January 27, 2016

Legal Cases Relating To Web Harvesting

This is the first of a series of articles regarding data harvesting. The below document presents data harvesting related legal cases. Issues such as copyright infringement, breach of contract, the Computer Fraud and Abuse Act, trespass to chattels, and 'Hot news' misappropriation have to be considered when undertaking data harvesting operations. Cases are listed below:

Copyright Infringement

Breach of Contract

The Computer Fraud and Abuse Act

Trespass to Chattels

'Hot News' Misappropriation

Terms of Service Agreements

Case 1 Associated Press v. Meltwater

Associated Press (AP) v. Meltwater U.S. Holdings, Inc. (March 21, 2013), United States District Court, Southern District of New York: link

Profile: AP

News clipping service provided by AP is rather influential within the news industry – a staff of about 3,700 produces more than thousand articles each day across 1,400 individual newspapers. An AP story lede is employed to "convey the heart of the story, rather than serving as a teaser for the remainder of the story." AP members and licensees (roughly 8,000) are the ones publishing articles and licensing fees constitute the major part of AP's revenue.

Profile: Meltwater

Meltwater is a multinational "software as a service". Meltwater News is a service offered in the US since 2005, the monitoring service works with the use of keywords. Meltwater gathered articles from AP and delivered headlines to their customers via email. Meltwater is competing with AP for customers and won a "mega-contract" away from an AP licensee.

Issue

AP obtained copyright registrations for thirty-three articles and it filed the action against Meltwater on February 14, 2012. The central issue was whether Meltwater's activities constituted fair and transformative use. AP's complaint stresses six causes of action with respect to: (1) copyright infringement; (2) contributory copyright infringement; (3) vicarious copyright infringement; (4) declaratory judgment of copyright infringement; (5) "hot news" misappropriation under New York common law; and (6) removal or alteration of copyright management information.

Holding and Decision

The court found that Meltwater, which provided its subscribers with nearly 500-character excerpts of copyrighted articles gathered from the website of the Associate Press's licensees, did not engage in a fair use of those articles. Meltwater did not facilitate the general public's access to information on the Internet, but instead only provided word-for-word excerpts of the copied articles to the aggregator's paying customers without transforming that content in any way.

The court further held that the aggregator's use of that content to generate analytics relating to the online news sources it covered, while potentially transformative in and of itself, "did not render the aggregator's excerpting transformative insofar as the analytics and excerpting were separate and distinct services." The parties subsequently settled the case.

Case 2 Kelly v. Arriba Soft Corp

Kelly v. Arriba Soft Corp (July 7, 2003), United States District Court, Central District of California: link

Profile: Kelly
Leslie Kelly is a professional photographer who has copyrighted his works. Some of his photographs feature on his website, and Kelly also granted licenses to other websites to use his works.

Profile: Arriba Soft Corp
Arriba Soft Corporation ran a website which employed a search engine. The website's webcrawler program gathered images it found on the Internet, downloaded full-size images onto the servers, reduced them to a thumbnail size, and discarded the full-size images from the servers. Arriba Soft used an "inline linking" process from January through June 1999 and a "framing" process from July 1999 to August 2000.

Issue
Arriba copied some of Kelly's photographs without his permission. Kelly complained to Arriba and it subsequently removed the images placing Kelly's website on the list of websites on which its webcrawler would not operate. However, Kelly's images were still included as they were crawled from the third-party websites that had licenses. The initial copyright infringement case was ruled in favor of Arriba and Kelly appealed.

Holding and Decision
The United States Court of Appeals, Ninth Circuit, partially reversed and partially affirmed the rulings of the trial court. The Copyright Act sets forth four factors to evaluate in determining whether a copying constitutes "fair use:" 1) the purpose and character of the use, including whether the use is for commercial purposes or is for nonprofit educational purposes; 2) the nature of the copyrighted work; 3) the amount and substantiality of the portion used; and 4) the effect of the use upon the potential market for, or value of, the copyrighted work.

"We hold that Arriba's reproduction of Kelly's images for use as thumbnails in Arriba's search engine is a fair use under the Copyright Act. However, we hold that the district court should not have reached whether Arriba's display of Kelly's full-sized images is a fair use because the parties never moved for summary judgment on this claim and Arriba never conceded the prima facie case as to the full-size images. The district court's opinion is affirmed as to the thumbnails and reversed as to the display of the full-sized images. We remand for further proceedings consistent with this opinion. Each party shall bear its own costs and fees on appeal."

Case 3 Ticketmaster v. Tickets.com

Ticketmaster v. Tickets.com (March 27, 2000), United States District Court, Central District of California: link

Profile: Ticketmaster
Ticketmaster Corporation and Ticketmaster Online-CitySearch, Inc. (collectively referred to as “Ticketmaster”) act as plaintiffs in this case. Tickets to entertainment events are sold on the Ticketmaster website homepage of which contains instructions and an events directory. Users are taken from the homepage to event pages where they can find more detailed information.

Profile: Tickets.com
Tickets.com sells tickets to events through its website. Events for which Tickets.com doesn’t sell tickets are also listed and information as to where those tickets can be purchased is also listed. This information carries deep links that take users to the Ticketmaster’s website where they can purchase tickets. Text is generally included with the deep links telling users that “these tickets are sold by another ticketing company. Although we can't sell them to you, the link above will take you directly to the other company's web site where you can purchase them."

Issue
At the time of the action, Terms and Conditions of Ticketmaster’s website were located at the bottom of the homepage. A user could use the site without having to read the Terms, nor click an “I Agree” button. The T&Cs provide that continuous use of the website constitutes users agreeing to be bound by the T&Cs, which also prohibits deep linking and commercial use of the contents. Plaintiffs claimed that defendant had breached the contract embodied in the T&Cs and also infringed the copyright.

Holding and Decision
The court made an important ruling concerning deep linking. First, the court found that "hyperlinking [without framing] does not itself involve a violation of the Copyright Act ... since no copying is involved." Instead, "the customer is automatically transferred to the particular genuine web page of the original author. There is no deception in what is happening. This is analogous to using a library's card index to get a reference to particular items, albeit faster and more efficiently." The court further held that "deep linking by itself (i.e. without the confusion of source) does not necessarily involve unfair competition."

The court ruled that extracting events data and presenting it in its own format did not constitute copyright infringement. The breach of contract claim was also dismissed as the court ruled that a contract is not created simply by the use of a website which has T&Cs at the bottom of the homepage.

Case 4 Parker v. Yahoo and Microsoft

Parker v. Yahoo, Microsoft (September 26, 2008), United States District Court, Eastern District of Pennsylvania: link

Profile: Parker
Gordon Roy Parker is the author of registered works such as 'Why Hotties Choose Losers' and 'Outfoxing the Foxes'. The works are available on Parker's website for free.

Profile: Yahoo, Microsoft
Yahoo and Microsoft own widely used internet search engines.

Issue
When a user of either Yahoo or Microsoft searched for Parker's work, the results included links to archived, or 'cached', copies of the web pages. A user could follow the link to Parker's website or view the 'cached' version that is saved on the defendants' servers.

Parker claimed that both Yahoo and Microsoft republish his works without permission by making cached copies of his website available. Five claims against the defendants were brought forward: direct copyright infringement, contributory copyright infringement, vicarious copyright infringement, breach of contract, and negligence.

Holding and Decision
The /robots.txt file is used by website owners in order to give instructions to web robots. This is called The Robots Exclusion Protocol and acts as a de-facto standard.

The plaintiff knew that Yahoo had a policy of not creating cached copies of websites deploying the protocol, but deliberately decided not to use the protocol. The court held that the plaintiff's failure to deploy the /robots.txt protocol granted the defendants an implied license to create cached copies of Parker's website.

Case 5 CollegeSource v. AcademyOne

CollegeSource v. AcademyOne (February 05, 2015), United States Court of Appeals, Third Circuit: link

Profile: CollegeSource
CollegeSource, Inc. provides access to subscription-based and free college catalogs, including curriculums, equivalencies, and transferability.

Profile: AcademyOne
AcademyOne, Inc. is a software development firm that builds systems allowing faculties to evaluate credit equivalency of academic courses.

Issue
CollegeSource hosts catalogs of college courses and updates databases annually. Customers get access to databases, equivalency tools, and a free service, CataLink, that enables schools to link directly to the digitized catalogs.

AcademyOne hired a software developer to build its own database of course descriptions. The developer downloaded catalogs from the CataLink database and collected the PDF files obtaining text descriptions. AcademyOne purchased search-engine keywords “college source” and “career guidance foundation”, both CollegeSource’s trademarks. CollegeSource decided to sue AcademyOne for unfair competition and trademark infringement.

Holding and Decision
CollegeSource’s unfair competition and infringement claims were dismissed by the court as no sufficient evidence was provided. The court decided that AcademyOne using CollegeSource’s trademarks was not likely to cause confusion. The court used the four-factor likelihood-of-confusion test for keywords citing the Ninth Circuit in Network Automation, Inc. v. Advanced Systems Concepts, Inc., 638 F.3d 1137, 1154 (9th Cir. 2011): (1) strength of the mark, (2) evidence of actual confusion, (3) types of goods and degree of care likely to be exercised by the typical purchaser, and (4) the labeling and appearance of the advertisements triggered by the keywords.

Case 6 Cvent v. Eventbrite

Cvent, Inc. v. Eventbrite (September 14, 2010), United States District Court, Eastern District of Virginia: link

Profile: Cvent, Inc.
Cvent is a software-as-a-service company that provides a variety of resources to event planners, including information about event venues and their communities.

Profile: Eventbrite, Inc.
Eventbrite operates an event planning website, which included profiles of event venues.

Issue
Eventbrite decided to create a “Venue Directory” on its website including a collection of public information about hotels, restaurants, bars, and meeting venues. Cvent claimed that instead of aggregating public information itself, Stephan Foley was hired by Eventbrite whose task was to collect the information from Cvent’s website. Eight claims were included in the complaint:
1. Copyright Infringement
2. Violation of the Computer Fraud and Abuse Act
3. Violation of the Virginia Computer Crimes Act (VCCA)
4. Lanham Act "reverse passing off"

5. Breach of Contract (based on the Terms of Use posted on the Cvent's website)
6. Unjust Enrichment
7. Business Conspiracy
8. Common Law Conspiracy

Holding and Decision
Eventbrite didn't move to dismiss Count One, it could not do so under Fed.R.Civ.P. 12(b)(6) which states that a complaint should not be dismissed "unless it appears certain that [plaintiff] can prove no set of facts that would support his claim and would entitle him to relief". Eventbrite moved to dismiss the further seven claims and it was granted as to Counts Two, Three, Five, Seven, and Eight, and denied as to Counts Four and Six.

Eventbrite argued against the CFAA's "unauthorised use" requirement claiming that Cvent had a public website, i.e. browsing was not restricted. Cvent claimed that its user agreement prohibited anyone to gather data from the website. But the court claimed that "the Terms of Use for Cvent's website are not displayed on the website in any way in which a reasonable user could be expected to notice them." Therefore, the court decided that Cvent's website was not protected by its Terms of Use.

The court decided that Count Three (The VCCA claim) was pre-empted by the copyright infringement allegation, so it was dismissed. Count Four was not dismissed as Cvent argued that Eventbrite re-branded and re-packaged its product in order to sell as its own. The court quoted McCarthy on Trademarks and Unfair Competition (2006): "In many cases a Lanham Act false designation claim accompanies a copyright infringement claim in the complaint because it is unclear if the copyright is valid, is owned by the plaintiff, or is infringed. The Lahman Act claim is included as a back up in case the copyright claim fails."

Count Five was dismissed because Cvent's Terms of Use failed the Uniform Computer Information Transactions Act requirement that the term be ""available in a manner that ought to call it to the attention of a reasonable person," … or that the website "disclose[s] the availability of the standard terms in a prominent place on the site" and "does not take affirmative acts to prevent printing or storage of the standard terms for archival or review purposes."

Count Six survived copyright infringement pre-emption as the court decided that the defendant was unjustly enriched by material that was not protected by copyright. Counts Seven and Eight were dismissed because Cvent argued that Eventbrite working together with Foley constituted a conspiracy while the court treated Foley as an agent.

Case 7 Pacific Stock v. MacArthur & Company

Pacific Stock, Inc. v. MacArthur & Company, Inc. et. al. (June 12, 2012), United States District Court, Hawaii: link

Profile:
Pacific Stock markets and licenses photographic works. Doug Perrine's works are of particular interest in this case.

Profile:
Defendants MacArthur & Company, Inc. et al. used the photographic work on a website operated by Dream Communications, Inc.

Issue
The plaintiff sued for copyright infringement. Defendants failed to respond and a default judgment was entered against them. The issue became more serious because MacArtur used false copyright information when posting photos.

Holding and Decision
The court made a decision in plaintiff's favor. There are statutory damages of per violation of the Copyright Act, but the defendants also violated the Digital Millennium Copyright Act, so the court announced damages in the amount of $45,000.00 in statutory damages, $5,905.75 in attorney's fees, and $583.45 in other costs.

Case 8 EF Cultural Travel BV v. Zefer and Explorica

EF Cultural Travel BV v. Zefer Corp. and Explorica, Inc. et al. (November 01, 2001), United States Court of Appeals, First Circuit: link

Profile: EF Cultural Travel BV
EF is an education company offering programs around the world, including language learning and cultural exchange.

Profile: Zefer Corp. and Explorica, Inc.
Explorica, founded by former EF employees, entered the student travel business in order to compete with EF.

Zefer Corporation provided services of Internet implementation and consulting.

Issue
Users coming to EF's website can search through the tour database and view prices according to different criteria (tour duration, destination cities, etc.) Explorica intended to compete with EF and decided to set their own tour prices slightly lower, so it hired Zefer to harvest EF's prices. EF found out about the harvesting activity during another case that involved back wages which Explorica's President brought up against EF.

EF sued Explorica, Zefer, and several of Explorica's employees. EF claimed that the defendants' actions violated the federal Copyright Act and the CFAA.

Holding and Decision
EF did not prohibit the use of harvesting technology in the Terms of Use at the time, so the court decided not to affirm the injunction. The court stated that Zefer could have been sure that its data harvesting activities would not please EF, but it also stated that EF would not have liked the same data compilation performed manually. The court mentioned that "EF did not purport to exclude competitors from looking at its website and any such limitation would raise serious public policy concerns."

Case 9 Southwest Airlines v. BoardFirst

Southwest Airlines Co. v. BoardFirst, LLC (September 12, 2007), United States District Court, Northern District of Texas, Dallas Division: link

Profile: Southwest Airlines Co.
Southwest, established in 1967, is the world's largest low-cost airline carrier. No first-class cabins or other fee differentiated services are offered. Instead, an "open seating" policy is employed with passengers divided into three ("A", "B", and "C") boarding groups. "A" group boards the plane first, then comes the "B" group and, lastly, group "C".

Customers can check in for their flights using the Southwest website within 24 hours of departure. Customers who check in earlier have the higher likelihood of getting an "A" boarding pass (limited tp the first 45 passengers).

Profile: BoardFirst, LLC
BoardFirst assisted Southwest customers in getting the desired "A" boarding pass for a fee of $5 (no charge if an "A" pass is not obtained). The customer had to authorize BoardFirst to act as his agent and provide his name, flight confirmation number, and credit card information. On average, BoardFirst procured fewer than 100 boarding passes for Southwest customers per day.

Issue
Southwest complained that BoardFirst's actions were in violation of their website's Terms and Conditions. At the bottom of Southwest's homepage, it is mentioned that the "[u]se of the Southwest websites . . . constitutes acceptance of our Terms and Conditions." T&Cs state (bold part added on February 1, 2006):

"Southwest's web sites and any Company Information is available to you only to learn about, evaluate, or purchase Southwest's services and products. Unless you are an approved Southwest travel agent, you may use the Southwest web sites and any Company Information only for personal, non-commercial purposes. ***For example, third parties may not use the Southwest web sites for the purpose of checking Customers in online or***

attempting to obtain for them a boarding pass in any certain boarding group."

BoardFirst continued operations despite two cease-and-desist letters sent by Southwest Airlines. The lawsuit was filed on May 17, 2006 with claims of breach of contract, violations of the CFAA, and harmful access by a computer under Chapter 143 of the Texas Civil Practice and Remedies Code.

Holding and Decision
The court granted Southwest's motion for summary judgment on its breach of contract claim, finding that the defendant's conduct directly contravened Southwest's prohibition on commercial uses of Southwest's website. It was decided that Boardfirst was subject to a binding browsewrap agreement with Southwest.

Browsewrap agreements, noted the Court, "may take various forms but typically … involve a situation where a notice on a website conditions use of the site upon compliance with certain terms or conditions, which may be included on the same page as the notice or accessible via a hyperlink. … A defining feature of a browsewrap license is that it does not require the user to manifest assent to the terms and conditions expressly – the user need not sign a document or click on an "accept" or "I agree" button. A party instead gives his assent simply by using the website."

Furthermore, Southwest Airlines demonstrated injuries as a result of BoardFirst's operations as they were likely to reduce the number of website visitors and the possibility of additional service sales.
BoardFirst's operations were found to be in violation of the Texas Penal Code which prevents a person from "knowingly accessing a computer, computer network or computer system without the effective consent of the owner." However, the court did not find BoardFirst in violation of the CFAA as the requisite amount of Southwest's loss was not determined.

Case 10 TrueBeginnings v. Spark Network Servs.

TrueBeginnings, LLC v. Spark Network Servs., NSHN (March 13, 2009), United Stated District Court, Northern District of Texas: link

Profile: TrueBeginnings, LLC
TrueBeginnings owns an online relationship and dating service, "true.com".

Profile: Spark Network Servs. and NSHN
Spark is the owner by assignment of U.S. Patent No. 6,272,467 B1 ("the '467 Patent"), entitled "System for Data Collection and Matching Compatible Profiles." NSHN is a Chicago law firm that represents Spark in the licensing and enforcement of the '467 Patent.

Issue
NSHN attorneys accessed the True.com website on several occasions with Jason Hicks taking a screenshot on November 2, 2007 that stated: “part of an investigation to determine whether the "True Compatibility Index" infringes the *467 Patent.” NSHN claimed that True.com infringed at least two claims of the '467 Patent’.

Plaintiff filed the action against Spark and NSHN for breach of contract, negligent misrepresentation, violations of federal and Texas computer protection statutes, common law trespass, and declaratory relief. It was claimed that NSHN acted on behalf of Spark and violated the Terms of Use by accessing the True.com website to investigate whether TrueBeginnings infringed the '467 Patent.

Holding and Decision
Spark Network Services use of the website to gather evidence for a patent lawsuit did not involve unauthorized uses of the dating services, and thus did not breach plaintiff's terms of use. Therefore, the court found that Spark Network Services did not violate the terms of service of plaintiff's dating website – which limited use of the “website and related services” to a visitor's “sole, personal use” – by visiting the website to obtain evidence for use in a patent infringement action against plaintiff.

Case 11 Internet Archive v. Shell

Internet Archive v. Shell (April 25, 2007), United States District Court, District of Colorado: link

Profile: Internet Archive
Internet Archive is a non-profit organization with the stated mission of “universal access to all knowledge”. Its goal is to preserve all websites, documents and other information on the Internet. Wayback Machine technology is used by Internet Archive in order to advance its operations. The Wayback Machine browses the web, copies the content and puts them in the Internet Archive. Website owners are not asked for permission, but they are provided with instructions as to how materials can be removed from the archive. Furthermore, the Internet Archive removes content upon the request of the website owners.

Profile: Shell
Shell owns a website, www.profane-justice.org (“Profane Justice,”) that provides information and services to individuals accused of child abuse or neglect.

Issue
The Wayback Machine reproduced Shell’s website approximately 87 times during May 1999 – October 2004 period. The website, registered with the Copyright Office, included a notice that stated: “If you copy or distribute

anything on this site — you are entering into a contract." This "contract" included the charge of $5,000.00 for each page copied and $250,000.00 for an "unauthorized use" plus $50,000.00 per each occurrence.

Shell discovered that Profane Justice had been archived by the Internet Archive and sent an email requesting the removal of all content. She also demanded payment of $100,000.00 threatening to sue otherwise. The Internet Archive immediately removed all content but did not pay the requested $100,000.00.

The Internet Archive sought a judicial determination that the defendant's copyright was not violated and filed a declaratory judgment action. Shell filed counterclaims for copyright infringement, breach of contract, conversion, civil theft, and racketeering under the Racketeering Influenced and Corrupt Organizations Act (RICO) and Colorado Organized Crime Control Act (COCCA).

Holding and Decision
The claims of conversion, civil theft, and racketeering were dismissed by the court, but the criminal infringement under RICO and the breach of contract claims were not. The Internet Archive enjoyed a financial benefit through advertising revenue, thus an infringing act had occurred (use of the Wayback Machine) and the defendant sufficiently pleaded the criminal copyright infringement claim. The court rejected Internet Archive's pre-emption (as it is a non-profit organization) argument, finding that Internet Archive's alleged agreement to refrain from the use of the material on plaintiff's website "for commercial or financial purposes … lie[s] well beyond the protections [the website owner] receives through the Copyright Act."

The court also determined the existence of a contract. Despite the Internet Archive's argument that "no human being from Internet Archive actually knew of the terms of use", the defendant had sufficiently alleged a breach of contract and resulting damages.

Case 12 QVC v. Resultly

QVC Inc. v. Resulty LLC (November 24, 2014), United States District Court, Eastern District of Pennsylvania: link

Profile: QVC Inc.
QVC Inc. is the video and e-commerce retailer. In 2014, e-commerce generated $3.5B for QVC out of $8.8B total revenue.

Profile: Resultly LLC

Resultly is a free online shopping app, their software crawls online shopping websites to obtain current prices of particular products.

Issue
QVC alleged that Resultly's program was crawling the QVC site at an "excessive rate" causing it to crash for two days. QVC also claimed that an attempt was made by Resultly to hide the activity of its program and IP address.

QVC's complaint stated that: 1) Resultly violated the site's Terms and Conditions as it was used for business rather than shopping; 2) Resultly's activity violated the Computer Fraud and Abuse Act CFAA); and 3) unjust enrichment, conversion, negligence and tortious interference with economic advantage took place.

Holding and Decision
In order to fall under the CFAA, Resultly must have intended to damage QVC's servers with its crawling activity. However, the evidence showed that Resultly's business plan required the website to stay functional. Therefore, the court denied the preliminary injunction request made by QVC. It stated: "Resultly was not QVC's competitor, a disgruntled QVC employee, or an unhappy QVC customer aiming to cause damage to QVC's server. To the contrary, Resultly's goal was to grow a loyal user base of people who gain something from being directed to QVC's website. For Resultly to meet this goal, it needed the QVC website to run smoothly, and it needed QVC to allow Resultly to crawl its site. Although Resultly may have ultimately damaged its relationship with QVC by: (1) assuming that QVC's website could handle Resultly's requests without implementing a crawl delay; and (2) failing to identify itself in its user name during the time it crawled the QVC server, neither of these "objective identifiers" suggests that Resultly wanted to damage QVC's server or thought damage was a likely outcome of its actions….At most, the objective indicators QVC offers regarding Resultly's crawl speed and user agent information suggest that, as a fledgling company, Resultly had yet to iron out certain wrinkles in its business operations."

Case 13 U.S. v. Auernheimer

U.S. v. Auernheimer (April 11, 2014), United States Court of Appeals for the Third Circuit: link

Profile: Auernheimer
Auernheimer is a member of "Goatse Security" computer experts group that uncovered a flaw in AT&T's security system which resulted in the exposure of iPad users' email addresses.

Issue
Customers who purchased the first iPad (introduced in 2010) with a cellular data capability had to get a contract from AT&T, the exclusive data provider for iPads at the time. Customers had to go through the registration process on a website under AT&T's control, receive a user ID, and create a password. AT&T decided to prepopulate the user ID field with the customers' email addresses in order to make the registration process easier. AT&T had to

program its servers to look for an iPad user's Integrated Circuit Card Identifier (ICC-ID) in order to automatically redirect the customer's browser from the general login page to a specific page. This redirection to the specific URL informed AT&T's servers which email addresses had to be populated on the login page.

Daniel Spitler discovered the way AT&T's registration and login processes worked and shared this information with Auernheimer. They designed a program that automatically changed ICC-IDs in the browser and collected 114,000 email addresses. Auernheimer informed various members of the media about their exploits and sent email addresses to Ryan Tate from Gawker. Tate published a story describing the security breach at AT&T and mentioned some of the names of email address holders. Auernheimer was subsequently charged with conspiracy to violate the CFAA and identity fraud in violation of 18 U.S.C. § 1028(a)(7).

Holding and Decision
The district court found Auernheimer guilty on both charges and sentenced him to forty-one months in jail. However, Auernheimer won the appeal as the Third Circuit stated that the venue of the original conviction (New Jersey) was improper as neither Auernheimer nor Spitler performed any "essential conduct element" in New Jersey.

The judges noted their skepticism of the original conviction stating that "in order to be guilty of accessing "without authorization, or in excess of authorization" under New Jersey law, the Government needed to prove that Auernheimer or Spitler circumvented a code- or password based barrier to access." Auernheimer and Spitler accessed only the publicly facing part of the login page and collected information that AT&T accidentally published.

Case 14 Craigslist v. 3Taps

Craigslist v. 3Taps (July 20, 2012), United States District Court, Northern District of California: link

Profile: Craigslist
Craigslist operates a well-known classified advertisements website.

Profile: 3Taps
Defendant 3Taps aggregated and republished Craigslist ads. 3Taps marketed a "Craigslist API" so third parties could access large amounts of Craigslist content, and also operated the website craiggers.com, which "essentially replicated the entire craigslist website."

Issue
Craigslist sued 3Taps claiming that 3Taps' harvesting activities were in violation of the Computer Fraud and Abuse Act. The claims of breach of Craigslist's terms of service, copyright and trademark infringement, contributory copyright infringement (3Taps shared the listings with PadMapper) were also brought up. PadMapper received a cease-and-desist letter from Craigslist but decided to ignore it.

Holding and Decision
The CFAA claim is only considered in a situation of an unauthorized access to a protected computer system. 3Taps claimed that everyone had the authorization to access Craigslist as it was a public website. The court didn't agree with this as the authorization granted to 3Taps was revoked.
3Taps argued that the CFAA was meant to protect private information against hackers rather than limit the social benefit of public data. Yet, the court denied the defendant's motion to dismiss and compared its decision to a store that is open to public but could also ban a disruptive person.

Case 15 U.S. v. Nosal

U.S. v. Nosal (April 10, 2012), United States Court of Appeals for the Ninth Circuit: link

Profile: Nosal
David Nosal used to work for an executive search firm, Korn/Ferry. He resigned and convinced some of his former colleagues to join him in a new competing venture.

Issue
The employees were still working for Korn/Ferry, downloaded source lists, contact information from a confidential database, and sent it all to Nosal. These employees had the authorization to access the database, but Korn/Ferry had a policy in place forbidding disclosure of confidential information.

Nosal was indicted by the government on twenty counts of the CFAA violations for helping the Korn/Ferry employees in "exceed[ing their] authorized access" with intent to defraud.

Holding and Decision
The Ninth Circuit held in an en banc decision that "the phrase 'exceeds authorized access' in the CFAA does not extend to violations of use restrictions," but rather concerns "hacking—the circumvention of technological access barriers."

Case 16 Fidlar v. LPS

Fidlar v. LPS (November 08, 2013), United States District Court, Central District of Illinois: link

Profile: Fidlar
Fidlar is a software firm that specializes in land records management systems.

Profile: LPS
LPS is a real estate data analytics company.

Issue
Fidlar developed a program called Laredo that transferred paper real estate records online. LPS used web harvesting techniques to bypass protocols that Fidlar had in place so they could capture electronic records, online minutes were not tracked and LPS did not have to pay certain print fees either. LPS didn't seek or receive Fidlar's consent when it decided to copy Loredo's traffic and copy the images of public records. Fidlar decided to file a suit stating that LPS' actions violated the Computer Fraud and Abuse Act, the Illinois Computer Crime Prevention Law, and constituted trespass to chattel. LPS filed a motion to dismiss all three counts.

Holding and Decision
The federal court decided to grant summary judgment for LPS and all three of Fidlar's claims failed. The claim of the CFAA violation failed as there was a lack of evidence proving LPS' intent to defraud and the fact of electronic information copying was not enough to fulfill the CFAA's damage requirement. An intent to defraud is defined as acting ""willfully and with specific intent to deceive or cheat, usually for the purpose of getting financial gain for one's self or causing financial loss to another."

The Illinois Computer Crime Prevention Law failed as it was not shown that LPS knew that its actions would cause Fidlar to lose subscription revenue. Fidlar's trespass to chattels claim also failed as the direct physical interference was not demonstrated.

Case 17 Facebook v. Power Ventures

Facebook Inc. v. Power Ventures (October 22, 2009), United Stated District Court, Northern District of California: link

Profile: Facebook
Facebook is an online social networking service launched in 2004.

Profile: Power Ventures
Power Ventures was offering an online service that aggregated various social networking sites so users could manage all of their profiles from one place.

Issue
Facebook sued Power Ventures claiming the violation of the Computer Fraud and Abuse Act and the California state equivalent. Power Ventures was connecting to Facebook data and allowing its users to access Facebook as well. Facebook blocked a specific Power IP address, yet the operations continued. Facebook also claimed the violation of CAN-SPAM Act because Power used Facebook Events (with the header information indicating messages from Facebook, not Power) in order to invite users and their friends to its system.

Holding and Decision
The district court upheld both claims and ordered the payment of more than $3 million in damages. Facebook argued that Power was intentionally trying to get around the IP block. Power, on the other hand, claimed that using multiple IP addresses constituted its normal business practice The court decided that Power's access to Facebook was without authorization and therefore in violation of the CFAA. This case is now pending before the Ninth Circuit.

Case 18 Pulte Homes v. Laborers' International Union

Pulte Homes, Inc. v. Laborers' International Union (August 02, 2011), United States Court of Appeals, Sixth Circuit: link

Profile: Pulte Homes
Pulte is a home building company founded in 1950.

Profile: Laborers' International Union
Laborers' International Union of North America (LIUNA) was formed in 1903, its goal is to advance the interests of its members (557,999 as of 2013).

Issue
In September 2009, Pulte fired a construction crew member for what they claimed was misconduct and poor performance. LIUNA decided to run a national campaign against Pulte to damage its reputation as union membership was thought to be the main reason for dismissal. Pulte's sales offices and executives were bombarded with emails and phone calls resulting in the overload of Pulte's system.

Pulte decided to sue claiming the CFAA violations. The district court dismissed the claim as it was not shown that LIUNA intentionally damaged Pulte's computer systems and phones. Pulte appealed.

Holding and Decision
The Sixt Circuit stated upheld Pulte's "transmission" claim. Pulte's operating ability, its usage of systems and data, was diminished because of LIUNA's actions. However, LIUNA could use phone and email systems under the CFAA as Pulte's systems were open to the public, thus anyone was authorized to use them.

Case 19 U.S. v. Phillips

U.S. v. Phillips (January 24, 2007), United States Court of Appeals, Fifth Circuit: link

Profile: Phillips
In 2003, Christopher Andrew Phillips was admitted to the Department of Computer Sciences of the University of Texas at Austin (UT). Phillips agreed not to scan university ports with his university account by signing UT's "acceptable use" computer policy.

Issue
Few weeks later, Phillips started using various programs in order to scan networks and steal encrypted data, including credit card numbers, birth records, passwords, bank account information, student financial aid statements, and Social Security numbers. He infiltrated hundreds of computers and designed the brute-force attack program. The program increased the monthly number of TXClass' (UT's employee training management system) unique requests received by the UT computer system from 20,000 to 1,200,000 causing it to crash several times in 2003. Phillips was convicted after a jury trial on a count of computer fraud and a count of possession of an ID document that contained stolen Social Security numbers. He was sentenced to five *219 years' probation and five hundred hours of community service. Phillips appealed.

Holding and Decision
Phillips argued that due to the fact that TXClass was a public website application, he had a de facto authorized access. The CFAA does not define the term "authorization", but differentiates between unauthorized users and those who "exceed authorized access". The conviction and sentence were affirmed.

Case 20 Ebay v. Bidder's Edge

EBay Inc. v. Bidder's Edge, Inc. (May 24, 2000), United States District Court, North District of California: link

Profile: eBay, Inc.
EBay is an online person-to-person trading site.

Profile: Bidder's Edge, Inc.
Defendant Bidder's Edge (BE) operated an auction aggregation web site offering information about ongoing auctions on different websites, including eBay. Approximately 69% of the BE site consisted of information about eBay auctions.

Issue
BE used a robot crawler in order to obtain information about eBay's auctions. This robot accessed eBay's website approximately 100,000 times a day representing between 1.11% and 1.53% of the total load on eBay's servers. The plaintiff permitted limited robot searches and attempted to block BE's access, but the defendant used proxy servers and evaded it. License arrangement was being worked on, but the attempts failed and eBay moved for an injunction to enjoin BE from accessing its computer system in any manner.

Holding and Decision
Trespass to chattels relates to physical harm caused to a website and its servers impeding their use or utility of its servers for different purposes. The defendant's spiders consumed a portion of eBay's server and server capacity, and thereby "deprived eBay of the ability to use that portion of its personal property for its own purposes." The unauthorized activity performed by the defendant established a cause of action for trespass to chattels. EBay argued that the defendant's activity could "encourage other auction aggregators to engage in recursive searching" and cause "irreparable harm from reduced system performance, system unavailability, or data losses." Thus, the court granted eBay's motion.

Case 21 Barclays v. Theflyonthewall.com

Barclays Capital Inc. et al. v. Theflyonthewall.com, Inc. (June 20, 2011), United States Court of Appeals for the Second Circuit: link

Profile: Barclays Capital, Morgan Stanley, Merrill Lynch
Barclays Capital, Morgan Stanley, and Merrill Lynch are investment banks that produce stock recommendations and investment research.

Profile: Theflyonthewall.com
Theflyonthewall.com, Inc. was providing a subscription-based news service.

Issue
The defendant was obtaining daily stock recommendations and investment research created by the investment banks. The defendant's subscribers could receive the information prior to the release by the plaintiffs. The plaintiffs decided to sue alleging copyright infringement and "hot news" misappropriation.

Holding and Decision
"Hot news" misappropriation provides a cause of action where a party reproduces factual, time-sensitive information that was gathered at the effort and expense of another party, and thereby deprives the gathering party of the commercial value of that information. This is the legacy of common law (originating from Int'l News Serv. v. Associated Press, the Supreme Court in 1918) and only applicable in 5 U.S States.

The court emphasized that the plaintiffs' claim lacked an “indispensable element of an INS ‘hot news' claim,” i.e., “free-riding by a defendant on a plaintiff's product, enabling the defendant to produce a directly competitive product for less money because it has lower costs.”

Though the defendant's conduct potentially threatened plaintiffs' businesses, the defendant was actually breaking news generated by the plaintiffs' recommendations and attributing the recommendations to plaintiffs, rather than merely repackaging news that had been reported by plaintiffs.

Case 22 Nguyen v. Barnes & Noble

Nguyen v. Barnes & Noble, Inc. (August 18, 2014), United States Court of Appeals, Ninth Circuit: link

Profile: Nguyen
Kevin Khoa Nguyen purchased two touchpads during an online “fire sale” held on Barnes & Noble website.

Profile: Barnes & Noble
Barnes & Noble, Inc. is a retail bookseller, the largest in the United States. It owns hundreds of bookstores and the website www.barnesandnoble.com.

Issue
In August 2011, Barnes & Noble decided to liquidate its inventory of Hewlett-Packard Touchpads by holding an online “fire sale”. On August 21, Kevin Khoa Nguyen purchased two items on the defendant’s website and received a confirmation via email. The next day, however, he received an email informing him about the cancellation because of high demand. Nguyen alleged that this delay in informing him about the cancellation prevented him from obtaining Touchpads for the discounted price. Nguyen stated that he had been “forced to rely on substitute tablet technology, which he subsequently purchased . . . [at] considerable expense.”

In April 2012, Nguyen filed a class action suit together with two other customers whose orders had been cancelled. The lawsuit was filed in California Superior Court with the claims of “deceptive business practices” and “false advertising” against the defendant. Barnes & Noble decided to move the action to the federal court and argued that Nguyen was bound by the website’s Terms of Use agreement.

Holding and Decision
The court determined that the Barnes & Noble website's Terms of Use was part of a "browsewrap" agreement (hyperlink at the bottom of the website) and distinguished it from a "clickwrap" agreement (users have to click "I agree"): "Unlike a clickwrap agreement, a browsewrap agreement does not require the user to manifest assent to the terms and conditions expressly."

The court did not find any evidence proving that Nguyen had known about the agreement and decided that ""proximity or conspicuousness of the hyperlink alone is not enough to give rise to constructive notice." Therefore, it was determined that Nguyen should not have been bound to the agreement.