim, the court found that the defendant circumvented technical barriers to access Facebook website, and thus accessed the website "without authorization" and that the plaintiff established that its losses exceeded the $5,000 CFAA threshold by offering evidence of the IT costs of attempting to thwart the unauthorized access into its network.

In *Pietrylo v. Hillstone Restaurant Group*, a jury found that an employer violated federal and state computer privacy laws, and was liable for back pay and damages for terminating two employees

---

[6] Facebook, Inc. v. Power Ventures, Inc., 2009 WL 1299698 (N.D. Cal. May 11, 2009). In further proceedings the court found denied the plaintiff's motion on the pleadings on its state law computer fraud claim, finding that the defendant did not act "without permission" within the meaning of Section 502 of the statute when Facebook account holders utilized the defendant's website to access and manipulate their user content on Facebook, even if such action violated Facebook's Terms of Use. However, the court ruled that to the extent that the plaintiff can prove that in doing so, the defendant Power circumvented Facebook's technical barriers, the defendant may be held liable for violation of Section 502. *See* Facebook, Inc. v. Power Ventures, Inc., 2010 WL 3291750 (N.D. Cal. July 20, 2010).

[7] 507 F. Supp. 2d 1096 (C.D. Cal. 2007).

[8] Facebook, Inc. v. Power Ventures, Inc., 844 F.Supp.2d 1025 (N.D. Cal. 2012).

after gaining unauthorized access to a private MySpace page that was created by the plaintiffs and was critical of the company.[9] The jury concluded that the company violated the federal Stored Communications Act and the New Jersey state computer privacy law when a manager asked another employee, presumably under the duress of maintaining her employment, for the password to the private MySpace page and then shared its contents with upper management, resulting in the termination of the plaintiffs. The jury also found that the employer was not liable for invasion of privacy.

The court in *Yath v. Fairview Clincs, N.P.* determined that the "publicity" element of a state law invasion of privacy claim, which required, in part, that the matter be made public by communicating it to the public at large, was satisfied when private healthcare information was posted on a publicly accessible social network website for 24 hours.[10]

In *Romano v. Steelcase Inc.*, the court held that a defendant is entitled to compel production of the plaintiff's social network data (including current and historical, deleted pages and related information) based upon a review of the public portions of the plaintiff's social network pages that allegedly revealed an active lifestyle that conflicted with the plaintiff's injury claims.[11] Rejecting the plaintiff's objections to producing her social network data, the court ruled that the information was both material and necessary to the defense of this action and that the plaintiff could not hide relevant information "behind self-regulated privacy settings."

In *Moreno v. Hanford Sentinel, Inc.*, the court held that the author of an article posted to a social network website cannot state a cause of action for invasion of privacy against the person who submitted that article to a newspaper for republication.[12] However, the court declined to dismiss the

---

[9] Pietrylo v. Hillstone Rest. Group, No. 06-5754 (D. N.J. jury verdict June 16, 2009).

[10] Yath v. Fairview Clinics, N.P., 767 N.W.2d 34 (Minn. Ct. App. 2009). *See also Arenas v. Shed Media*, 881 F.Supp.2d 1181 (C.D. Cal. 2011) (basketball player not likely to succeed on right of publicity claims against reality TV show due to the availability of a "public interest" defense; plaintiff had made aspects of his personal life a matter of public concern based on his series of posts to his Twitter account). *But see* Lalonde v. Lalonde, 2011 WL 832465 (Ky. Ct. App. Feb. 25, 2011) (holding that under ordinary circumstances, "[t]here is nothing within the law that requires permission when someone takes a picture and posts it on a Facebook page. There is nothing that requires permission when she [is] 'tagged' or identified as a person in those pictures").

[11] Romano v. Steelcase Inc., 30 Misc.3d 426 (N.Y. Sup. Ct. Suffolk Cty. 2010). *See also* Thompson v. Autoliv ASP, Inc., 2012 WL 2342928 (D. Nev. June 20, 2012) (plaintiff ordered, with certain restrictions, to upload five years of social media materials onto external hard drive for inspection; plaintiff's public Facebook profile provided evidence of the plaintiff's post-accident activities and mental state and were relevant to the claims and defenses in the case); Davenport v. State Farm Mutual Auto. Ins. Co., 2012 WL 555759 (M.D. Fla. Feb. 21, 2012) (finding that defendant's discovery requests for social media access were overly broad and limited the defendant to discovery of photographs added to any social networking website since the date of the subject accident that depict the plaintiff, including photos that she posted online or ones in which she was "tagged"; court denied defendant's request that the plaintiff grant access to all electronic devices used by the plaintiff to access social networks, commenting that the defendant did not have a generalized right to rummage at will through information that the plaintiff has limited from public view). *But see* McCann v. Harleysville Ins. Co. of N.Y., 78 A.D.3d 1524 (N.Y. App. Div., 4th Dept. 2010) (affirming lower court decision to deny of the defendant's motion to compel a signed authorization for access to the plaintiff's social network account because defendant "failed to establish a factual predicate with respect to the relevancy of the evidence" and essentially sought permission to conduct "a fishing expedition into plaintiff's Facebook account"); Tompkins v. Detroit Metro. Airport, 278 F.R.D. 387 (E.D. Mich. 2012) (declining to allow the defendant to view the plaintiff's entire Facebook account or all posted photographs, finding that public postings and surveillance photographs that showed the plaintiff holding a toy dog and pushing a shopping cart did not belie the plaintiff's claims of injury and were not a sufficient predicate showing that the private Facebook material would be reasonably calculated to lead to the discovery of admissible evidence); Mailhoit v. Home Depot U.S.A., Inc., 285 F.R.D. 566 (C.D. Cal. 2012) (denying motion to compel social media postings relating to emotional events or reactions as overly vague, but allows discovery into postings between plaintiff and fellow employees that referenced her employment or the ongoing litigation).

[12] Moreno v. Hanford Sentinel, Inc., 172 Cal.App.4th 1125 (2009).

defendant's intentional infliction of emotional distress claim, concluding that it was a question of fact, since reasonable people might differ on whether the defendant's action were extreme and outrageous.

In *Facebook Inc. v. Wallace*, a social network was entitled to a preliminary injunction against an alleged spammer who accessed user accounts without authorization or through phishing schemes and allegedly perpetrated a widespread spam and phishing campaign.[13]

In a formal opinion, the Association of the Bar of the City of New York Committee on Professional Ethics stated that a lawyer may not attempt to gain access to a social networking website under false pretenses, either directly or through an agent.[14] Rather, a lawyer should rely on discovery procedures sanctioned by the ethical rules and case law to obtain relevant evidence, such as the truthful "friending" of unrepresented parties or by using formal discovery devices such as subpoenas directed to non-parties in possession of information maintained on an individual's social networking page.

III. PRIVACY RIGHTS AND DATA SECURITY

There is no comprehensive set of privacy rights or legislation in the United States addressing the collection, storage, transmission or use of personal information on the Internet or in other business environments. Instead, privacy has generally been protected by common law and by federal and state legislation enacted as new technologies develop, to target specific privacy-related issues.

For example, the Electronic Communications Privacy Act (ECPA) is the federal statute that updated wiretapping laws to include protection for electronic communications, such as emails. The Act further proscribes the intentional use of the contents of any wire, oral, or electronic communication, obtained through interception, and allows for both criminal penalties and civil causes of action for violations of its provisions. Specifically, the ECPA protects "point-to-point" electronic communications, or communications as they travel through cyberspace. The ECPA contains two sections: Title 1 amended the Wiretap Act, and Title II created the Stored Communications Act. Consequently, the ECPA established a two-tier system, creating separate categories of violations predicated upon whether the electronic communications are accessed while "in transit" or while "in storage."

---

[13] Facebook, Inc. v. Wallace, 2009 WL 840391 (N.D. Cal. Mar. 24, 2009). *See also* Facebook, Inc. v. Fisher, 2011 WL 250395 (N.D. Cal. Jan. 26, 2011) (large default judgment against spammers).

[14] Ass'n of the Bar of N.Y.C. Comm. on Prof'l Ethics, Formal Op. 2 (2010) (Obtaining Evidence From Social Networking Websites). *See also* NYCLA Comm. on Prof'l Ethics, Formal Op. 743 (2011) (a lawyer may search a prospective or sitting juror's social networking profile, provided there is no contact or communication with the prospective or sitting juror and the lawyer does not seek to "friend" jurors, or subscribe to their Twitter accounts, or otherwise contact them; if a lawyer discovers juror misconduct, he or she must promptly bring such misconduct to the attention of the court, under N.Y. Rules of Professional Conduct 3.5(d)); San Diego Cty. Bar Ass'n., Legal Ethics Op. 2 (2011) (rules of ethics bar an attorney from making an *ex parte* friend request to a represented party because an attorney's communication to a represented party intended to elicit information about the subject matter of the representation is impermissible no matter what words are used in the communication; moreover, an attorney may not send a friend request to an unrepresented witnesses without disclosing the purpose of the request); NY State Bar Ass'n, Comm. on Prof'l Ethics, Op. 843 (2010) (lawyer representing a client in pending litigation may access the public pages of another party's social networking website for the purpose of obtaining possible impeachment material for use in the litigation); The Phila. Bar Ass'n Prof'l. Guidance Comm., Op. 2 (2009) (act of hiring an investigator to mislead a potential witness by becoming social network "friends" with the witness in order to obtain access to personal pages for future impeachment was deemed a violation of ethical rules); Carino v. Muenzen, 2010 WL 3448071 (N.J. Super. A.D. Aug. 30, 2010) (unpublished) (searching prospective jurors in the courtroom is permissible).

Although many privacy laws address the government's use of personal information, many others address the use of personal information by private entities, whether it be financial, medical, or sensitive consumer information, commercial messages sent via email, facsimile or SMS, or electronic data intercepted during transmission or improperly accessed from data storage. Moreover, federal and state data security laws that impact electronic privacy concerns have recently been enacted to stem the scourge of malicious software and identity theft, and at least 46 states have passed some form of a data security breach notification law requiring notice in the event of a qualifying data breach of sensitive consumer information.

Advances in Internet technology have also allowed website operators and advertisers to collect, compile and distribute personal information about users' Internet browsing activities, both with and without the user's consent. Such practices will almost always implicate privacy concerns.

In *Patco Constr. Co. v. People's United Bank,* the First Circuit held that a bank's security procedures for a commercial account holder, who was the victim of fraudulent wire transfers, were not commercially reasonable under UCC Article 4A.[15] The appeals court reversed the lower court's grant of summary judgment to the bank and remanded the case. The court concluded that the bank, whose security system prompted users logging in to answer challenge questions on any transaction over $1, increased the risk that such answers would be captured by keyloggers or other malware. Moreover, the court concluded that the bank's failure to monitor and immediately notify customers of abnormal transactions that had been flagged by its security software was not commercially reasonable. The court stated that such collective failures taken as a whole rendered the bank's security system commercially unreasonable under the UCC. The appeals court also reinstated some of the plaintiff's common law claims, finding that while Article 4A displaced the plaintiff's negligence claim, the plaintiff's breach of contract and breach of fiduciary duty were not preempted by Article 4A because such claims were not inherently inconsistent or in conflict with the plaintiff's overarching Article 4A claim. However, despite ruling that the bank's security procedures were not commercially reasonable, the appeals court affirmed the denial of the plaintiff's summary judgment claim. The court noted several disputed issues of fact surrounding the question of whether the plaintiff had satisfied its obligations and responsibilities under Article 4A, or at least to the question of damages.

Users alleging that a social media website disclosed "personally identifiable browsing histories" and unique identifiers to third-party advertising companies via cookies have standing via the Stored Communications Act (SCA), but failed to state a cognizable SCA claim on the merits because LinkedIn was neither acting as a "electronic communication service" (e.g., email provider) or "remote computing service" (e.g., virtual storage provider) when it disclosed LinkedIn IDs and URLs of users' viewed pages to third parties.[16] The court dismissed the plaintiffs' amended complaint, including the plaintiffs' common law invasion of privacy claim because they failed to meet the high standards for the type of invasion that is actionable (i.e., an intrusion that is "highly

[15] Patco Constr. Co. v. People's United Bank, 684 F.3d 197 (1st Cir. 2012). *See also* Experi-Metal, Inc. v. Comerica Bank, 2011 WL 2433383 (E.D. Mich. June 13, 2011) (genuine issue of material fact as to whether the defendant bank accepted in "good faith" fraudulent wire transfers initiated by unknown phishers in the plaintiff's name); Choice Escrow and Land Title, LLC v. BancorpSouth Bank, No. 10-03531 (W.D. Mo. order denying motion regarding sufficiency of plaintiff's responses at deposition Aug. 20, 2012) (in a dispute between a customer and bank over unauthorized ACH wire transfers, UCC Article 4A preempts indemnity provision whereby the customer agreed to indemnify the bank for any losses, costs, liabilities, or expenses).

[16] Low v. LinkedIn Corp., 2012 WL 2873847 (N.D. Cal. July 12, 2012).

offensive to a reasonable person"). The court also dismissed the plaintiffs' breach of contract claim because the alleged decrease in the value of plaintiffs' personal information did not constitute cognizable contract damages for the purposes of a contract claim.

The Northern District of California held in *Keller v. Electronic Arts, Inc.* that a former college athlete may proceed with right of publicity claims against a video game maker that designed a game with virtual football players to resemble real-life college football athletes because the game maker's use of the player's image was not sufficiently transformative that the First Amendment would bar his California right of publicity claims as a matter of law.[17] The court stated that the game maker's use of the player's image was not transformative, because the game presented virtual players that were nearly identical to their real-life counterparts (i.e. sharing the same jersey numbers, similar physical characteristics and background information); depicted the plaintiff in the same setting he was known for, namely, a collegiate football field; and allowed users to download actual team rosters and players' names into the game. The court distinguished the Eighth Circuit's holding in *C.B.C. Distribution and Marketing v. Major League Baseball Advanced Media,*[18] which involved a company's use of player's names and statistics for "fantasy sports" games, concluding that the defendant's game "does not merely report or publish Plaintiff's statistics and abilities. On the contrary, [the defendant] enables the consumer to assume the identity of various student athletes and compete in simulated college football matches."

An individual who was the victim of his ex-spouse's installation of keylogging software on his computer could not bring federal communications privacy or state law negligence claims against the software maker for his emotional distress and humiliation, the Eastern District of Tennessee held in *Hayes v. SpectorSoft Corp.*. The court dismissed the plaintiff's complaint.[19] The court found that the plaintiff's federal communications privacy claim failed because plaintiff failed to rebut evidence of the software maker's lack of intent to divulge the plaintiff's private communications and the software maker's right to expect that its software should be used in accordance with the accompanying licensing agreement. In addition, the court dismissed the plaintiff's product liability claim, finding it noticeably lacking in any suggestion of the kind of injury required by Tennessee law, namely, personal injury, death, or property damage. The court also deemed the plaintiff's negligence claim deficient, concluding that no authority suggested that a manufacturer of monitoring software owed a duty to avoid emotional injury to the victim of the misuse of that software in violation of the software's licensing agreement.

---

[17] Keller v. Elec. Arts, Inc., 2010 WL 530108 (N.D. Cal. Feb. 8, 2010). *But see* The Univ. of Ala. Bd. of Trs. v. New Life Art, Inc., 683 F.3d 1266 (11th Cir. June 11, 2012) (artist's First Amendment interests clearly outweigh whatever consumer confusion that might exist concerning his paintings depicting University of Alabama football games; Lanham Act claims over the sale of paintings, prints and calendars that include the University's football crimson and white uniforms are dismissed); Hart v. Electronic Arts, Inc., 808 F.Supp.2d 757 (D.N.J. 2011) (finding sufficient elements of the videogame maker's own expression in the game such that its use of a former college football player's image in a NCAA football videogame was transformative and the First Amendment barred plaintiff's right of publicity claim); Habush v. Cannon, 2011 WL 2477236 (Wis. Cir. Ct. June 8, 2011) (attorneys right of publicity claims against a competing law firm that purchased their last names as keywords dismissed because while the plaintiffs had shown that the keyword purchase was an unauthorized use under the statute, the plaintiff failed to show that the use was done "unreasonably," given the general nature of competition and the fact that the competing law firm did not use the plaintiffs' names in the advertisement text, among other things).

[18] C.B.C. Distribution and Marketing v. Major League Baseball Advanced Media, 505 F.3d 818, 820-21 (8th Cir. 2007).

[19] Hayes v. SpectorSoft Corp., 2009 WL 3713284 (E.D. Tenn. Nov. 3, 2009). *But see* Klumb v. Goan, 884 F.Supp.2d 644 (E.D. Tenn. 2012) (finding that "interception" occurs when spyware automatically routes a copy of an email, which is sent through the internet, back through the internet to a third party's email address when the intended recipient opens the email for the first time).

In *Markert v. Becker Technical Staffing Inc.*, the court held that the federal SCA is not violated simply by reading printouts of emails that were electronically stored at one point; instead, the Act attaches liability to the accessing of the stored communication without authorization.[20] The court granted the moving defendants' motion to dismiss the SCA claims, as well as state privacy law intrusion upon seclusion claims. Similar to the reasoning behind the dismissal of the SCA claim, the court found the plaintiff did not automatically have a cause of action against those who subsequently viewed his previously private emails. The court stated that once the emails were obtained from the plaintiff's personal email, the intrusion upon seclusion was complete and that any cause of action that the plaintiff had for invasion of privacy would be against the person who initially invaded the privacy and subsequently disseminated the information.

Zheng v. Yahoo! Inc. held there is no language in the ECPA itself, nor to any statement in the legislative history indicating Congress intended the statute to apply to activities occurring outside the United States.[21] The court dismissed the plaintiff's federal electronic privacy-related claims stemming from an alleged disclosure of user information to Chinese authorities. The court also rejected the plaintiffs' argument that because the defendant email provider had servers located around the globe, email communications may have traveled through the defendant's networks in the United States. The court stated that because the alleged interceptions and disclosures occurred "locally" within China, the ECPA did not apply, even if the communications, prior to their interception and disclosure, traveled electronically through a network located in the United States.

According to the District of Connecticut in *McLoughlin v. People's United Bank, Inc.*, theft of personal consumer data that resulted in a risk of future injury, but no actual misuse of information, does not represent an ascertainable loss under Connecticut state law.[22] While the district court found that the plaintiff alleged an adequate injury-in-fact for standing purposes, it ultimately granted the

[20] Markert v. Becker Technical Staffing, Inc., 2010 WL 1856057 (E.D. Pa. May 7, 2010). *See also* Van Alstyne v. Elec. Scriptorium Ltd., 560 F.3d 199 (4th Cir. 2009) (finding that proof of actual damages is a prerequisite to recovering statutory damages under the Stored Communications Act, though not for an award of either punitive damages or attorney's fees under the statute); Worix v. MedAssets Inc., 2012 WL 787210 (N.D. Ill. Mar. 8, 2012) (finding that alleged failure to take steps to protect database from theft and security breach did not constitute "knowingly divulging" information under the SCA); Thompson v. Ross, 2010 WL 3896533 (W.D. Pa. Sept. 30, 2010) (unauthorized access of previously received email messages that had been downloaded by the recipient and saved to the hard drive of a personal laptop computer does not violate the Stored Communications Act because SCA protection does not extend to emails and messages stored only on a personal computer and not with an ISP or other electronic communications service); Chasten v. Franklin, 2010 WL 4065606 (N.D. Cal. Oct. 14, 2010) (Stored Communications Act bars the enforcement of a subpoena directed to an email service provider to obtain the contents of an account holder's emails, absent the consent of the account holder); In re Beluga Shipping GMBH v. Suzlon Energy, Ltd., 2010 U.S. Dist. LEXIS 104705 (N.D. Cal. Sept. 23, 2010) (SCA prohibits email service from divulging the stored messages of a non-party witness pursuant to a civil subpoena, absent application of certain statutory exceptions or the account holder's consent); Fontenot v. Brouillette, No. 10-01053 (S.D. Tex. Feb. 9, 2012) (because email messages were still maintained on the system and not downloaded or removed from electronic storage, subpoena to service provider seeking plaintiff's personal emails was quashed); Bower v. Bower, 808 F.Supp.2d 348 (D. Mass. 2011) (court cannot imply an intent to consent to the disclosure of electronic information from email providers under the SCA based upon the party's default or status as a fugitive). *But see* Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp, LLC, 759 F.Supp.2d 417 (S.D.N.Y. 2010) (small award of SCA damages for employer's unauthorized access to ex-employee's private email accounts).

[21] Zheng v. Yahoo! Inc., 2009 WL 4430297 (N.D. Cal. Dec. 2, 2009). *But see* Suzlon Energy Ltd. v. Microsoft Corp., 671 F.3d 726 (9th Cir. 2011) (the protections of the ECPA extend to the contents of communications of foreign citizens; however, "the Court does not address here whether the ECPA applies to documents stored or acts occurring outside of the United States").

[22] McLoughlin v. People's United Bank, Inc., 2009 WL 2843269 (D. Conn. Aug. 31, 2009). *See also* FAA v. Cooper, 132 S.Ct. 1441 (2012) (the federal Privacy Act does not unequivocally authorize damages for mental or emotional distress; because Congress did not speak unequivocally, the Court adopted an interpretation of "actual damages" limited to proven pecuniary harm).

defendant's motion to dismiss the plaintiff's negligence, unfair trade practice and other state law claims. The court concluded that the plaintiff's alleged injuries were solely the result of a perceived and speculative risk of future injury that might never occur, unsupported by any allegation of malfeasance, and as such, could not form a cognizable claim.

In *Quon v. Arch Wireless Operating Co., Inc.*, the Ninth Circuit held that under the SCA, a text message service is prohibited from disclosing contents of text messages, absent the consent of the addressee or intended recipient of such communications.[23] The appeals court reversed the lower court's ruling that the text message service permissibly released transcripts of the plaintiff-police officer's text messages sent and received from his work-issued pager for the purpose of an audit by his employer. The court also ruled that the government employer had violated the employer's reasonable expectation of privacy under the Fourth Amendment. The court found that, under the SCA, the text message service was an "electronic communication service" (i.e., any service which provides users the ability to send or receive wire or electronic communications). Accordingly, the text message service was prohibited from releasing the contents of a communication without the lawful consent of the addressee or intended recipient.

In further proceedings, the Supreme Court granted certiorari on the sole issue of ruling on the Ninth Circuit's holding that the city employer violated the Fourth Amendment.[24] The Court was reticent to fashion a general principle about electronic privacy around text messages sent or received by government employees and decided the case on narrower grounds. The Court stated that even assuming the city employee had a reasonable expectation of privacy in his text messages, the city did not necessarily violate the Fourth Amendment by obtaining and reviewing the transcripts of the messages because (1) there were reasonable grounds for suspecting that the search was necessary for a non-investigatory work-related purpose; (2) the review of the transcripts was an efficient and expedient way to determine whether the employee's excess usage was due to personal use; and (3) even if the SCA forbade the cellular phone carrier from turning over the transcripts, it did not follow that the city's actions were unreasonable under the Fourth Amendment.

In *United States v. Weaver*, the Central District of Illinois held that under the federal SCA, a court can compel an ISP to comply with a trial subpoena and produce the contents of a subscriber's previously-opened Web-based emails that had not been downloaded onto the subscriber's computer but remained in online storage and were less than 181 days old.[25] The court commented that under § 2703 of the Act, governmental entities must use a warrant to obtain certain types of electronic communications, but they can access others using only a trial subpoena such as emails less than 181

[23] Quon v. Arch Wireless Operating Co., 529 F. 3d 892 (9th Cir. 2008).

[24] City of Ontario v. Quon, 130 S.Ct. 2619 (2010).

[25] United States v. Weaver, 636 F.Supp.2d 769 (C.D. Ill. 2009). *But see* United States v. Warshak, 631 F.3d 266 (6th Cir. 2010) (a subscriber enjoys a reasonable expectation of privacy in the contents of emails that are stored with, or sent or received through, a commercial ISP and the government may not compel a commercial ISP to turn over the contents of a subscriber's emails without first obtaining a warrant based on probable cause); Matter of Historical Cell-Website Information, 809 F.Supp.2d 113 (E.D.N.Y. 2011) (request for 113 days of cumulative cell-website location records for the cell phone of an individual who was the target of a criminal investigation constitutes a search under the Fourth Amendment); United States v. Jones, 132 S.Ct. 945 (U.S. Jan. 23, 2012) (attachment of a GPS tracking device to an individual's vehicle, and subsequent use of that device to monitor the vehicle's movements on public streets for an extended period, constituted a search within the meaning of the Fourth Amendment); In re Applications for Search Warrants for Info. Associated with Target Email Address, 2012 WL 4383917 (D. Kan. Sept. 21, 2012) (Fourth Amendment protects emails stored with, sent to or received from an email service provider; Government's warrant seeking all emails and online faxes linked to the account deemed overly broad and not particularized).

days old, under certain circumstances. The court found that the ISP's Web-based email service held or maintained subscribers' emails solely to provide customer storage or computer processing services, and not for the purpose of backup protection (which would have triggered the warrant requirement), and thus the ISP was required to comply with the government's subpoena.

The warrantless search of data within a cell phone seized incident to an arrest is prohibited by the Fourth Amendment when the search is unnecessary for the safety of police officers and there are no exigent circumstances, according to *State v. Smith*.[26] The Ohio Supreme Court there reversed and remanded to the trial court for a new trial based upon the trial court's improper admission of the call records and phone numbers from the defendant's phone. In an issue of first impression, the court rejected the state's argument that a cell phone is akin to a closed container and subject to search for the preservation of evidence, concluding that even the more basic models of modern cell phones are capable of storing a wealth of digitized information wholly unlike any physical object found within a closed container, giving the individual a privacy interest in the contents that goes beyond the privacy interest in a simple address book or pager.

In *Merritt, Flebotte, Wilson, Webb & Caruso, PLLC v. Hemmings*, an employer that removed all biographical information and links pertaining to departing employees from its website, but did not take steps to remove the photo files that were stored on an outside server such that an Internet search engine might return links to some of the deleted biographical pages, was not liable for misappropriation for a commercial purpose of the employees' image or biographies.[27]

According to *Boring v. Google, Inc.*, residents' state privacy claims against a search engine that offered online "street view" mapping images from their private driveway, including images of the outside of the plaintiffs' residence, are not cognizable because such conduct would not be highly offensive to a person of ordinary sensibilities.[28] The appeals court affirmed the dismissal of privacy and negligence claims against the search engine, but reversed the lower court's dismissal of the plaintiffs' trespass claim. The court allowed the trespass claim to go forward, because the plaintiffs alleged that the defendant entered their property without permission, which, if proven, would constitute a trespass. The court commented that there was no requirement under Pennsylvania law that damages be pled, either nominal or consequential, in trespass cases, even though "it may well be

[26] State v. Smith, 920 N.E.2d 949 (2009). *See also* United States v. Kirschner, 823 F.Supp.2d 665 (E.D. Mich. 2010) (subpoena requesting that defendant reveal password to encrypted contents of his computer was deemed testimony and violated the defendant's right against self-incrimination under the Fifth Amendment). *But see* United States v. Fricosu, 841 F.Supp.2d 1232 (D. Colo. 2012) (Fifth Amendment is not implicated by requiring production of the unencrypted contents of a criminal defendant's laptop that had previously been authenticated as the defendant's personal home computer); United States v. Skinner, 690 F.3d 772 (6th Cir. 2012) (criminal suspect did not have a reasonable expectation of privacy in the data emanating from his pay-as-you-go cell "burner" mobile phone that emanated GPS data revealing its location to police); United States v. Flores-Lopez, 670 F.3d 803 (7th Cir. 2012) (warrantless search of individual's cell phone as an incident to arrest to ascertain its assigned telephone number did not violate Fourth Amendment); People v. Diaz, 51 Cal.4th 84 (Cal. 2011) (a warrantless search of the text message folders of an arrestee's cell phone 90 minutes after being taken into custody was valid as being "incident to a lawful custodial arrest"); Sitton v. Print Direction, Inc., 718 S.E.2d 532 (Ga. App. 2011) (employer's viewing and printing of incriminating emails viewable from plaintiff's laptop open on office desk showed plaintiff was impermissibly conducting a competing business did not constitute computer theft or trespass since it was not done "without authority" and pursuant to the company's computer usage policy that stated that "[Employer] will ... inspect the contents of computers, voice mail or electronic mail in the course of an investigation triggered by indications of unacceptable behavior").

[27] Merritt, Flebotte, Wilson, Webb & Caruso, PLLC v. Hemmings, 676 S.E.2d 79 (N.C. Ct. App. 2009).

[28] Boring v. Google Inc., 362 Fed.Appx. 273 (3rd Cir. 2010).

that, when it comes to proving damages from the alleged trespass, the [plaintiffs] are left to collect one dollar and whatever sense of vindication that may bring."

The court in *Burnett v. County of Bergen* held that a request by a commercial entity for the bulk release of land title records that contain citizens' social security numbers must be redacted before release to protect citizen privacy, with the requestor ordered to pay the redaction and duplication costs.[29] The court found that the twin aims of public access and the protection of personal information weighed in favor of redacting social security numbers from the requested records before releasing them. The court limited its holding to the facts of this case, which involved a bulk request for millions of realty records, spanning decades, containing a substantial number of social security numbers the requestor did not need, whose dissemination via a centralized computer database would pose an increased risk of identity theft to countless individuals with no possibility of advance notice to those individuals and where the request does not further the state Open Public Records Act's core aim of transparency in government.

In *Pinero v. Jackson Hewitt Tax Service Inc.*, mere violations of a firm's written privacy policy following the alleged mishandling of the disposal of confidential documents cannot form the basis of a fraudulent inducement action, absent showing of actual damages and heightened factual pleading.[30] After the plaintiff filed an amended complaint, the defendants again moved to dismiss, arguing that the plaintiff failed to plead fraud with the requisite particularity. The court denied the defendant's motion, concluding that the plaintiff's new allegations that delineated nine specific ways the defendants failed to maintain policies and procedures to protect customer privacy satisfied the heightened pleading requirements and could form the basis of a claim that the defendant's alleged misrepresentation as to its written privacy policy induced the plaintiff to transact business with the defendant.[31]

A. *Privacy-Related Enforcement Actions*

The FTC has taken an active role with respect to protecting privacy rights in connection with the collection and use of personal information for commercial purposes. Most notably, the FTC has undertaken enforcement actions against entities that sold information to third parties for commercial purposes contrary to a website privacy policy, failed to keep consumer information secure, installed malicious spyware or adware onto unknowing consumers' computers, or violated the federal do-not-call list with an unlawful telemarketing campaign. In addition, federal civil rights laws and the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, together protect individuals' rights of nondiscrimination and health information privacy, with enforcement falling upon the Department of Health and Human Services (HHS) Office for Civil Rights (OCR). In *In re*

[29] Burnett v. County of Bergen, 968 A.2d 1151 (N.J. 2009).

[30] Pinero v. Jackson Hewitt Tax Service Inc., 594 F.Supp.2d 710 (E.D. La. 2009). *See also* Cornelius v. Deluca, No. 10-27 (D. Idaho Mar. 15, 2011) (non-party, volunteer website moderator's First Amendment right to post anonymously outweighs plaintiffs' need for relevant discovery; moderator had an expectation of privacy based on the website's Terms of Service and Privacy Policy). *See generally* Lee v. The Picture People Inc., No. 10C-07-002 (Del. Super. Ct. Mar. 19, 2012) (breach of warranty claims related to sale of photographs cannot be based on company's unrelated website privacy policy).

[31] *See* Pinero, 594 F.Supp.2d at 710. *See also* Smith v. Trusted Univ. Standards in Electronics Transactions, Inc., 2010 WL 1799456 (D. N.J. May 04, 2010) (plaintiff's alleged reliance on certain online privacy policy provisions allegedly violated by his ISP could form the basis of a contract action, but the claim failed because the plaintiff did not plead any loss stemming from the alleged breach).

ScanScout, Inc., the court held that an online advertiser agreed to settle FTC charges that it deceptively claimed that consumers could opt out of receiving targeted ads by changing their browser settings to block cookies, when in fact, the advertiser used flash cookies that could not be blocked by browser settings.[32] The proposed settlement, among other things, bars misrepresentations about the company's data-collection practices, and requires that the advertiser provide a user-friendly mechanism to allow consumers to opt out of being tracked, including the use of a hyperlinked, embedded within or immediately next to its targeted display ads, to take consumers to a choice mechanism where consumers can opt out of receiving targeted ads.

A healthcare insurer agreed to pay a civil fine of $1,500,000 to settle certain HIPAA violations stemming from the theft of 57 unencrypted computer hard drives that contained the protected health information of over a million individuals in *In re Blue Cross Blue Shield of Tennessee*.[33] According to the HHS allegations, the insurer failed to implement appropriate administrative safeguards to adequately protect data servers remaining at an unused, leased facility by not performing the required security evaluations and implementing appropriate physical protections as required by the HIPAA Security Rule. Notably, this was the first enforcement action under the data breach rules mandated by the Health Information Technology for Economic and Clinical Health Act ("HITECH Act").

In *FTC v. Frostwire LLC*, a peer-to-peer file-sharing application developer settled FTC charges that its software likely would cause consumers to unwittingly expose sensitive personal files stored on their mobile devices.[34] According to the FTC complaint, the mobile file-sharing application was likely to cause consumers to unwittingly disclose personal files stored on their smartphones and tablet computers because the application's default settings were configured such that immediately upon installation and set-up, it would publicly share users' files stored on those devices. Among other things, the settlement bars the developer from using default settings that share consumers' files and requires clear and prominent disclosures about file sharing and how to disable it.

A retailer agreed to settle FTC charges that it failed to disclose adequately the scope of consumers' personal information it collected via a downloadable software application in *In Re Sears Holdings Mgmt. Co.*[35] According to the FTC's administrative complaint, the retailer represented to consumers that the marketing software, which consumers agreed to download in exchange for a monetary payment, would track their "online browsing." The FTC charged that the software monitored consumers' online sessions to a greater degree than disclosed by the retailer and that the extent of the tracking was only recited in a lengthy user license agreement available to consumers at the end of the multi-step registration process. Under the final consent order, the retailer would stop collecting data from the consumers who downloaded the software and destroy all data previously

---

[32] ScanScout, Inc., 76 Fed. Reg. 71566 (proposed Nov. 18, 2011). *See also* United States v. Rental Research Services, Inc., No. 09-00524 (D. Minn. settlement announced Mar. 5, 2009) (consumer reporting agency that failed to properly screen prospective customers and, as a result, sold multiple credit reports to identity thieves, settled FTC charges that it violated the Fair Credit Reporting Act); In re Genica Corp., FTC File No. 082 3113 (settlement announcement Feb. 5, 2009) (online computer seller that collected sensitive information from consumers and allegedly failed to take basic security measures settled FTC charges); United States v. Central Florida Investments, Inc., No. 09-104 (M.D. Fla. Jan. 20, 2009) (company that called consumers whose phone numbers were on the Do Not Call Registry without consent or an "established business relationship" settled FTC charges that it violated the Do Not Call Registry provisions).

[33] In re Blue Cross Blue Shield of Tennessee (HHS Settlement announced Mar. 13, 2012).

[34] FTC v. Frostwire LLC, No. 11-23643 (S.D. Fla. Stipulated Final Order Oct. 12, 2011).

[35] In Re Sears Holdings Mgmt. Co., No. C-4264 (Decision and Order Aug. 31, 2009).

collected, as well as prominently disclose the types of data the software will monitor, record, or transmit in the future prior to installation and separate from any user license agreement.

In *In re CVS Caremark Corp.*, a national pharmacy agreed to settle FTC charges that it failed to take appropriate security measures to protect the sensitive financial and medical information when it disposed of pill bottles containing labels bearing sensitive personal information of its customers.[36] In a coordinated action by the HHS OCR, the pharmacy agreed to pay $2.25 million and to implement a robust correction action plan for safeguarding patient information during disposal.

B. *Computer Fraud and Abuse Act*

Among other things, the CFAA[37] prohibits accessing a computer and obtaining information "without authorization" or by "exceeding authorized access." The statute lists many different types of criminal "hacking" conduct punishable by fines or imprisonment. In relevant part, §1030(a)(2)(C) provides: "[Whoever] intentionally accesses a computer without authorization or exceeds authorized access and thereby obtains…information from any protected computer if the conduct involved an interstate or foreign communication…shall be punished," and in related statutory language, §1030(a)(4) prohibits similar behavior with an intent to defraud.

The court held in *United States v. Nosal* that under the criminal provisions of the CFAA, a departing employee who accessed his employer's databases to help start a competing business did not "exceed authorized access" of the computer system even if such use of the proprietary materials violated the employer's computer use policy.[38] The Ninth Circuit, sitting en banc, affirmed the lower court's dismissal of the criminal CFAA claim and rejected the Government's broad interpretation of the CFAA that would have "transform[ed] the CFAA from an anti-hacking statute into an expansive misappropriation statute." The court held that the language "exceeds authorized access" in the CFAA is limited to violations of restrictions on "access" to information, and not restrictions on its "use," that the statute targets "the unauthorized procurement or alteration of information, not its misuse or misappropriation." Clarifying the two-prongs of the CFAA's prohibitions, the court stated: "'[W]ithout authorization" would apply to *outside* hackers (individuals who have no authorized access to the computer at all) and 'exceeds authorized access' would apply to *inside* hackers (individuals whose initial access to a computer is authorized but who access unauthorized information or files)." Construing the criminal statutory language narrowly, the appeals court found that a broad interpretation of the CFAA would turn minor online dalliances by employees using company computers into federal crimes and that significant notice problems would arise if criminal liability turned on the vagaries of corporate computer use polices that are lengthy, opaque, subject to change and seldom read.

---

[36] In re CVS Caremark Corp., FTC File No. 072 3119 (settlement announced Feb. 18, 2009).

[37] 18 U.S.C. §1030 (2008).

[38] United States v. Nosal, 676 F.3d 854 (9th Cir. 2012). *See also* WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199 (4th Cir. 2012) (CFAA fails to provide a remedy for misappropriation of trade secrets or violation of a use policy where authorization has not been rescinded (citing *Nosal*); based on the ordinary meaning of "authorization," an employee is authorized to access a computer when his employer approves or sanctions his admission to that computer and acts "without authorization" when he gains admission to a computer without approval; similarly, an employee "exceeds authorized access" when he has approval to access a computer, but uses his access to obtain or alter information that falls outside the bounds of his approved access; neither of these definitions extends to the improper use of information validly accessed).

A misdemeanor violation under the 18 U.S.C. §§ 1030(a)(2)(C) and 1030(c)(2)(A) of the CFAA upon the conscious violation of a website's terms of service runs afoul of the void-for-vagueness doctrine, because of the absence of minimal guidelines to govern law enforcement and actual notice deficiencies, according to the decision reached in *United States v. Drew*.[39] The court granted the defendant's motion for a post-verdict acquittal and vacated her CFAA misdemeanor conviction. The court commented that the concept of accessing a computer "without authorization" usually involved a computer hacker, a disloyal employee accessing proprietary files, or an entity in breach of a contract. Within the breach of contract approach, the court determined that most judges, in the civil law context, have held that a conscious violation of a website's terms of service will render the access unauthorized and/or cause it to exceed authorization. It cannot be considered "a stretch of the law to hold that the owner of an Internet website has the right to establish the extent to (and the conditions under) which members of the public will be allowed access," according to the court. However, the court stated that individuals of "common intelligence" are arguably not on notice that a breach of a terms of service contract can become a crime under the CFAA. Notably, the court reasoned that if a website's terms of service controls what is "authorized" and what is "exceeding authorization" – which in turn governs whether an individual's conduct is criminal or not – the statute would be unacceptably vague because "it is unclear whether any or all violations of terms of service will render the access unauthorized, or whether only certain ones will."

Although principally a criminal statute, the CFAA also provides for a private civil right of action, allowing for awards of damages and injunctive relief in favor of any person who suffers a loss due to a violation of the act. Although the CFAA was enacted almost 25 years ago, courts continue to decide how the statute applies to new factual scenarios in a rapidly and ever-changing computerized world.

According to the Northern District of Illinois in *Cassetica Software, Inc. v. Computer Sciences Corp.*, the unauthorized downloading of software from a computer system after a licensing agreement had expired does not satisfy the "damage" element under the CFAA, because the statute only recognizes damage when the violation causes a diminution in the completeness or usability of the data on a computer system.[40] The court found that the plaintiff failed to allege that the defendant's downloads resulted in lost data, the inability to offer downloads to its customers, or that the downloads affected the availability of the software. The court also found that the plaintiff's allegations of "loss" were not cognizable because they were costs that were not related to the impairment or damage to a computer or computer system.

---

[39] United States v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009). *See also* United States v. Aleynikov, 737 F.Supp.2d 173 (S.D.N.Y. 2010) (government's argument that defendant, who was authorized to access his employer's trading system source code, violated the criminal provisions of the CFAA by misappropriating the source code was rejected), *reversed by*, United Stated v. Aleynikov 676 F.3d 71 (2nd Cir. 2012) (conviction under federal EEA overturned because, among other things, the wrongful uploading of his employer's proprietary source code did not implicate a system that was "produced for" or "placed in" interstate or foreign commerce). *See generally* United States v. Zhang, 2012 WL 1932843 (N.D. Cal. May 29, 2012) (applying the Ninth Circuit's holding in *Nosal*, departing employee who misappropriated confidential information in violation of nondisclosure agreement did not exceed authorized access and was not guilty of CFAA charges; defendant convicted for theft of trade secrets under federal law); Lee v. PMSI, Inc., 2011 WL 1742028 (M.D. Fla. May 6, 2011) (court rejects employer's CFAA claim against employee that allegedly engaged in excessive Internet usage and visited social network websites and personal webmail accounts, because, among other things, the employer failed to allege damage to its computer system; "both the letter and the spirit of the CFAA convey that the statute is not intended to cover an employee who uses the internet instead of working").

[40] Cassetica Software, Inc. v. Computer Sciences Corp., 2009 WL 1703015 (N.D. Ill. June 18, 2009).

In *State Analysis Inc. v. American Financial Services Assoc.*, the Eastern District of Virginia held that a company that accessed a password-protected proprietary database using the "shared" password of another entity could be liable for common law trespass and unauthorized access under the CFAA, while the entity that allowed the company to use its old password may be liable for trafficking in passwords under the CFAA, but not unauthorized access.[41]

The Sixth Circuit in *Pulte Homes Inc. v. Laborers International Union of North America* held that a company that suffered impairment to its systems and networks due to a union's intentional campaign to bombard the company with emails and voicemails may proceed with CFAA transmission claims, which, in part, concern knowingly causing the transmission of information that causes damage without authorization to a computer.[42] The appeals court reversed the lower court's dismissal of the plaintiff's CFAA transmission claim, finding that the email campaign prevented the plaintiff's employees from accessing or sending some emails and voicemails, which could be deemed "damage" under the statute. The court, however, affirmed the dismissal of the plaintiff's CFAA unauthorized access claims because the union's calls and emails did not enter the plaintiff's networks "without authorization" since the company used unprotected public communications systems.

Most notably, the CFAA has been used increasingly in civil suits by employers to sue former employees and their new companies for misappropriation of information from the employer's computer system, beyond the standard state causes of action for trade secret misappropriation and breach of contract. A civil cause of action under the CFAA frequently is pleaded in cases where an employer is suing a former employee for misappropriation of trade secrets or proprietary information, where the misappropriation involved some kind of access to or use of the employer's computer network. However, federal courts disagree in interpreting the term "unauthorized access." Under an expansive view, courts have found that an employee's access was unauthorized after she engaged in conduct, which could constitute a breach of her duty of loyalty to the company. Taking a narrower reading of the statute, many courts have found that a departing employee, who copied proprietary files while still having full access to his employer's protected computer databases, did not access information "without authorization" or otherwise "exceed authorized access" under the CFAA.[43]

A departing employee who emailed certain company documents to his own personal computer before departure did not access the computers "without authorization" or in excess of "authorized access" as required under the CFAA to establish a violation, according to the decision in *LVRC Holdings, LLC v. Brekka*.[44] The Ninth Circuit affirmed the dismissal of the CFAA claims against the

---

[41] State Analysis Inc. v. American Financial Services Assoc., 621 F. Supp. 2d 309 (E.D. Va. 2009). *See also* AtPac Inc. v. Aptitude Solutions Inc., 2010, 730 F.Supp.2d 1174 (E.D.Cal. 2010) (third parties are not always liable under the CFAA for exploiting a licensee's violation of its license agreement; rather, such liability is perhaps best applied in situations where the third-party defendant uses subterfuge—like using user names and passwords that do not belong to it—to gain access to a licensor's protected materials on the licensor's own website, computers, or servers).

[42] Pulte Homes Inc. v. Laborers Int'l Union of North America, 648 F.3d 295 (6th Cir. 2011).

[43] *See also* Flynn v. Liner Grode Stein Yankelevitz Sunshine Regenstreif & Taylor LLP, 2011 WL 2847712 (D. Nev. July 15, 2011) (no aiding and abetting civil liability does not exist under §1030).

[44] LVRC Holdings, LLC v Brekka, 581 F.3d 1127 (9th Cir. 2009). *See also* ReMedPar Inc. v. AllParts Medical LLC, 683 F. Supp. 2d 605 (M.D. Tenn. 2010) (CFAA does not extend to situations where the employee's access was technically authorized but the particular use of the information was not; also, the employer's "loss" at issue (i.e., the misappropriation of trade secret information) as well as the costs incurred by the employer in its efforts to seek redress for those acts and retain new employees are not the type of losses covered by the statute because they are unrelated to any interruption in computer service); Lewis-Burke

ex-employee. The court found that a person uses a computer "without authorization" when the person has not received permission to use the computer for any purpose (e.g., a hacker) or when the employer has rescinded permission to access the computer and the employee thereafter accesses the company network. In this case, the court concluded that the employee's use of the company computers to email documents did not violate the CFAA, because he was authorized to access the company computers during his employment. The court reasoned that there was no language in the CFAA that supported the proposition that authorization to use a computer ceases when an employee resolves to use the computer contrary to the employer's interest. The court declined to follow the Seventh Circuit decision, *International Airport Centers, LLC v. Citrin*,[45] which held that an employee acts without authorization under the CFAA when he obtains company information for an improper purpose.

In *TelQuest Int'l Corp. v. Dedicated Business Systems, Inc.*, the District of New Jersey held that departing employees who allegedly violated a non-competition employment agreement and used private customer information to initiate their own business did not violate the CFAA because the employer failed to allege facts that the damage or loss it incurred was related to investigating or remedying damage to its computer system.[46] The court dismissed the employer's CFAA claims. The court found that the employer allegations regarding losses related to hiring a computer expert failed to provide the type of investigation or description of how its computer system was interrupted,

---

Assocs. LLC v. Widder, 2010 WL 2926161 (D.D.C. July 28, 2010) (following *Brekka*, an employer's decision to allow or terminate an employee's authorization is the determining factor as to whether the employee acted with or without authorization; whether defendant had permission to copy documents onto a thumb drive or to subsequently use the data after he had left the plaintiff's employ, is not a question that relates to his liability under the CFAA); Orbit One Communications, Inc. v. Numerex Corp., 692 F. Supp. 2d 373 (S.D.N.Y. 2010) (departing employees had unfettered access to employer's computers prior to leaving the company and thus plaintiff-employer failed to advance any evidence that the departing employees accessed the plaintiff's computer system without authorization or exceeded their authorized access in violation of the CFAA); Oce North America Inc. v. MCS Services Inc., 2010 WL 3703277 (D. Md. Sept. 16, 2010) (ex-employee who allegedly copied printer diagnostic software from his ex-employer and used it during his work for a competitor did not access the software "without authorization" under the CFAA; CFAA claims against the employee's new employer were also dismissed because the plaintiff did not allege that the defendant accessed any "protected computer" without authorization or in excess of that authorization to obtain the plaintiff's software); Sebrite Agency, Inc. v. Platt, 884 F.Supp.2d 912 (D. Minn. 2012) (misuse or misappropriation of confidential information stored on a employer's computer to which the defendant had authority to access does not give rise to liability).

[45] Int'l Airport Centers, LLC v. Citrin, 440 F.3d 418 (7th Cir. 2006).

[46] TelQuest Int'l Corp. v. Dedicated Business Systems, Inc., 2009 WL 3234226 (D. N.J. Sept. 30, 2009). *See also* Mintel Int'l Group Ltd. v. Neergheen, 636 F.Supp.2d 677 (N.D.Ill. 2009) (departing employee's act of copying and emailing electronic files from his employer's computer database is not enough to satisfy the damage requirement of the CFAA; fees paid to expert to assess the ex-employee's improper actions are not "losses" under the CFAA because an alleged "loss" must relate to the investigation or repair of a computer or computer system following a violation that caused impairment or unavailability of data or interruption of service); Catapult Communications Corp. v. Foster, 165 F.3d 747 (9th Cir. 1999) (alleged losses in the form of expenses incurred from conducting forensic analysis on defendant's computer are not compensable losses under the CFAA, without any evidence that plaintiffs' computers were damaged by defendant's alleged unauthorized access); M-I LLC v. Stelly, 2010 WL 733 F.Supp.2d 759 (S.D.Tex. 2010) (employer allegations of damages "to its business in the form of lost profits, loss of customers and loss of future business opportunities" caused by departing employees cannot form a cognizable CFAA claim; "[the plaintiff] asserts no damages whatsoever relating to their investigation of computer damage, or costs incurred because any computer service was interrupted"); General Scientific Corp. v. Sheervision, Inc., 2011 WL 3880489 (E.D. Mich. Sept. 2, 2011) (losses under the CFAA are limited to costs incurred and profits lost as a direct result of interrupted computer service; the CFAA's damage requirement is not concerned with sales lost through the use of the information accessed); Schatzki v. Weiser Capital Management LLC, 2012 WL 2568973 (S.D.N.Y. July 3, 2012) (plaintiffs' claim inadequate to meet the definition of damages and losses under the CFAA; the complaint does not allege that the defendant, a former business partner, destroyed or impaired the plaintiff's proprietary data, nor does it make any specific allegation as to the cost of identifying, securing or remedying the alleged damage caused by the defendant's access).

damaged, or restored. The court also commented that gathering evidence from a computer to prove state law employment claims does not turn employee conduct–even allegedly disloyal conduct in breach of contract–into the kind of conduct that violates the CFAA.

As discussed in *Vurv Technology LLC v. Kenexa Corp.*, departing employees who were authorized to access the information they copied from a company laptop, but allegedly did so for a wrongful purpose, did not access their employer's computers "without authorization" as required under the CFAA to establish a violation, notwithstanding the existence of a employment confidentiality agreement.[47] However, the court found that the employer may proceed with CFAA claims relating to the copying of proprietary information after the defendants left the employment of the plaintiff.

The costs that would be incurred by examining other parties' computers – computers onto which the defendant allegedly copied material taken from the plaintiff's thumb drive – and permanently deleting any such material found are not cognizable losses under the CFAA that can satisfy the jurisdictional threshold, according to the decision reached in *Doyle v. Taylor*.[48] The court granted the defendant's motion for summary judgment on the CFAA claim and declined to exercise supplemental jurisdiction on the related state claims. The court found that while the act of accessing another's thumb drive without authorization may fall within the scope of the CFAA, there was no basis in the record to find that the thumb drive was impaired or that the plaintiff will incur any costs associated with restoring any interruption of service. The court noted that the CFAA's definitions of

[47] Vurv Technology LLC v. Kenexa Corp., 2009 WL 2171042 (N.D. Ga. July 20, 2009). *See also* Mortgage Now Inc. v. Stone, 2009 WL 4262877 (M.D. Fla. Nov. 24, 2009) (departing employees who allegedly stole proprietary information from their employer's computers and "scrubbed" their computers' hard drives to conceal their activity did not violate the CFAA because a party who is permitted to view proprietary information does not act "without authorization" when he accesses it); Clarity Services Inc. v. Barney, 698 F.Supp.2d 1309 (M.D.Fla. 2010) (departing employee that checked email and reformatted laptop after resigning neither accessed the employer's computers "without authorization" nor "exceeded his authorized access"); American Family Mut. Ins. Co. v. Hollander, 2009 WL 535990 (N.D. Iowa Mar. 3, 2009) (departing employee that reviewed his employer's client lists before departure did not access the computers "without authorization" or in excess of "authorized access" as required under the CFAA to establish a violation); Envtl. Safety Consultants, Inc. v. Allied Safety Consultants Inc., 95 Fed.Cl. 77 (2010) (company's allegations that it suffered damages as a result of an ex-employee's misappropriation of proprietary information were insufficient to state a claim under the CFAA where the company failed to plead any interruption of computer service; lost revenue was only recoverable if it was incurred because of an "interruption in service"). *But see* Musket Corp. v. Star Fuel of Oklahoma LLC, 2012 WL 3595048 (W.D. Okla. Aug. 21, 2012) (departing employee that downloaded shareware against company policy and then used it to copy proprietary files for use with his new position at a competitor contrary to a non-disclosure agreement may have exceeded authorized access" under the CFAA); *see also* Deloitte & Touche LLP v. Carlson, 2011 WL 2923865 (N.D. Ill. July 18, 2011) (CFAA claims may proceed against departing employee who destroyed and replaced hard drive before returning company-issued laptop to allegedly cover his tracks in wrongfully soliciting a competitor in violation of employee agreement); LKQ Corp. v. Thrasher, 785 F.Supp.2d 737 (N.D. Ill. 2011) (no allegation that the employer specifically restricted its employees is necessary to state a CFAA claim against a departing employee who wiped his company laptop before returning it; the employer's allegation of a breach of duty is enough to allege a lack of authorization); Lasco Foods Inc. v. Hall, 600 F.Supp.2d 1045 (E.D.Mo. 2009) (while a departing employee ordinarily may have been authorized to access the information appropriated from his employer, that authorization was terminated when the defendant destroyed the agency relationship by accessing and appropriating the protected information for his own personal gain and contrary to the interest of the employer).

[48] Doyle v. Taylor, 2010 WL 2163521 (E.D. Wash. May 24, 2010). *See also* Intl. Chauffeured Services, Inc. v. Fast Operating Corp., 2012 WL 1279825 (S.D.N.Y. Apr. 16, 2012) (expenses for monitoring network for future unauthorized activity not a "loss" under the CFAA; "loss" only encompasses costs to repair and costs associated with investigating the damage). *But see* Navistar, Inc. v. New Baltimore Garage, Inc., 2012 WL 4338816 (N.D. Ill. Sept. 20, 2012) (plaintiff can satisfy the requirements of loss under the CFAA by alleging costs reasonably incurred to respond to an alleged CFAA offense, even if the offense turned out not to have caused damage to the computer system; using a password to access a copyrighted work, even without authorization, does not constitute circumvention under the DMCA because it does not involve descrambling, decrypting, or otherwise bypassing a technological measure).

"damages" and "loss" should be strictly construed and that the plaintiff must identify impairment of or damage to the computer system that was accessed without authorization.

In *Ervin & Smith Adver. & Public Relations, Inc. v. Ervin*, the court held departing employees who, against company policy, emailed themselves proprietary data may be liable under CFAA as per the Seventh Circuit's decision in *International Airport Centers LLC v. Citrin*.[49] The court stated that while the defendants ordinarily may have been authorized to access the information they appropriated from the plaintiff, such authorization was terminated when the defendants destroyed the agency relationship by accessing and appropriating the protected information for their own personal gain and against the interest of their employer.

Most CFAA claims were dismissed against ex-employees who had initial access to proprietary information that was allegedly copied from employer's computer system in *US Bioservices Corp. v. Lugo*. However, the court allowed the plaintiff to proceed on those claims that were based upon violations for exceeding authorized access when defendants allegedly accesses certain information to which they were not entitled.[50]

Beyond federal law, a majority of states have enacted computer trespass and fraud statutes that allow claims for various degrees of unauthorized access and copying, schemes to defraud, and the unlawful destruction of proprietary data.

The District of Nebraska held in *Joseph Oat Holdings Inc. v. RCM Digesters Inc.* that an entity who secretly accessed the servers of its former business partner, copied proprietary files and changed administrative passwords following the dissolution of the parties' joint venture violated California and New Jersey state computer trespass laws.[51] The court granted summary judgment on defendant's computer trespass counterclaims, holding that at the time the plaintiff accessed the defendant's computer server (which had formerly been used by the joint venture), the server had reverted back to the property of the defendant because the joint venture had been officially defunct. The court rejected the plaintiff's argument that it copied the defendant's files to preserve evidence pursuant to a litigation hold letter, finding that an adversary's counsel's letter regarding the duty to preserve evidence does not "afford a party carte blanche authority" to secretively copy computer files located on the adversary's computer server, even if many of those files on the server had once been property of that party, and even if that party still had access to those files.

C. *Commercial Email and Spam*

The CAN-SPAM Act,[52] which imposes requirements on those who send commercial email messages to consumers and establishes civil and criminal penalties for the transmission of unsolicited commercial electronic mail, or spam, that does not comport with the Act's requirements, continues to garner the public's attention as spam remains a stubborn problem. Essentially, the CAN-SPAM Act protects consumers by offering them a legal right to "opt out" of future spam. In most situations, it is not required that a business get permission from a potential recipient before sending commercial

[49] Ervin & Smith Adver. & Public Relations, Inc. v. Ervin, 2009 WL 249998 (D. Neb. Feb. 3, 2009).

[50] US Bioservices Corp. v. Lugo, 595 F.Supp.2d 1189 (D. Kan. Jan. 21, 2009).

[51] Joseph Oat Holdings Inc. v. RCM Digesters, Inc., 665 F. Supp. 2d 448 (D.NJ 2009).

[52] 15 U.S.C. §7701.

email. Still, businesses are not permitted to send commercial emails to those who request to be removed from the businesses' lists.

Notably, the Act expressly preempts all state laws to the extent that they address the permissibility of unsolicited commercial email, except for those that apply "falsity or deception in any portion of a commercial electronic mail message or information attached thereto." Courts have wrestled with the question of what constitutes falsity or deception under the statute, whether cognizable state claims must be based on the traditional tort theory of common law fraud and deceit, which usually requires a plaintiff to plead it with particularity, or whether state consumer or anti-spam laws may survive preemption for regulating something less than fraud. District courts to have addressed the issue have reached differing results.

The CAN-SPAM Act applies to social networking communications—including internal messages to users' walls, "news feeds," the "home" page of users' friends, and the Facebook inbox of users' friends—despite the fact that such electronic messages are not delivered to a traditional email "inbox."[53] In *Facebook, Inc. v. Maxbounty, Inc.*, the court refused to dismiss the plaintiff's CAN-SPAM claims against an Internet marketer that had allegedly set up fraudulent fan pages through its affiliates to draw traffic to outside websites and advertisers through a series of messages and notifications to Facebook users. The court rejected the defendant's argument that an "electronic mail message" under the CAN-SPAM Act must be capable of characterization as "email" or must be directed to a traditional email inbox or address with a local part and domain part (i.e., user@domain.com).

A provider of free email accounts for a small number of individuals who took no steps to stem the flow of spam emails does not have standing to pursue claims under the CAN-SPAM Act as a result of unsolicited commercial email sent to its users, according to *Gordon v. Virtumundo, Inc.*.[54] The Ninth Circuit affirmed the lower court's grant of summary judgment to the defendant and also ruled that the plaintiff's state anti-spam claims were preempted by the CAN-SPAM Act. The court held that the plaintiff was not a "provider of an Internet access service" who was adversely affected by a statutory violation, and thus, did not have private standing to bring CAN-SPAM Act claims. While the court recognized that statutory standing was not limited to traditional ISPs (and included providers such as social network websites), the court rejected any overly broad interpretation of "Internet access service" (IAS) that would include an entity that merely provided email accounts and email access. The court commented that the plaintiff neither had physical control over nor access to the hardware at issue, which was owned by another provider, and was "troubled" by the extent to which the plaintiff failed to operate as a "*bona fide* email provider," such that the plaintiff purposefully avoided taking even minimal efforts to avoid or block spam messages and accumulated

---

[53] Facebook, Inc. v. Maxbounty, Inc., 274 F.R.D. 279 (N.D. Cal. 2011).

[54] Gordon v. Virtumundo, Inc., 575 F.3d 1040 (9th Cir. 2009). *See also* Asis Internet Servs. v. Azoogle.com, Inc., 357 Fed.Appx. 112 (9th Cir. 2009) (mere cost of ordinary filtering and carrying spam over plaintiff's facilities does not constitute a harm as required by the CAN-SPAM Act; plaintiff did not suffered a harm within the meaning of the statute and lacked standing.), *further proceedings at* Asis Internet Servs. v. Optin Global, Inc., 2010 WL 2035327 (N.D. Cal. May 19, 2010) (defendant awarded attorney's fees in the amount of $806,978.84); Asis Internet Services v. Active Response Group, 2010 WL 519830 (N.D. Cal. Feb. 9, 2010) (following *Virtumundo* and *Azoogle* in dismissing the plaintiff's action for lack of standing because the mere cost of carrying spam emails over plaintiff's facilities does not constitute a harm under the CAN-SPAM Act); RJ Prod. Co. v. Nestle USA, Inc., 2010 WL 1506914 (D.D.C. Apr. 15, 2010) (digital media outsourcing and consulting firm that made no allegations that it was an Internet access service that suffered any network harms lacked standing under the CAN-SPAM Act); Melaleuca Inc. v. Hansen, No 07-212 (D. Idaho Sept. 30, 2010) (marketing company that possessed a domain name and also offered email services through a third party was not a bona fide ISP under the CAN-SPAM Act and lacked standing to pursue a claim).

spam through a variety of means for the purpose of facilitating litigation. As to the "adversely affected" standing requirement, the court stated that the fact that the plaintiff received a large volume of commercial email was not enough to establish his statutory standing. Rather, the court found that a plaintiff must plead those types of harms uniquely encountered by IAS providers, that is, network crashes, higher bandwidth utilization, and increased costs for hardware and software upgrades, network expansion and additional personnel, such that, in most cases, "evidence of some combination of operational or technical impairments and related financial costs attributable to unwanted commercial email would suffice." Interestingly, the appeals court noted that trial courts must take a closer look at services that may not be *bona fide* providers and "be careful to distinguish the ordinary costs and burdens associated with operating an Internet access service from actual harm," and that courts should also expect a legitimate service provider to "secure adequate bandwidth and storage capacity and take reasonable precautions, such as implementing spam filters, as part of its normal operations."

In *Ferguson v. Active Response Group*, the Ninth Circuit held that an Internet access service provider that offers free email forwarding services lacks standing under the CAN-SPAM Act because he was not "adversely affected" by incoming spam when he was forced to switch to a broadband connection.[55] The appeals court affirmed the district court's grant of summary judgment to the defendant online marketing company because the plaintiff failed to prove more than negligible harm due to the spam, such as increased costs for server maintenance, network harm, or for customer service personnel to handle complaints.

Claims under California's deceptive email advertising law are not preempted by the CAN-SPAM Act.[56] Regarding CAN-SPAM Act preemption of state laws, the *Asis Internet Services v. Consumerbargaingiveaways LLC* court ruled that "falsity or deception" was not limited just to common-law fraud and other similar torts such that anti-deception state actions not insisting on every element of common-law fraud are not preempted.

---

[55] Ferguson v. Active Response Group, 348 Fed. Appx. 255 (9th Cir. 2009). *See also* Haselton v. Quicken Loans Inc., 2010 WL 1180353 (W.D. Wash. Mar. 23, 2010) (website host that attempted to grow a spam business and did not use any e-mail filtering programs was not bona fide IAS provider and accordingly lacked standing to pursue a claim under the CAN-SPAM Act; in addition, the plaintiff did not show it was "adversely affected" by any alleged violation of the CAN-SPAM Act since it suffered harm, if at all, by its own failure to implement spam reducing measures and its actions to actively seek out such communications).

[56] Asis Internet Services v. Consumerbargaingiveaways LLC, 622 F. Supp. 2d 935 (N.D. Cal. 2009). *See also* Hypertouch, Inc. v. Valueclick, Inc., 191 Cal.App.4th 1209 (Cal. App. 2011) (CAN-SPAM Act's savings clause applies to any state law that prohibits material falsity or material deception in a commercial e-mail regardless of whether such laws require plaintiff to prove and plead each and every element of common law fraud; moreover, the application of California's spam statute is not limited to entities that "send" the offending e-mails nor does it require a plaintiff to establish that defendant had knowledge of such e-mails); Hoang v. Reunion.com, No. 08-03518 (N.D. Cal. Mar. 31, 2010); Asis Internet Services v. Subscriberbase Inc., 2009 WL 4723338 (N.D. Cal. Dec. 4, 2009); Asis Internet Services v. Member Source Media, LLC, No. 08-1321 (N.D. Cal. Apr. 20, 2010) (state anti-spam law claims based upon header deficiencies preempted by CAN-SPAM Act; claims based upon deceptive subject lines not preempted); Ferron v. SubscriberBase Holdings, Inc., 2009 WL 650731 (S.D. Ohio Mar. 11, 2009) (claims stemming from allegedly deceptive commercial email solicitation brought under state consumer protection statute are not preempted by the CAN-SPAM Act). *But see* Hypertouch, Inc. v. Azoogle.com, Inc., 2010 WL 2712217 (9th Cir. July 09, 2010) (unpublished) (claims under California anti-spam law for commercial email advertisements that contained "falsified," "misrepresented," "forged," or misleading information must comply with the Federal Rules of Civil Procedure's heightened pleading standards for fraud).

It is not a violation of Section 17519.5(a)(2) of the California anti-spam law, which prohibits "falsified or forged header information," to send commercial email advertisements from multiple, accurately-registered domain names for the purpose of bypassing spam filters.[57]

The disclosure of an email address that resulted in the receipt of spam, but no other misuse, is not sufficient to constitute damage to the plaintiff or sustain breach of contract and fiduciary claims.[58]

D. *Telephone Consumer Protection Act*

The Telephone Consumer Protection Act (TCPA) was originally adopted in 1991 to, among other things, protect the privacy of citizens by restricting the use of telephones for unsolicited advertising and, more specifically, curb telemarketers from using autodialers to make millions of unsolicited calls to residential and business telephone numbers, fax machines and cellular telephones. The TCPA also prohibits the use of any fax machine, computer, or other device to send unsolicited fax advertisements, absent certain consent requirements.

According to *Satterfield v. Simon & Schuster,* the transmission of an SMS text message to a cellular telephone is a "call" within the meaning of the TCPA.[59] The Ninth Circuit reversed the district court's grant of summary judgment to the defendant and remanded the case to determine if the text message at issue was sent using an "automatic telephone dialing system" as required under the statute, that is, whether the equipment used for transmission had the "capacity" to both (1) store or produce numbers to be called using a random or sequential number generator and (2) to dial such numbers. The court found that the TCPA's prohibition on certain automated calls to wireless numbers encompasses both voice calls and SMS text messages, deferring to the FCC's regulations and interpretation of the Act and the plain meaning of the term "call." The court reasoned that the purpose and history of the TCPA indicated that Congress was trying to prohibit the use of automatic dialers to communicate with others by telephone in an invasive manner, and that a voice message or a text message were not distinguishable in terms of being an invasion of privacy. The court further held that while the TCPA exempts those calls "made with the prior express consent of the called party," no express consent was given in this case because the plaintiff's consent to receive promotional material from a third-party marketer and its "affiliates and brands," cannot be read as consenting to the receipt of the commercial messages of the defendant, an unrelated entity.

The court in *Abbas v. Selling Source, LLC* held that an unsolicited, commercial SMS message is a "call" within the meaning of the TCPA because Congress intended to restrict unsolicited, automated advertisements and solicitations by telephonic means, which includes text messages.[60]

---

[57] Kleffman v. Vonage Holdings Corp., 49 Cal.4th 334 (2010).

[58] Cherny v. Emigrant Bank, 604 F.Supp.2d 605 (S.D.N.Y. 2009).

[59] Satterfield v. Simon & Schuster, 569 F.3d 946 (9th Cir. 2009). *See also In re* Jiffy Lube Intl., 847 F.Supp.2d 1253 (N.D. Cal. 2012) (advertiser not permitted to avoid TCPA liability merely because it hired a different firm to send text message advertisements to its customers). *But see* Thomas v. Taco Bell Corp., 879 F.Supp.2d 1079 (C.D. Cal. 2012) (a party can be held liable under the TCPA directly if it personally "makes" a call in the method proscribed by the statute, or vicariously, such as, if it was in an agency relationship with the party that sent the text message; plaintiff failed to present any evidence that defendant directed or supervised the manner and means of the text message campaign conducted by an association of its franchisees).

[60] Abbas v. Selling Source, LLC, 2009 WL 4884471 (N.D. Ill. Dec. 14, 2009). *See also* Lozano v. Twentieth Century Fox Film Corp., 702 F. Supp.2d 999 (N.D. Ill. 2010) (promotional text message sent to plaintiff constitutes a "call" for the purposes of the TCPA; the plain language of the TCPA does not require plaintiff to allege that he was charged for receipt of the text message that forms the basis for his complaint). *But see* Ibey v. Taco Bell Corp., 2012 WL 2401972 (S.D. Cal. June 18, 2012) (advertiser's

The court denied the defendant's motion to dismiss the defendant's TCPA claims. The court rejected the defendant's argument that the TCPA was inapplicable because there was no evidence that the plaintiff was "charged for the call," concluding that beyond "cost-shifting" concerns, Congress was just as concerned with consumers' privacy rights and the nuisances of telemarketing such that a cellular phone customer need not necessarily be charged for the call to make that call actionable.

The New York Court of Appeals held in *Stern v. Bluestone* that unsolicited, faxed "commentaries containing short essays on legal topics in an attorney's field of practice that also list the sending attorney's law firm name and contact information fit the FCC's framework for an "informational message." and are not unlawful "unsolicited advertisements" under the TCPA.[61] The Court of Appeals reversed the lower court's grant of summary judgment to the plaintiff on his TCPA claims. The court found that the defendant's commentaries, which provided academic legal information, did not promote a commercial product and to the extent that the defendant devised the commentaries as a way to advertise his expertise to other attorneys and gain referrals, the faxes contained at most, "[a]n incidental advertisement of his services, which [did] not convert the entire communication into an advertisement."

Certain regulatory violations of the TCPA fall outside the scope of private enforcement actions.[62] The New York court concluded that there was no private right of action for failure on the part of an automated telemarketing call to identify itself or provide its phone number since the enforcement of such identification requirements was within the province of state attorneys general and the FCC, and could not form the basis of a private enforcement action.

E. *First Amendment Issues in Digital Content*

The First Amendment's freedom of speech and the press provide protection for certain uses of content on the Internet or in a digital application and can limit rights of publicity in one's name or likeness for newsworthy and other purposes. Moreover, in certain instances, students and public employees can be subject to restrictions in the name of school discipline and the objectives of a public employer.

---

single, confirmatory text message in response to an opt-out request from plaintiff, who voluntarily had provided his phone number by sending the initial text message, does not violate the TCPA).

[61] Stern v. Bluestone, 12 N.Y.2d 873 (2009). *See also* Holmes v. Back Doctors, Ltd, 2009 WL 3425961 (S.D. Ill. Oct. 21, 2009) (faxed newsletter that contained bona fide medical information that changed each month and was sent to specific recipients on a regular schedule does not constitute an "advertisement" under the TCPA; while the faxes contained some advertising material, "it is worth noting that the TCPA actually requires the sender of a fax to include its contact information in the fax…and the Court sees no reason why [defendant's] compliance with the statute should become…the linchpin for finding that [defendant's] faxes constitute advertising"); Holtzman v. Turza, 2010 WL 3076258 (N.D. Ill. Aug. 3, 2010) (faxed newsletters that contained editorial and promotional content that were ghostwritten and transmitted on attorney's behalf as part of a paid marketing campaign were deemed unsolicited advertisements under the TCPA), *further proceedings at* Holtzman v. Turza, 2011 WL 3876943 (N.D. Ill. Aug. 29, 2011) (plaintiff granted summary judgment, with the court awarding $4,215,000 in damages, $500 in statutory damages for each of the 8,430 times faxes successfully sent to the class members).

[62] Burdge v. Ass'n Health Care Mgmt., 2009 WL 414595 (S.D. Ohio Feb. 18, 2009). *See also* Dobbin v. Wells Fargo Auto Finance, Inc., 10-268 (N.D. Ill. June 14, 2011) (recipients of cell phone calls failed to establish a genuine issue of fact regarding whether manually dialed calls made from a bank call center desk phone were made "using" equipment with the capacity to autodial within the meaning of the TCPA since such desk phones could be used independently of the predictive dialing technology employed by the bank); CE Design, Ltd. v. Prism Bus. Media, Inc., 606 F.3d 443 (7th Cir. 2010)) (the "established business relationship exception" to the TCPA's junk fax prohibitions applies to both business and residential customers).

According to *FreeLife Int'l Inc. v. American Educational Music Publications, Inc.*, a non-disparagement clause contained in an online adhesion contract between a direct sales company and a prospective independent distributor is enforceable because it is neither procedurally nor substantively unconscionable and does not violate the First Amendment.[63] In ruling on the enforceability of the online contract's non-disparagement clause, the court found that the defendant completed the application and stated affirmatively that he accepted the terms and that the non-disparagement clause was not objectively bizarre or oppressive such that the adhering party "would not have assented to the particular term had he or she known of its presence." The court commented that the defendant accepted the contract with the non-disparagement clause, and after that he allegedly had breached it, cannot be heard to claim it is unfair because of the possible consequences of his breach. The court also rejected the defendant's First Amendment argument, stating that the First Amendment protects individuals from government infringement on speech, not private infringement.

The Northern District of California in *Estavillo v. Sony Computer Entertainment* held that a user that was banned from the defendant's videogame network after multiple violations of its terms of use cannot state a plausible First Amendment claim for relief, because the defendant was merely providing a private commercial product and did not have a sufficient structural or functional nexus to the government for the First Amendment to apply.[64]

In *Richerson v. Beckon*, the transfer of an education instructional coach to another position after it was discovered that she wrote a publicly-available blog that included several highly personal and vituperative comments about her employers and fellow teachers did not violate the instructional coach's First Amendment rights.[65] The court found that the legitimate administrative interests of the school district outweighed the plaintiff's First Amendment interests in not being transferred because of her speech, despite the fact that it arguably touched on matters of public concern.

A state administrative hearing officer's termination due to her personal blog that addressed the same special education topics that she heard in her judicial capacity called did not violate her First Amendment or other civil rights in *Stengle v. Office of Dispute Resolution*.[66] The court granted the government agency's motion for summary judgment on the plaintiff's constitutional and civil rights claims, finding that her blog posed a legitimate threat to the efficient operation of the government

---

[63] FreeLife Int'l Inc. v. Am. Educ. Music Publ'ns, Inc., 2009 WL 3241795 (D. Ariz. Oct. 1, 2009).

[64] Estavillo v. Sony Computer Entm't, 2009 WL 3072887 (N.D. Cal., Sept. 22, 2009). *See also* Stern v. Sony Corp., No. 09-7710 (C.D. Cal. Feb. 8, 2010) ("To the extent Plaintiff is suing Sony as a manufacturer of video games, and the provider of online services, Sony is not a 'place of public accommodation' and is therefore not liable for violating Title III of the ADA").

[65] Richerson v. Beckon, 337 Fed.Appx. 637 (9th Cir. 2009). *See also* Yoder v. Univ. of Louisville, 2012 WL 1078819 (W.D. Ky. Mar. 30, 2012) (nursing school that expelled student for making social media posting about a patient's birth did not violate her First Amendment rights; the school had a legitimate pedagogical purpose in requiring students to sign a confidentiality policy and the student "cannot now complain that she had a First Amendment right to publish on the internet the information she agreed not to reveal").

[66] Stengle v. Office of Dispute Resolution, 631 F.Supp.2d 564 (M.D. Pa. 2009). *See also* Zellner v. Herrick, 639 F.3d 371 (7th Cir. 2011) (teacher dismissal for violating computer use policy against viewing adult materials was warranted and unrelated to his outside union activities). *But see* Love v. Rehfus, 946 N.E.2d 1 (Ind. 2011) (firefighter was improperly terminated for sending a private email supporting a local political candidate to a small group of citizens because the email was constitutionally protected speech and there was little evidence suggesting the speech caused or had the potential to cause disruption or harm to the Fire Department's operations); Rubino v. City of New York, 950 N.Y.S.2d (2012) (public school teacher's termination for tasteless Facebook posting about her students was not warranted where the petitioner had a long and otherwise unblemished employment history).

agency such that the plaintiff's free speech rights as a government officer could be constitutionally abridged in these circumstances. A California state court stated that the plaintiff failed to show that her blogging activities had no potential to disrupt the governmental operations, particularly since her blog had the potential to induce recusal motions from those who came before her in her hearing officer capacity and encourage losing parties to question her impartiality following an adverse decision.

A school's transfer and discipline of student who created a slide show that was later posted on YouTube that depicted violence against a teacher was likely justified.[67] The court reasoned that even if the student's posting was protected speech, it was reasonable, given the violent language and unusual photos depicted in the video slide show, for school officials to forecast substantial disruption of school activities.

IV. JURISDICTION AND PROCEDURE

As plaintiffs increasingly have urged courts to exercise jurisdiction over non-resident parties based on their Web presence, two lines of analysis have arisen in the judicial opinions. One line of reasoning developed from the opinion in *Zippo Manufacturing Co. v. Zippo Dot Com Inc.*,[68] where the Eastern District of Pennsylvania proposed that "the likelihood that personal jurisdiction can be constitutionally exercised is directly proportional to the nature and quality of commercial activity that an entity conducts over the Internet." The *Zippo* court established a "sliding scale" of Internet activity. On one end of the scale lie passive websites that only provide information and do not allow any interaction between a user and the website, and thus, are unlikely to provide a basis for the exercise of jurisdiction. On the other end of the scale are fully interactive websites where a defendant conducts business over the Internet, a website much more likely to provide a basis for the exercise of jurisdiction.

---

[67] O.Z. v. Bd. of Trs. of Long Beach Unif. Sch. Dist., 2008 WL 4396895 (C.D. Cal. Sept. 9, 2008). *See also* Kowalski v. Berkeley Cnty Schs., 652 F.3d 565 (4th Cir. 2011) (student suspension over creation of MySpace page dedicated to ridiculing a fellow student did not violate the plaintiff's free speech rights because it was foreseeable that such conduct would reach the school via computers and smartphones and create a foreseeable substantial disruption there); D.J.M. v. Hannibal Pub. Sch. Dist., 647 F.3d 754 (8th Cir. 2011) (suspension upheld where student sent violent threats over instant messenger program from his home); Harris v. Pontotoc Cnty. Sch. Dist., 635 F.3d 685 (5th Cir. 2011) (school did not violate student's due process rights in suspending for causing a denial of service attack against the school network); Doninger v. Niehoff, 642 F.3d 334 (2d Cir. 2011) (school officials acted reasonably and deserved qualified immunity for prohibiting a student from running for Senior Class Secretary because of offensive off-campus blog posts that pertained to a school event); Tatro v. Univ. of Minn., 816 N.W.2d 509 (Minn. 2012) (university mortuary sciences program did not violate the free speech rights of graduate student by imposing sanctions for her Facebook posts that violated academic program rules where the academic program rules were narrowly tailored and directly related to established professional conduct standards); Bell v. Itawamba Cnty. Sch. Bd, 859 F.Supp.2d 834 (N.D. Miss. 2012) (student's suspension over rap video posted on YouTube and Facebook containing allegations against a teacher was upheld because lyrics caused a material and/or substantial disruption at school and it was reasonably foreseeable to school officials the song would cause such a disruption). *But see* J.S. v. Blue Mountain Sch. Dist., 650 F.3d 915 (3d Cir. 2011) (en banc) (school that suspended student for creating a lewd MySpace profile of the principal violated student's First Amendment rights because the facts simply do not support the conclusion that the School District could have reasonably forecasted a substantial disruption of or material interference with the school as a result of fake social media profile created off-campus); Layshock v. Hermitage Sch. Dist., 650 F.3d 205 (3d Cir. 2011) (en banc) (student's suspension for creating fictitious, offensive social media profile of school official not justified under exceptions that allow punishment for off-campus behaviors); R.S. v. Minnewaska Area Sch. Dist., 2012 WL 3870868 (D.Minn. Sept. 6, 2012) (First Amendment and privacy claims against school may proceed based upon search of student's Facebook account after a posting that was not truly threatening or disruptive to the school environment).

[68] 952 F.Supp. 1119 (E.D. Pa. 1997).

Another line of cases follow the reasoning of the Supreme Court's decision in *Calder v. Jones,*[69] a pre-Internet defamation case in which the Court held that jurisdiction could be premised on the intentional conduct of defendants outside the forum state that is calculated to cause injury to the plaintiffs within the forum state. Courts typically apply the *Calder* "effects test" in cases involving defamation or some other intentional tort, including trademark infringement.

The Northern District of California held in *Zynga Game Network Inc. v. Does* that an online videogame company that sought discovery from third-party web hosting companies and other websites seeking the identity of domain name holders who are allegedly operating infringing websites must narrow the scope of its subpoenas to information related to the identify and name the John Doe defendants.[70] The court granted the plaintiff's motion to conduct limited discovery, but narrowed the scope of the subpoenas, stating that the plaintiff's request for items such as server logs, website content transaction histories and correspondence remotely linked to the defendants was overbroad. The court ultimately limited the reach of the subpoena to "all documents necessary to obtain the name, current and permanent addresses, telephone numbers, and valid email addresses of the owner(s) of [the defendant's allegedly infringing website] or similar information suitable for identification and location of defendants."

In copyright infringement cases involving the uploading of a copyrighted printed literary work onto the Internet, the situs of injury for purposes of determining long-arm is the location of the principal place of business of the copyright holder, according to *Penguin Group, Inc. v. Am. Buddha.*[71] In answering a certified question from the Second Circuit, the New York Court of Appeals rejected the defendant's argument that a derivative economic injury felt in New York based solely on the domicile of the plaintiff was insufficient to establish an in-state injury within the meaning of the long-arm statute. The court commented that in the case of online infringement and digital piracy, where the harm is dispersed throughout the country, the place of uploading is inconsequential and it is difficult, if not impossible, to correlate lost sales to a particular geographic area, such that the out-of-state location of the infringing conduct carries less weight in the jurisdictional inquiry. Indeed, the court noted, "the absence of any evidence of the actual downloading of Penguin's four works by users in New York is not fatal to a finding that the alleged injury occurred in New York."

According to the Florida Supreme Court in *Internet Solutions Corp. v. Marshall*, a nonresident defendant commits the tortious act of defamation in Florida for purposes of Florida's long-arm statute when the nonresident makes allegedly defamatory statements about a Florida resident by

---

[69] 465 U.S. 783 (1984).

[70] Zynga Game Network Inc. v. Does 1-5, 2010 WL 271426 (N.D. Cal., Jan. 21, 2010). *See also* Pacific Century Int'l Ltd. v. Does, 2011 WL 2690142 (N.D. Cal. July 8, 2011) (mere allegation that multiple Doe defendants used the same BitTorrent network to infringe a copyrighted work is insufficient to meet the standards for joinder set forth in Rule 20; court found no evidence that users acted together to download the work, despite the collaborative nature of members of a BitTorrent "swarm").

[71] Penguin Group, Inc. v. Am. Buddha, 16 N.Y.3d 295 (2011). Following the ruling by the New York Court of Appeal on the certified question, the Second Circuit vacated the lower court's order and remanded to determine whether the plaintiff established the four remaining jurisdictional requistes under the New York long-arm statute, and the extent to which the assertion of personal jurisdiction would be consistent with the requirements of Due Process. Penguin Group Inc. v. Am. Buddha, 640 F.3d 497 (2d Cir. May 12, 2011). *But see* Troma Entm't Inc. v. Centennial Pictures Inc., 853 F.Supp.2d 326 (E.D.N.Y. 2012) (mere claims of infringement against New York copyright holder is insufficient to trigger *Penguin* rule; downloading of films over the Internet and subsequent unauthorized licensing of the works is far different than the uploading of copyrighted works and online distribution that occurred in *Penguin*).

posting those statements on a website, provided that the website posts containing the statements are accessible in the forum and accessed in the forum.[72] In answering this certified question from the Eleventh Circuit, the Florida Supreme Court did not address the second part of the long-arm jurisdictional analysis, namely whether an exercise of jurisdiction over a non-resident defendant under these circumstances violates the due process clause.

In *CoStar Realty Information Inc. v. Field*, unauthorized users' repeated exposure to website terms of use a over several year period bound them to terms, subjecting them to jurisdiction in the forum based upon their express and implied assent to the forum selection clause contained in the terms of use.[73]

In *Consulting Engineers Corp. v. Geometric Ltd.*, foreign software developers were not subject to personal jurisdiction in a Virginia forum based upon email and telephone contacts concerning a project in India, particularly since no agreement to perform work was ever reached.[74]

A social network website that allegedly used technology to embed advertisements into infringing, user-uploaded videos is subject to long-arm jurisdiction in the forum based upon evidence that the defendant sold advertisements to New York companies and sought to participate in advertising campaigns specifically directed at New York users, according to the decision in *Capitol Records LLC v. VideoEgg Inc.*.[75] The court found that such a showing was sufficient to establish that the defendant used its website to "transact business" in the forum.

The court held in *Chanel, Inc. v. Lin* that service of process by alternative means through an email address is not warranted where there is doubt that the defendant sends and receives emails from the address.[76] The court concluded that the plaintiff had not demonstrated that such alternative service would reasonably notify the defendant that litigation was pending against him.

---

[72] Internet Solutions Corp. v. Marshall, 2010 WL 2400390 (Fla. June 17, 2010). But see Penachio v. Benedict, 2012 WL 10971 (2d Cir. Jan. 4, 2012) (out-of-state witnesses in a family court proceeding who posted allegedly defamatory videos on YouTube, but had no related commercial interest in the forum, are not amenable to long-arm jurisdiction in New York).

[73] CoStar Realty Info. Inc. v. Field, 39 So.3d 1201 (Fla. 2010). In further proceedings, the court ruled that the plaintiffs' claim of loss based solely on the lost revenue from the license fees that plaintiffs would have recouped had some defendants entered into a license agreement to use its services is insufficient to qualify as a loss under the CFAA. *See* CoStar Realty Info. Inc. v. Field, 737 F.Supp.2d 496 (D. Md. 2010. Subsequently, the court ruled that the defendants were liable for breach of contract and copyright infringement for unauthorized uses that violated the database license agreement. *See also* CoStar Realty Information Inc. v. Field, 2010 WL 5391463 (D. Md. Dec. 21, 2010).

[74] Consulting Eng'rs Corp. v. Geometric Ltd., 561 F.3d 273 (4th Cir. 2009). *But see* Gallup, Inc. v. Bus. Research Bureau (PVT.) Ltd., 2008 WL 4857027 (N.D. Cal. Nov. 10, 2008) (federal court had subject matter jurisdiction over foreign defendants to hear the plaintiff's Lanham Act claims based upon allegation that "Gallup" trademark had an adverse effect on U.S. commerce).

[75] Capitol Records LLC v. VideoEgg Inc., 611 F. Supp. 2d 349 (S.D.N.Y. 2009).

[76] Chanel, Inc. v. Lin, 2009 WL 1034627 (S.D. Fla. Apr. 16, 2009). *See also* Chanel Inc. v. Zhibing, 2010 WL 1009981 (W.D. Tenn. Mar. 17, 2010) (email service of process on alleged online counterfeit product seller permitted where defendant's physical address could not be determined and he conducted business electronically via email); Chanel Inc. v. Zhixan, 2010 WL 1740695 (S.D. Fla. Apr. 29, 2010) (service via email to apparently active email accounts permitted where defendant had falsified WHOIS listing information and had no verifiable address in China); Gaffigan v. Does 1-10, 689 F.Supp.2d 1332, 1342 (S.D. Fla. 2010) ("[I]n this case, email was the method of communication used by Defendants in confirming orders placed on its websites, and thus, email should be calculated to provide Defendants with notice."); McCluskey v. Belford High Sch., 2010 WL 2696599 (E.D. Mich. June 24, 2010) (while the court disallowed alternate service via the defendant's web hosting company and posting on a website related to the ongoing lawsuit, it granted the plaintiff's motion to serve process to a working fax number and email address, as well as through the "live chat" feature on the defendants' website); Fortunato v. Chase Bank USA, N.A., 2011 WL 5574884 (S.D.N.Y. June 7, 2012) (court disallows service of process on individual via Facebook or her listed email address as on Facebook, but directed the defendant to serve third-party defendant via publication).

Service of process via a functional email address and international mail was authorized against an alleged foreign cybersquatter in an *in rem* action under the ACPA, captioned *Jenkins v. Pooke*.[77]

In *Chang v. Virgin Mobile USA, LLC*, an Australian company that downloaded a Flickr photo of a Texas resident pursuant to a Creative Commons License was not subject to Texas long-arm jurisdiction based upon tenuous contacts with the forum and the fact that the computer contracting processing may have been routed through servers located in the forum.[78]

V. CONCLUSION

The development of the Internet and new electronic media has created a host of new issues in almost all areas of the law – a not unsurprising form of new wine in old bottles. Digital media have impacted on subjects ranging from intellectual property, to privacy, to the First Amendment, and labor. As shown by the diversity of the above discussion, today's lawyers have had to develop new knowledge and skills. They seem to be off to a good, creative, and productive start.

[77] Jenkins v. Pooke, 2009 WL 412987 (N.D. Cal. Feb. 17, 2009). *See also* Chanel, Inc. v. Song Xu, 2010 WL 396357 (W.D. Tenn. Jan. 27, 2010) (effecting service of process on e-commerce merchants at their preferred email addresses permitted where WHOIS mailing address was invalid and email provided the greatest likelihood of generating a response from the served parties); Craigslist, Inc. v. Meyer, 2010 WL 2975938 (N.D. Cal. July 26, 2010) (service via email is appropriate since plaintiff demonstrated that, despite best efforts, it was unable to obtain a physical address for the defendant and the defendant conducted business solely through the Internet, and email service would not be prohibited by international agreement); Alfred E. Mann Living Trust v. ETIRC Aviation S.A.R.L., 78 A.D.3d 137 (1st Dept. 2010) (guaranty's provision waiving personal service of process and authorizing service of notices, demands, requests or other communications to a specific email address constitutes a waiver of personal service and the requirements that would otherwise dictate the manner to serve the foreign defendant, namely, CPLR 308 and the Hague Convention); U.S. Commodity Futures Trading Com'n v. Rubio, 2012 WL 3614360 (S.D. Fla. Aug. 21, 2012) (court allows service of process via defendant's still-active Yahoo email address that defendant previously swore under oath was used by him because it is reasonably calculated to give defendant notice of the action and defendant's address is unknown).

[78] Chang v. Virgin Mobile USA, LLC, 2009 WL 111570 (N.D. Tex. Jan. 16, 2009).