Brooklyn Law Review

Volume 81 | Issue 1 Article 11

2015

Breaching and Entering: When Data Scraping Should Be a Federal Computer Hacking Crime

Myra F. Din

Breaching and Entering

WHEN DATA SCRAPING SHOULD BE A FEDERAL COMPUTER HACKING CRIME

"No foreign nation, no hacker, should be able to shut down our networks, steal our trade secrets, or invade the privacy of American families . . . ."[1]

INTRODUCTION

In July 2015, hackers known as the Impact Team breached AshleyMadison.com and threatened to expose the private lives and extramarital affairs of over 30 million users.[2] This hack was just one of many; indeed, within the past two years, Americans have seen a huge increase in the number of large-scale data breaches. In November 2014, hackers made global headlines when they exposed media conglomerate Sony's confidential company data.[3] Between February and March of 2014, the global retailer eBay, which has over 148 million accounts, suffered a major data hack that it did not detect until May of that year.[4] In April 2014, hackers attacked AOL, compromising the email addresses, passwords, and contact lists of 120 million users.[5] In mid-2014, hackers seized the private financial information of 76 million households and 7 million small

---

[1] President Barack Obama, State of the Union Address (Jan. 20, 2015), https://www.whitehouse.gov/the-press-office/2015/01/20/remarks-president-state-union-address-january-20-2015 [http://perma.cc/57PL-HSDU].

[2] *World's Biggest Data Breaches*, INFORMATION IS BEAUTIFUL (Aug. 11, 2015), http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/ [http://perma.cc/BU4J-4PL8]; *Ashley Madison Users Face Threats of Blackmail and Identity Theft*, N.Y. TIMES (Aug. 27, 2015), http://www.nytimes.com/2015/08/28/technology/ashley-madison-users-face-threats-of-blackmail-and-identity-theft.html [http://perma.cc/DE67-Q3WT].

[3] Brooks Barnes & Michael Cieply, *Sony Cyberattack, First a Nuisance, Swiftly Grew Into a Firestorm*, N.Y. TIMES (Dec. 30, 2014), http://www.nytimes.com/2014/12/31/business/media/sony-attack-first-a-nuisance-swiftly-grew-into-a-firestorm-.html?r=0 [http://perma.cc/3EQJ-LE9M].

[4] Jose Pagliery, *eBay Customers Must Reset Passwords after Major Hack*, CNN MONEY (May 21, 2014, 2:53 PM), http://money.cnn.com/2014/05/21/technology/security/ebay-passwords/index.html [http://perma.cc/6HDV-SWTU].

[5] *Id.*

businesses that used JP Morgan.[6] In August 2014, up to 200 photographs of celebrities were hacked and posted on the website 4chan.[7] And in September 2014, Home Depot suffered a data breach that resulted in the theft of 56 million of its customers' credit card numbers.[8]

The recent proliferation of data hacking underscores the need for robust antihacking laws to effectively punish data hacking criminals. Yet as society becomes adept at using the Internet for numerous beneficial purposes, it is necessary to ensure that such laws clearly distinguish between criminal computer hacking and permissible uses of the digital realm.

The need for clear antihacking legislation is not new. Data hacking first became a federal concern several decades ago. In the early 1980s, during the nascent years of the Internet, Congress began to recognize that computer hacking posed novel threats to national security. Congress enacted the first legislation to combat computer fraud in 1984. The act, known as the Counterfeit Access Device and Computer Fraud and Abuse Act (CADCFAA),[9] created criminal sanctions for the unauthorized use of computers.[10] In proscribing computer fraud and the use of counterfeit access devices in the same act, Congress likened computer hacking to the crimes of credit card fraud and identity theft.[11] But while existing laws were directed only at perpetrators of credit card fraud, the CADCFAA targeted computer hackers.

The CADCFAA described "hackers" as individuals who could "access (trespass into) both private and public computer systems, sometimes with potentially serious results," and who could "access and control high technology processes vital to our everyday lives."[12] Although these phrases indicate that Congress

---

[6] Jessica Silver-Greenberg, Matthew Goldstein & Nicole Perlroth, *JPMorgan Chase Hacking Affects 76 Million Households*, N.Y. TIMES (Oct. 2, 2014, 12:50 PM), http://dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/?_php=true&_type=blogs&_r=1 [http://perma.cc/2ERF-KDUK].

[7] Fay Strang, *Celebrity 4chan Shock Naked Picture Scandal: Full List of Star Victims Preyed upon by Hackers*, MIRROR ONLINE (Oct. 10, 2014, 10:00 AM), http://www.mirror.co.uk/3am/celebrity-news/celebrity-4chan-shock-naked-picture-4395155 [http://perma.cc/HGR2-HBBF].

[8] Melvin Backman, *Home Depot: 56 Million Cards Exposed in Breach*, CNN MONEY (Sept. 18, 2014, 5:56 PM), http://money.cnn.com/2014/09/18/technology/security/home-depot-hack/ [http://perma.cc/DJ3U-NXF4].

[9] Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, 98 Stat. 2190 (codified as amended at 18 U.S.C. § 1030 (2008)); H.R. REP. NO. 98-894, at 21 (1984).

[10] H.R. REP. NO. 98-894.

[11] "[T]here are indications of a growing problem in counterfeit credit cards and unauthorized use of account numbers or access codes to banking system accounts . . . ." *Id.*

[12] H.R. REP. NO. 98-894, at 10 (1984); Counterfeit Access Device and Computer Fraud and Abuse Act of 1984.

was beginning to understand the nature of computer hacking, the phrases' generality demonstrates that Congress only had a rudimentary framework to define this new type of crime.[13] To that end, the CADCFAA only prohibited the hacking of certain types of information, such as matters concerning national security, foreign relations, and financial credit.[14] It also only applied to select computers, such as those that were operated for or on behalf of the government[15] or those that belonged to financial institutions and contained financial records.[16] Moreover, shortly after enacting the CADCFAA, Congress separately passed the Electronic Communications Privacy Act of 1986 (ECPA) to prohibit other computer crimes, such as wiretapping.[17] As a consequence of all these limitations, the CADCFAA's scope was quite narrow.

In 1986, Congress passed the Computer Fraud and Abuse Act (CFAA), which proscribes more conduct than the CADCFAA.[18] Since its ratification, a large number of cases have been brought under the CFAA. The diversity of cases, their mixed outcomes, and the evolution of hacking since the passage of the CFAA demonstrate that the definition of computer hacking is still unsettled. While certain conduct—such as intentionally releasing worms that cause massive secured computer networks to crash[19]—closely embodies the traditional concept of data hacking, other conduct—such as creating fake MySpace accounts in order to harass teenagers—less clearly constitutes hacking.[20] Much of this uncertainty is due to the novel ways of engaging in Internet communication, such as through social media, which did not exist when the CFAA was enacted.

---

[13] While drafting the Act, the House discussed the difficulties that arose because much of the intangible property involved did not fit well into traditional categories of property subject to abuse or theft. *See* H.R. REP. NO. 98-894, at 9-10. Additionally, the House specifically noted that the criminal justice system at the time was "largely uninformed concerning the technical aspects of computerization, and bound by traditional legal machinery which in many cases may be ineffective against unconventional criminal operations." *Id.*

[14] MICHAEL D. SCOTT, *§ 17.12 Federal Computer Crime Legislation*, *in* SCOTT ON INFORMATION TECHNOLOGY LAW (2014).

[15] *Id.*

[16] Act of Oct. 12, 1984, Pub. L. No. 98-473, tit. II, §§ 1602(a), 2102(a), 98 Stat. 2183, 2190.

[17] *See Electronic Communications Privacy Act (ECPA)*, ELECTRONIC PRIVACY INFORMATION CTR., https://epic.org/privacy/ecpa/ [http://perma.cc/4R8B-TUH2] (last visited Dec. 6, 2015); Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat.1848 (codified as amended in various sections of 18 U.S.C.).

[18] For example, in 1994, Congress added private causes of action to the CFAA to allow victims to recover economic damages in civil cases. *See* Computer Fraud and Abuse Act, 18 U.S.C. § 1030(g) (2012).

[19] United States v. Morris, 928 F.2d 504, 505 (2d Cir. 1991).

[20] Kim Zetter, *Judge Acquits Lori Drew in Cyberbullying Case, Overrules Jury*, WIRED (July 2, 2009, 3:04 PM), http://www.wired.com/2009/07/drew_court/ [http://perma.cc/S63V-WMLH].

One of the murkier activities that may constitute hacking is data scraping. Unlike traditional hacking, scraping involves using computer programs, known as scrapers, to extract large amounts of data from websites.[21] Scrapers automatically compile Internet search results, filter inappropriate content, and extract large amounts of information from public and private websites.[22] Because scrapers are fairly inexpensive and easy to access, they are used for a variety of purposes, both beneficial and harmful.[23]

In order to be considered beneficial, scrapers should meet at least three criteria. First, the scraper should gather data that is already publicly available and is not protected by a code barrier, such as a password or other technical security measure. Second, the scraper should be used to amalgamate data and present it in a manner that offers some benefit to a consumer in terms of efficiency or ease-of-access. And third, the scraper should be used in a way that does not directly harm the data host from which it retrieves the data, such as by inhibiting the data host's own access to its data, compromising the safety of the data host's consumers, or seriously undermining the data host's website functionality or profitability.

One example of a beneficial type of scraper is a targeted advertiser. This is a company that aggregates large amounts of data in order to develop personalized advertising, which identifies and fills consumer demand.[24] A second example is a price aggregator; this is a company that parses data from a number of industry-specific websites, such as airline ticket websites, to create a cohesive comparison for consumers of the various price offerings on the Internet.[25] A third example is a personal finance management service like Mint.com or inDinero.com, which use scrapers to aggregate their consumers' banking information to allow users to track their spending and finances.[26] But scrapers

---

[21] Aaron Rubin & Tiffany Hu, *How Website Operators Use CFAA to Combat Data-Scraping*, LAW360 (Aug. 25, 2014, 10:01 AM), http://www.law360.com/articles/569325?utm_source=rss&utm_medium=rss&utm_campaign=articles_search [http://perma.cc/64WX-HFVY]. Sometimes scrapers are referred to as web site scrapers, content miners, web site rippers, web extractors, automated data collectors, or HTML scrapers. *What is a Screen Scraper?* WISEGEEK, http://www.wisegeek.com/what-is-a-screen-scraper.htm [http://perma.cc/TTV3-XKAL] (last visited Dec. 6, 2015).

[22] EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 579 (1st Cir. 2001).

[23] *See Software for Web Scraping*, WEB SCRAPING, http://scraping.pro/software-for-web-scraping/ [http://perma.cc/4Y3A-7V8Y] (last visited Dec. 6, 2015) (listing available web data extraction applications).

[24] *Id*.

[25] *See* Ticketmaster Corp. v. Tickets.Com, Inc., No. CV997654HLHVBKX, 2003 WL 21406289, at *2 (C.D. Cal. Mar. 7, 2003).

[26] *Mint. It's All Coming Together*, MINT, https://www.mint.com/how-mint-works [http://perma.cc/934M-2S7J] (last visited Dec. 6, 2015); *About inDinero*, INDINERO, https://indinero.com/about-indinero [http://perma.cc/LN76-6SLQ] (last visited Dec. 6,

can also be used harmfully. Harmful uses of scrapers differ from beneficial uses in at least two key ways. First, harmful scrapers amalgamate data that is *not* intended for public use, such as confidential information that was protected by a code barrier or other technological measure.[27] Second, in amalgamating nonpublic data, harmful scrapers directly harm the data host by diminishing the data host's website operability or severely undercutting its profits. If a scraper meets these two conditions, then the scraper is harmful even if the scraper's ultimate use benefits certain consumers. Such scrapers are also likely aggregating data in a manner that the CFAA would consider unlawful hacking. To understand how the CFAA conceptualizes hacking and whether scraping might constitute unlawful hacking, it is important to differentiate between various types of scrapers and to determine what, if any, damage they cause.

Whether scraping constitutes hacking is most unclear when the breached data is not protected by a technical barrier but is clearly unintended for public use. This was the situation in the widely publicized case *United States v. Auernheimer*.[28] In *Auernheimer*, which arose around the time that Apple first introduced the iPad, customers who wanted to send and receive data over cellular networks had to purchase a data contract from AT&T. Additionally, customers had to register their accounts with AT&T on a website that AT&T controlled. The customers were assigned a user identification (their email address) to access their accounts through AT&T's website. In order to make it easier for customers to log in to their accounts, AT&T programmed their servers to search for customers' identifiers based on the customers' unique URLs. The servers could then prepopulate the customers' login screens. Defendants Spitler and Auernheimer discovered AT&T's login configuration and wrote a scraper (what they called an "account slurper") to automatically access AT&T's website through different URLs and save all the different emails that AT&T generated in the login box. Through their scraper, Spitler and Auernheimer recorded 114,000 of AT&T's customers' email addresses.[29] Although technically, the email addresses were publicly accessible, AT&T designed them to be practically inaccessible unless an individual visited the correct, publicly available URL. The case was dismissed on venue grounds, and so

---

2015); Mary Wisniewski, *Is It Time to End Screen Scraping?*, AM. BANKER (Nov. 7, 2014), http://www.americanbanker.com/news/technology/is-it-time-to-end-screen-scraping-1071118-1.html [http://perma.cc/TH72-L4H9].

[27] *Ticketmaster Corp.*, 2003 WL 21406289, at *2.

[28] United States v. Auernheimer, 748 F.3d 525, 529-31 (3d Cir. 2014).

[29] *Id.* at 531.

the question of whether the defendants' scraper violated the CFAA remains open.[30]

This note analyzes the jurisprudence of federal scraping cases and places scraping within the broader framework of computer hacking prohibited under the CFAA. In doing so, this note clarifies when scraping constitutes hacking in violation of federal criminal law.

Part I provides an overview of data scraping and explains why it is both beneficial and harmful to society. Part II explains why the CFAA contains ambiguous language regarding the critical term "authorization." Part II explains how this drafting ambiguity has caused confusion about the application of the CFAA to scraping (resulting in a circuit split) and undermined the CFAA's effectiveness as an antihacking statute. Part III analyzes the jurisprudence of several CFAA scraping cases. It argues that those courts adopting a broad definition of the term authorization in the CFAA are creating further problems for the statute. A broad definition of authorization fails to distinguish between those types of data-accessing activities that are forbidden and those that are permissible. Therefore, it provides inadequate notice to scraper developers and users of when their conduct is unlawful. Part III also discusses how courts have applied the common law legal doctrine of trespass to chattels to scraping and utilized this doctrine as a tool to combat scrapers that directly harm competing businesses without breaking technical codes.

In conclusion, this note argues that only those scrapers that circumvent a technical code to access information that a data host clearly intended to block from public access should be liable under the CFAA. Only by limiting the CFAA's application to scraping in this manner will courts protect the statute's integrity and allow society to continue to reap the benefits of scrapers.

I. SCRAPING: THE BENEFITS AND THE HARMS

Scraping is the practice of extracting large amounts of data, usually from publicly available websites, through the use of scrapers.[31] Scrapers are computer programs with the ability to automatically compile Internet search results, filter for inappropriate content, and extract large amounts of data from public or private websites.[32] Generally, scrapers search through all the code in a website and filter out the extraneous data that is

---

[30] *Id.* at 540-41.

[31] Rubin & Hu, *supra* note 21.

[32] EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 579 (1st Cir. 2001).

merely in place for the website's aesthetic appeal.[33] After extracting the valuable data, scrapers present it in an easy-to-use format, such as graphs, tables, and indexes, which can be used for a variety of purposes.[34]

Businesses often hire experts to design sophisticated scrapers.[35] Due to the ease of acquiring and using scrapers, individuals often engage in scraping as well. Individuals can readily find scraping software through a simple Internet search.[36] Scrapers also have broad appeal due to their speed. They "can retrieve several pages on a server simultaneously" and "access target websites automatically thousands of times per day."[37] Scrapers can also translate various computer languages, such as HTML, JavaScript, or PHP.[38] Due to these capabilities, it is unsurprising that businesses and individuals prefer using scrapers to manually collecting data.

The websites from which scrapers collect data are called "data hosts."[39] Whether a scraper is beneficial or harmful depends in part on how much direct damage, if any, it causes to the data host. Certain scrapers, such as price amalgamators and targeted advertisers, cause minimal to no damage to data hosts and allow businesses to efficiently cater to consumer demands. Other scrapers cause extensive damage to data hosts. For example, if the data host and scraper user have competing businesses and the scraper user collects the data host's valuable data for its own competitive advantage, it may drive traffic away from the competitor's site and directly undercut the data host's revenue.[40]

It is important to distinguish between beneficial and harmful scraping because harmful scraping that damages data hosts by accessing confidential, technically protected information is the type of hacking that the CFAA was designed to deter. In order

---

[33] *What is a Screen Scraper?*, *supra* note 21.

[34] *Id.*

[35] *See, e.g.*, EF Cultural Travel, 274 F.3d at 579; Facebook, Inc. v. ConnectU LLC, 489 F. Supp. 2d 1087, 1089 (N.D. Cal. 2007).

[36] *See* Jeffrey Kenneth Hirschey, *Symbiotic Relationships: Pragmatic Acceptance of Data Scraping*, 29 BERKELEY TECH. L.J. 897, 904 (2014) ("A quick web search offers numerous options to scrape data: how-to guides about scraping, guidance in writing your own scraping program, and even options to purchase scraping software."); *see also* Rubin & Hu, *supra* note 21 ("Though sometimes difficult to combat, scraping is quite easy to perform. A simple online search will return a large number of scraping programs, both proprietary and open source, as well as DIY tutorials."); *What is a Screen Scraper?*, *supra* note 21.

[37] Marc S. Friedman & William T. Zanowitz, *The Invasion of the "Screen Scrapers"!*, 6 E-COMMERCE L. REP., May 2004, at 4.

[38] *What is a Screen Scraper?*, *supra* note 21.

[39] Hirschey, *supra* note 36, at 897.

[40] EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 583 (1st Cir. 2001). EF Cultural Travel and Explorica were competing businesses in the teenage tour market. Explorica designed a scraper to glean pricing information from EF's website. Explorica alleged that EF's scraping caused Explorica's business to suffer loss. *Id.*

to ensure that scraper users receive adequate notice and to protect beneficial scraping, only harmful scraping should be unlawful under the CFAA.

A. Beneficial Scraping

Internet users frequently interact with and benefit from scrapers. Common scrapers are search engines, business advertisers, auction compilers, price aggregators, real estate listing services, financial data aggregators, financial money management applications, social media sites, and even tools such as Google's PageRank.[41] Many of these devices scrape data hosts without causing them serious harm. In fact, operators of data hosts often do not know that their websites have been scraped[42] or are not troubled by scraping due to the benefits it provides them.[43] For instance, price amalgamators—such as airline ticket compilers— benefit consumers by helping them access more widespread data, but they also benefit data hosts by increasing their visibility.[44] Similarly, targeted advertisers parse through customers' stored content and personal data to cater to their specific interests.[45] Studies indicate that customers appreciate and rely on such scraping, which in turn helps businesses generate tremendous revenue.[46]

One of the best examples of a beneficial scraper is a search engine. Search engines constantly access thousands of websites and present data to end users in the form of easily readable search results.[47] Yet they usually pull only small amounts of data, such as the user's search terms, in order to link the user to relevant search results. Further, search engines only compile publicly available data; they do not break through password barriers in order to provide users private, protected data. Due to their universal appeal, search engines are considered "an

---

[41] "Google's ubiquitous PageRank algorithm is perhaps the largest scraping system and uses a web crawler called GoogleBot to scrape data from billions of webpages. This model is predicated upon unfettered access to data, and data hosts provide little resistance given the overwhelming benefit that they receive." Hirschey, *supra* note 36, at 897-98 (citation omitted).

[42] *Id.* at 898.

[43] *Id.* at 897-98.

[44] *Id.* at 921-22.

[45] William Jeremy Robison, *Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act*, 98 GEO. L.J. 1195, 1220-21 (2010).

[46] *Id.*

[47] *What is a Screen Scraper?*, *supra* note 21.

instrumental part of the online ecosystem."[48] Thus, Google's scraping activities are rarely found to be unlawful.[49]

Beneficial scrapers can also promote business efficiency by helping businesses pull data from various "keyword-related websites in order to generate graphs, charts, spreadsheets, and comparative data" in clean formats.[50] These displays help end users make reports and presentations in a fraction of the time that it would take if users had to extract data manually.[51] Additionally, scrapers can be useful when data is "stored on a system that can no longer be accessed due to compatibility issues with newer hardware or software."[52] This is because most scrapers can capture data that is no longer present on the live website but is available through a cache.[53] Because scraping can benefit businesses and consumers without harming data hosts, it is often considered a "blessing."[54] But scraping also has a darker side.

B. Harmful Scraping

In addition to beneficial scraping, there is a great deal of clandestine, harmful scraping. Harmful scrapers collect information that was not intended for public access and extensively harm data hosts. These scrapers steal and publish personal data from websites, collect and spam huge numbers of personal email accounts, and acquire protected, confidential company data in order to create competing websites. Data hosts usually suffer from "increased bandwidth usage, network crashes, the need to employ anti-spam and filtering technology, user complaints, reputational damage," and costs associated with mitigating the damage—all of which negatively impact the data host.[55]

Harmful scrapers also often collect information without the consent of data hosts. In many cases, the scrapers republish the scraped data on a different website, which in turn decreases consumer traffic on the original website and undercuts the data

---

[48] Hirschey, *supra* note 36, at 898.

[49] *See, e.g.*, Field v. Google Inc., 412 F. Supp. 2d 1106 (D. Nev. 2006) (granting summary judgment for Google where a data host sued Google, alleging that GoogleBots had unlawfully provided access to the data host's web content through Google's search engine results); *see also In re* Google Android Consumer Privacy Litig., No. 11-MD-02264 JSW, 2013 WL 1283236 (N.D. Cal. Mar. 26, 2013) (granting Google's motions to dismiss under the CFAA and trespass to chattels where Google's aggregate collection of geolocation data from cell phone applications did not significantly harm the functioning of the cell phone systems).

[50] *What is a Screen Scraper?*, *supra* note 21.

[51] *Id.*

[52] *Id.*

[53] *Id.*; *What is a Browser Cache?*, PC TOOLS, http://www.pctools.com/security-news/what-is-a-browser-cache/ [http://perma.cc/4CDM-SMEN] (last visited Dec. 6, 2015).

[54] *What is a Screen Scraper?*, *supra* note 21.

[55] Rubin & Hu, *supra* note 21.

host's revenue.[56] Additionally, in these instances, the owners of data hosts may not know until later that content from their original website was used elsewhere and may feel that their original work was distorted, compromising their reputations.[57] Such scraping can also implicate free speech and copyright issues.[58] Finally, harmful scrapers might also collect personally identifiable information, which implicates privacy issues[59] and often upsets the data hosts' membership base.[60]

Another example of a harmful scraper is one designed to automatically con people out of money. These types of scrapers were the subject of a recent case in which the Federal Trade Commission charged operators of Jerk.com for scraping personal information from Facebook to create profiles that labeled people as "jerk" or "not a jerk."[61] The operators of Jerk.com then falsely told more than 73 million consumers, including children, that they could revise their online profiles by paying $30.[62] Another example is from *United States v. TomorrowNow Inc.*, where a scraper extracted confidential support materials from Oracle's restricted-access Customer Connection website in order to sway customers of Oracle's

---

[56] "[S]ites that depend on advertising to generate revenue have problems when their ads are being discarded by the screen scraper." *What is a Screen Scraper?*, *supra* note 21; *see also* eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1061-62 (N.D. Cal. 2000). Bidder's Edge was a scraper that scraped eBay's auction listings and even copied the auction format on its own website without incurring any of the investment or operating costs that eBay incurs. Then eBay claimed that Bidder's Edge caused it to suffer damages from: "(1) lost capacity of [eBay's] computer systems . . . ; (2) damage to eBay's reputation and goodwill caused by BE's misleading postings; (3) dilution of the eBay mark; and (4) BE's unjust enrichment." *Id.* at 1064.

[57] *See, e.g.*, *Bidder's Edge*, 100 F. Supp. 2d at 1063.

[58] *See What is a Screen Scraper?*, *supra* note 21 ("Copyright issues become blurry when a screen scraper extracts someone's hard work and presents it in another format for another website . . . ."); George H. Fibbe, *Screen-Scraping and Harmful Cybertrespass after* Intel, 55 MERCER L. REV. 1011, 1012 (2004).

[59] Hirschey, *supra* note 36, at 899; *see, e.g.*, *In re* Google Android Consumer Privacy Litig., No. 11-MD-02264 JSW, 2013 WL 1283236, at *2 (N.D. Cal. Mar. 26, 2013). Plaintiffs filed suit alleging "that the Google Defendants used code hidden in Apps . . . to collect personally identifiable information [], including Plaintiffs' name, gender, zip code, App activity (including search terms or selections), geolocation data, and their phones' universally unique device identifiers . . . without providing proper notice" or obtaining consent. *Id.* (internal citation omitted).

[60] In March 2014, LinkedIn filed an amended complaint against Robocog for the alleged harm it caused when it scraped LinkedIn and copied the profiles of various LinkedIn members without their permission. *See* Parties' Joint Case Management Statement at 1, LinkedIn Corp. v. Robocog Inc., No. C14-00068 (N.D. Cal. May 1, 2014), ECF No. 22, 2014 WL 2444973.

[61] *FTC Charges Operators of "Jerk.com" Website with Deceiving Consumers*, FED. TRADE COMMISSION (Apr. 7, 2014), http://www.ftc.gov/news-events/press-releases/2014/04/ftc-charges-operators-jerkcom-website-deceiving-consumers [http://perma.cc/C9GL-4GSF].

[62] *Id.*

PeopleSoft products away from Oracle.[63] When scrapers are intentionally used to defraud and harm data hosts, consumers, and general Internet users, criminal liability is appropriate.

C. Scraping Litigation

In recent years, the number of lawsuits involving scrapers has increased. A primary reason for this increase is that many websites are ill equipped to combat harmful scraping. Since websites are usually designed to be easy to use, their format benefits scrapers. Additionally, the diversity of available scrapers makes it difficult for data hosts to fully anticipate and prevent data scraping.[64] Even when websites are formatted in code that might be "gibberish" to an uninformed reader, they are still susceptible to sophisticated scrapers.[65]

In 2013, web scraping accounted for over 10% of site visitors and more than 20% of all Internet traffic.[66] Such figures indicate that scraping litigation related to hacking will continue to increase. Since scraping did not exist when the CFAA was first enacted, and because scraper users have been sued under the CFAA, it is important to understand the history and provisions of the CFAA in order to understand when scraping should be a crime under the act.

II. THE CFAA: A POTENT ANTIHACKING STATUTE

A. Historical Context of the CFAA

Congress enacted the first version of the CFAA in 1986 at a time when personal computers were only beginning to populate the workplace as stores for valuable information.[67] At the time, the media depiction of computer culture, such as the 1983 film *War Games*,[68] led to Congress's conception of a hacker

---

[63] *SAP to Pay $20 Million Criminal Fine in "Web Scraping" Case*, 24 WESTLAW J. SOFTWARE L., No. 12 , 2011, at 6.

[64] Hirschey, *supra* note 36, at 904.

[65] EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 583 (1st Cir. 2001).

[66] Rubin & Hu, *supra* note 21.

[67] Glenn R. Schieck, *Undercutting Employee Mobility: The Computer Fraud and Abuse Act in the Trade Secret Context*, 79 BROOK. L. REV. 831, 831-32 (2014) (citing Greggory S. Blundell, *Personal Computers in the Eighties*, BYTE (Jan. 1983), http://archive.org/stream/byte-magazine-1983-01/1983_01_BYTE_08-01_Looking_Ahead#page/n175/mode/2up [http://perma.cc/ZV2Y-KEQS] (During "the late 1970's and early 1980's . . . [n]ew managers entering the business community brought with them a keen awareness of computer systems gained from both college study and home use.")).

[68] Laura Bernescu, *When Is a Hack Not a Hack: Addressing the CFAA's Applicability to the Internet Service Context*, 2013 U. CHI. LEGAL F. 633, 637 (2013);

as "'a bright, intellectually curious, and rebellious youth,' who could 'become the white-collar crime superstar of tomorrow.'"[69]

Because the CFAA drafters did not know how the digital landscape would develop when they drafted the statute, the CFAA was amended numerous times between 1990 and 2001. Its widest expansion was in 1994, when Congress established a private right of action for individuals harmed by certain violations of the CFAA.[70] This allows a private party "'who suffers damage or loss by reason or violation of [the statute]' to bring a civil action 'to obtain compensatory damages and injunctive relief or other equitable relief.'"[71] Thus, it exposes a violator of the CFAA to civil and criminal liability.

In order to be exposed to civil liability, a violator's action must meet at least one of six additional factors listed in the statute.[72] These include: "loss . . . aggregating to at least $5,000 in value,"[73] "the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals,"[74] "physical injury to any person,"[75] "a threat to public health or safety,"[76] "damage affecting a computer used by or for . . . the United States Government in furtherance of the administration of justice, national defense, or national security,"[77] or "damage affecting 10 or more protected computers during any 1-year period."[78]

Joseph M. Olivenbaum, *<Ctrl>-<Alt>-<Delete>: Rethinking Federal Computer Crime Legislation*, 27 SETON HALL L. REV. 574, 582 (1997).

[69] Schieck, *supra* note 67, at 831.

[70] Computer Abuse Amendments Act of 1994, Pub. L. No. 103-322, 108 Stat. 1796, 2098.

[71] WEC Carolina Energy Sols. LLC v. Miller, 687 F.3d 199, 201 (4th Cir. 2012), *cert. dismissed*, 133 S. Ct. 831 (2013) (quoting 18 U.S.C. § 1030(g)).

[72] Computer Fraud and Abuse Act, 18 U.S.C. § 1030(c)(4)(A)(i)(I)-(VI) (2012).

[73] *Id.* § 1030(c)(4)(A)(i)(I). Notably, the $5,000 loss provision itself is not too difficult to reach, because § 1030(e)(11) defines the loss provision such that it includes efforts by a company to fix the damage.

> [T]he term 'loss' means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.

Id. § 1030(e)(11).

[74] *Id.* § 1030(c)(4)(A)(i)(II).

[75] *Id.* § 1030(c)(4)(A)(i)(III).

[76] *Id.* § 1030(c)(4)(A)(i)(IV).

[77] *Id.* § 1030(c)(4)(A)(i)(V).

[78] *Id.* § 1030(c)(4)(A)(i)(VI).

B. Relevant Statutory Provisions

Many computer hacking crimes brought under the CFAA arise under sections 1030(a)(2) and 1030(a)(4). Section 1030(a)(2), which is the broadest provision of the statute, makes it a crime when a person

> intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—(A) information contained in a financial record of a financial institution . . . (B) information from any department or agency of the United States; or (C) information from any protected computer.[79]

Section 1030(a)(4) has a narrower focus on fraudulent activity and makes it a crime when a person

> knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period.[80]

While the language of section1030(a)(4) is similar to that of 1030(a)(2), section 1030(a)(4) has the added requirement that the offender have the specific intent to defraud and further the intended fraud by causing a loss of value of at least $5,000 through his/her use.[81] Data-breaching crimes also arise under section 1030(a)(5), which penalizes one who:

> (A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer; (B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or (C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.[82]

Finally, section 1030(g) covers the civil liability expansion when the offender's actions also meet one of the six elements set out in sections 1030(c)(4)(A)(i)(I)-(V).[83]

---

[79] *Id.* § 1030(a)(2)(A)-(C).
[80] *Id.* § 1030(a)(4).
[81] *Id.*
[82] *Id.* § 1030(a)(5)(A)-(C).
[83] *Id.* § 1030(g), (c)(4)(A)(i)(I)-(V).

C. Ambiguity in Critical Language of Authorization

Sections 1030(a)(2), 1030(a)(4), and 1030(a)(5) all include either the phrase: "without authorization" or "exceeds authorized access." The phrase "exceeds authorized access" is defined in the statute as: "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled to so obtain or alter." Although this definition establishes that unauthorized computer access constitutes hacking, problematically, the word "authorized" is never defined. Consequently, circuits have interpreted the term "authorization" differently depending on the context of the case; as a result, the statute has not been consistently interpreted.[84]

It is important to understand the circuit split regarding the meaning of authorization because the statute carries serious penalties.[85] The split is particularly relevant in scraping cases because the factors that motivated certain circuits to adopt a broad view of what constitutes authorization are not implicated in scraping cases. These broad definitions of authorization were formed in the context of cases involving unfair competition, trade secret misappropriation, threats to individuals' privacy and security, and other legal wrongs—crimes that are inherently different from scraping.

Additionally, allowing courts to apply a broad definition of authorization fails to provide users of scrapers with adequate notice of when they are violating criminal law. Because there are many beneficial scrapers that do not harm data hosts or consumers, adopting a broad view of authorization would cast too much uncertainty on whether scraping is authorized and would

---

[84] Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1596 (2003); *see, e.g.*, United States v. Nosal, 676 F.3d 854, 864 (9th Cir. 2012) (en banc) (holding that the phrase "exceeds authorized access" is limited to *access* restrictions, not *use* restrictions). *But see* Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1125, 1129 (W.D. Wash. 2000) (holding that Shurgard lost authorization and breached the CFAA when he became an agent of a direct competitor and used his employer's proprietary information in a way that damaged his employer).

[85]

> (1)(A) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and
>
> (B) a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph . . . .

Computer Fraud and Abuse Act, 18 U.S.C. § 1030(c) (2012).

thereby deter beneficial scraping. Thus, in order to ensure that only those engaged in harmful scraping are punished, the scope of authorization must be based on the narrow view that only technical breaches violate the CFAA.[86]

1. Narrow View of Authorization

The Fourth and Ninth Circuits have adopted a narrow definition of authorization.[87] In the seminal case *United States v. Nosal*, employees of an executive search firm used their access to the employer's database to obtain and pass along confidential company information to a former employee whom they knew was trying to set up a competing business. The Ninth Circuit held that because the current employees had logged into the firm database with their valid credentials, they had proper authorization and had not violated the CFAA, even though their ultimate *use* of the information was inconsistent with the purpose for which they had been granted access. In determining that the phrase "exceeds authorized access" did not extend to violations of *use* restrictions,[88] the opinion referred to the original Senate Reports that discussed how computer hacking was akin to intentional trespass.[89]

The court did not foreclose the possibility that hackers could be inside employees. Rather, it interpreted the phrase "without authorization" as designed to apply to *outside* hackers who have no authorized access to a computer and the phrase "exceeds authorized access" to apply to *inside* hackers "whose initial access to a computer is authorized but who access unauthorized information or files."[90] Thus, the court's focus was on the *technical* means by which data was obtained. Insiders would be hackers only if they obtained data to which they did not have precise access, even if they had access to the broader network where such data was stored.

---

[86] A technical breach is one that violates a code barrier, such as a password.

[87] *Nosal*, 676 F.3d at 864 (holding that the phrase "exceeds authorized access" is limited to *access* restrictions, not *use* restrictions); WEC Carolina Energy Sols. LLC v. Miller, 687 F.3d 199, 206 (4th Cir. 2012), *cert. dismissed*, 133 S. Ct. 831 (2013); LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1137 (9th Cir. 2009).

[88] "Therefore, we hold that 'exceeds authorized access' in the CFAA is limited to violations of restrictions on *access* to information, and not restrictions on its *use*." *Nosal*, 676 F.3d at 863-64.

[89] "[I]ntentionally trespassing into someone else's computer files, the offender obtains at the very least information as to how to break into that computer system." *Id.* at 858 (citing S. REP. No. 99-432, at 9 (1986) (Conf. Rep.)).

[90] *Nosal*, 676 F.3d at 858.

The court found that only a narrow interpretation of authorization comported with the plain meaning of the statute.[91] It stated that any other meaning would turn a serious federal criminal hacking statute into a "sweeping Internet-policing mandate"[92] and would displace a substantial portion of the common law.[93] The court was also concerned with the rule of lenity.[94] This rule of statutory interpretation states that in construing a criminal statute that contains an ambiguity, after "seizing everything from which aid can be derived," courts ought to resolve the ambiguity in favor of the defendant so that they do not "penalize those whose conduct does not create the risks of harm at which the statute aims."[95] Using the rule of lenity, the court in *Nosal* found that unless it interpreted authorization narrowly, it would "make criminals of large groups of people who would have little reason to suspect they are committing a federal crime."[96] The same concerns with notice and lenity apply to scraper users, particularly when the scrapers are beneficial and the users' conduct is not what the statute aims to deter.

---

[91] "This is a perfectly plausible construction of the statutory language that maintains the CFAA's focus on hacking rather than turning it into a sweeping Internet-policing mandate." *Nosal*, 676 F.3d at 858. The court arrived at a similar holding three years earlier in *LVRC Holdings LLC v. Brekka*, which also involved a rogue employee who misappropriated company information for his own purposes. Again the court found that under the plain meaning of the statute, Brekka did not violate the CFAA, as he had access to the information and was therefore not "without authorization." *LVRC Holdings*, 581 F.3d at 1137.

[92] *Nosal*, 676 F.3d at 858.

[93] "Under the presumption that Congress acts interstitially, we construe a statute as displacing a substantial portion of the common law only where Congress has clearly indicated its intent to do so." *Id.* at 857.

[94]

> If Congress wants to incorporate misappropriation liability into the CFAA, it must speak more clearly. The rule of lenity requires penal laws . . . to be construed strictly. [W]hen choice has to be made between two readings of what conduct Congress has made a crime, it is appropriate, before we choose the harsher alternative, to require that Congress should have spoken in language that is clear and definite.

Id. at 863 (internal citations and quotations omitted).

[95] Muscarello v. United States, 524 U.S. 125, 138-39 (1998).

[96]

> While it's unlikely that you'll be prosecuted for watching Reason.TV on your work computer, you *could* be. Employers wanting to rid themselves of troublesome employees without following proper procedures could threaten to report them to the FBI unless they quit. Ubiquitous, seldom-prosecuted crimes invite arbitrary and discriminatory enforcement.

Id. at 859-60 (footnote omitted).

2. Broad View of Authorization

In contrast to the Fourth and Ninth Circuits, the First, Fifth, and Eleventh Circuits have adopted broad definitions of authorization.[97] This is largely because the addition of the CFAA's civil liability provision has encouraged employers to increasingly use section 1030(g) to bring disloyal employees into federal court. Further, now that companies store the bulk of their information digitally, rather than in filing cabinets and safes, employers use the civil liability provisions to sue employees who access and misuse such information. The First, Fifth, and Eleventh Circuits have creatively adapted agency, duty of loyalty, and contract theories, and created use-based theories, in order to find CFAA liability in such instances.

a. Duty of Loyalty/Agency Theory

The duty of loyalty theory provides that authorization implicitly ends as soon as an employee becomes disloyal to his/her employer, even if he or she still has technical authorization. Thus, in *Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*, a district court in the Western District of Washington held that Shurgard lost authorization and breached the CFAA when he became an agent of a direct competitor and used his employer's proprietary information in a way that was adverse to his employer's interests.[98] Similarly, in *International Airport Centers v. Citrin*, the court held that an employee exceeded authorized access and therefore violated the CFAA when, after deciding to go into business for himself, he erased certain programs belonging to his former employer to which he still had access.[99]

b. Contract Theory

The contract-based understanding of authorization provides that if an individual acquires or utilizes information in breach of a written policy, such as a confidentiality agreement, workplace rules of conduct, or a terms-of-service

---

[97] *See, e.g.*, United States v. Czubinski, 106 F.3d 1069, 1078-79 (1st Cir. 1997); United States v. John, 597 F.3d 263, 271 (5th Cir. 2010); United States v. Rodriguez, 628 F.3d 1258, 1261-63 (11th Cir. 2010).

[98] Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1125, 1129 (W.D. Wash. 2000).

[99] Once the employee breached his duty of loyalty to the company, he terminated the agency relationship and "with it his authority to access the laptop, because the only basis of his authority had been that relationship." Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 420-21 (7th Cir. 2006).

agreement, then even technically authorized use constitutes unauthorized use under the CFAA.[100] In *EF Cultural Travel BV v. Explorica, Inc.*, a case in which the teenage tour company EF Cultural Travel sued its competitor, Explorica, the First Circuit held that Explorica violated the CFAA when it used a scraper to glean information from EF Cultural Travel.[101] In that case, the vice president of Explorica directed his company to hire an expert to design a scraper that would automatically glean EF Cultural Travel's pricing information from its website.[102] Because the vice president of Explorica previously worked at EF Cultural travel and had signed a confidentiality agreement with Explorica, the court reasoned that Explorica's use of the scraper breached this confidentiality agreement, and as such, exceeded authorization under the CFAA.[103]

c. "Intended Use" Theory

The Fifth and Eleventh Circuits have both employed what they call an "intended use" theory. Under this theory, courts look at the underlying purpose of certain company policies to determine whether an employee breached or exceeded technically authorized access. The analysis is similar to the contract theory, but can be broader, as it considers how employees *used* the information they obtained even if those employees did not directly breach a written policy or contract.

One example of a case where this theory was adopted is *United States v. John*.[104] There, the Fifth Circuit held that an employee violated the CFAA when she used data from Citigroup's internal computer system to obtain customer account information, which she then shared with a third party in order to engage in

---

[100]

> The owner can condition use of the computer on a user's agreement to comply with certain rules. If the user has a preexisting relationship with the owner/operator, the conditions may take the form of Terms of Service. If no such relationship exists, the conditions may appear as Terms of Use to the service the computer provides, such as a click-through agreement that might appear prior to use of a website. For example, an adult website may require a user to promise that she is at least eighteen years old before allowing her to access adult materials available through the website. Finally, the restriction may be implicit rather than stated in the written text.

Kerr, *supra* note 84, at 1645-46.

[101] EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 578 (1st Cir. 2001).

[102] *Id.* at 579-84.

[103] *Id.*

[104] United States v. John, 597 F.3d 263, 269 (5th Cir. 2010).

fraudulent activity.[105] The court stated that such use was not what the company intended when it granted her access.[106] Similarly, in *United States v. Rodriguez*, the Eleventh Circuit held that an employee of the United States Social Security Administration violated the CFAA when, in violation of the agency's broad policy against obtaining information for nonbusiness purposes, he obtained confidential personal information from the agency's computers that included: the social security numbers, birthdates, income, and home addresses of his ex-wife, ex-girlfriend, coworkers, and other acquaintances.[107]

The duty of loyalty, contract, and intended use theories have certain differences; however, they each represent an example of how circuits have supported a broad interpretation of authorization under the CFAA in order to include breaches of data that were not technical. Predictably, there are problems with circuits employing different theories to interpret the term authorization in the context of scraping, especially since the CFAA contains civil and criminal provisions, which create concerns about notice and deterrence.

3. General Problems With the Interpretation of Authorization and Why the Narrow Approach Must Apply to Scraping Cases

The circuit split over critical language in the CFAA is problematic for both the judiciary and the citizenry. Professor Orin Kerr attributes the circuits' varying interpretations of authorization under the CFAA to the courts' focus on "results-oriented outcomes."[108] He believes that "[w]hen computer misuse caused harm to a victim in some way," courts tended to conclude that the victims were deprived of some property right and would find reasons to hold the defendants liable.[109] But "[w]hen no appreciable harm resulted, courts tended to . . . hold that the defendants committed no crime."[110] He argues that although many of those decisions have "rough appeal," when analyzed on a case-by-case basis, invoking various common law theories derails

---

[105] *Id.* at 272. "John accessed account information for individuals whose accounts she did not manage, removed this highly sensitive and confidential information from Citigroup premises, and ultimately used this information to perpetrate fraud on Citigroup and its customers." *Id.*

[106] *Id.* at 271 (stating that John's use of Citigroup's computer system to perpetrate a fraud was also contrary to Citigroup's employee policies, of which she was aware).

[107] United States v. Rodriguez, 628 F.3d 1258, 1260-62 (11th Cir. 2010).

[108] Kerr, *supra* note 84, at 1611.

[109] *Id.*

[110] *Id.*

the integrity of the CFAA as an antihacking statute that is based on theories of criminal theft, fraud, and trespass. Professor Kerr's characterization of the circuits' results-oriented outcomes helps explain their varying approaches. And often, when the cases are analyzed individually, their results appear reasonable. But the circuit split ultimately prevents the judiciary from establishing a cohesive jurisprudence regarding the concept of authorization under the CFAA. The problems with this statutory incoherence will only amplify as hacking becomes more sophisticated.

Inconsistent interpretations of key language in the CFAA are highly problematic because they can induce noncompliance with congressional intent, displace the common law, abuse federal jurisdiction, and violate the rule of lenity. Of these, the biggest problem is insufficient notice, because potential offenders ought to know when their seemingly harmless conduct may subject them to serious criminal penalties. Further, because the rule of lenity mandates that when a statute is ambiguous, courts should resolve the ambiguity in favor of the defendant, courts should cure the ambiguity in the statute now so that they will not have to resort to this rule when public safety concerns and the need to deter dangerous cybercriminals arise.

The Fourth Circuit discussed at length how the rule of lenity was implicated in *WEC Carolina Energy Solutions*.[111] In that case, a former employee of WEC made a presentation to a potential customer, incorporating proprietary information that he had gained from his former employer before leaving.[112] The Fourth Circuit held that he did not violate the CFAA.[113] The court stated that in the interest of providing "fair warning" to potential offenders, one had to "construe this criminal statute strictly and avoid interpretations not 'clearly warranted by the text.'"[114] The court also stressed that individuals must know "what the law intends to do if a certain line is passed."[115] This is critical when the line is paper thin, as it is in the CFAA.

Similarly, in *Nosal*, the Ninth Circuit Chief Judge Kozinski recognized that employees frequently procrastinate, unaware that their seemingly innocuous conduct breaches federal computer crime laws. He stated, "Minds have wandered since the beginning of time and the computer gives employees new ways to

---

[111] WEC Carolina Energy Sols. LLC v. Miller, 687 F.3d 199, 204 (4th Cir. 2012), *cert. dismissed*, 133 S. Ct. 831 (2013).

[112] *Id.* at 202.

[113] *Id.* at 204.

[114] *Id.* (citing Crandon v. United States, 494 U.S. 152, 160 (1990)).

[115] *WEC Carolina Energy Sols.*, 687 F.3d at 204 (citing Babbitt v. Sweet Home Chapter of Cmtys. for a Great Or., 515 U.S. 687, 704 n.18 (1995)).

procrastinate, by g-chatting with friends, playing games, shopping or watching sports highlights."[116] He emphasized that even if employees are seldom disciplined for such frivoling, under the broad interpretation of the CFAA, whenever a company has a policy against such actions, harmless dalliances could become federal crimes, and thus, "[e]mployers wanting to rid themselves of troublesome employees . . . could threaten to report them to the FBI unless they quit."[117] He warned that "[u]biquitous, seldom-prosecuted crimes invite arbitrary and discriminatory enforcement."[118] Indeed, enabling employers to get rid of delinquent employees with the threat of criminal sanctions contravenes the express purpose of the CFAA. It also defies the spirit of American criminal jurisprudence, which admonishes arbitrary and discriminatory law enforcement, especially when employees are unaware of their violations.

The Ninth Circuit reasonably recognized that in modern times, employees use computers for a number of purposes that, while not conducive to their jobs, do not directly harm employers. Because the Ninth Circuit wanted to ensure that procrastinating employees are not needlessly swept under the ambit of a powerful criminal statute, it interpreted authorization narrowly, requiring that there be a code breach before employees could be liable for violating the CFAA. The same reasoning must apply to scraping so that those operating scrapers know when their actions violate the CFAA.

The need for adequate notice is arguably more pressing in the scraping context than in the employment context. Most employment cases that arise under the CFAA involve a current or former employee who misappropriated trade secrets or violated a confidentiality agreement, both of which are still unlawful actions. But many beneficial scrapers have not violated any law. Thus, when CFAA suits are brought against

---

[116] United States v. Nosal, 676 F.3d 854, 860 (9th Cir. 2012) (en banc).

[117] *Id.*

[118] *Id.* As Chief Judge Kozinski further noted,

> Suppose an employee spends six hours tending his FarmVille stable on his work computer. The employee has full access to his computer and the Internet, but the company has a policy that work computers may be used only for business purposes. The employer should be able to fire the employee, but that's quite different from having him arrested as a federal criminal. Yet under the government's construction of the statute, the employee "exceeds authorized access" by using the computer for non-work activities. Given that the employee deprives his company of six hours of work a day, an aggressive prosecutor might claim that he's defrauding the company, and thereby violating section 1030(a)(4).

Id. at 860 n.7.

such scrapers, the CFAA is not being used in place of another charge; rather, it is being used to condemn Internet activity that is perfectly permissible.

In cases with harmful scrapers where the user did not breach a code but still seriously damaged a data host, there may be an adequate remedy in the common law doctrine of trespass to chattels. Because different remedies are available under various laws, it is important to understand why courts increasingly require a code or technical breach for scraping to violate CFAA. Additionally, it is crucial to understand that a code-based requirement will not leave data hosts that do not erect code barriers without legal recourse, as many harmful scraper users can still be liable under the common law doctrine of trespass to chattels. Thus, it is important to see how trespass to chattels can provide data hosts with remedies in some scraping cases.

III. SCRAPING, THE CFAA, AND TRESPASS TO CHATTELS

A. Scraping and the CFAA: The Journey Towards a Code Requirement

In recent CFAA litigation, courts have shifted their focus from contractual theories of liability to technical theories of liability. More courts now embrace a code-based requirement to find scrapers liable under the CFAA. This is partly due to the realization that a code-based requirement effectively deters the use of harmful scrapers, which Congress likely intended to proscribe, and it protects users of beneficial scrapers who do not know that they could be violating criminal law.

1. Early Days: No Code Requirement

A good place to begin an analysis of scraping claims brought under the CFAA is by looking at the 2001 case *EF Cultural Travel BV v. Explorica, Inc.*[119] There, employees who initially worked for EF Cultural Travel when it was one of the world's largest teenage tour organizations went to work for Explorica when it later entered the teenage tour market.[120] To try and gain a competitive advantage over EF Cultural Travel, the vice president of Explorica (a former EF Cultural Travel employee) hired an Internet consultant to design a scraper that

[119] EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577 (1st Cir. 2001).
[120] *Id.* at 579.

could glean pricing information from EF Cultural Travel's website.[121] Explorica then used the scraped information to undercut EF Cultural Travel's prices.[122] The district court and the First Circuit approved an injunction against Explorica.[123] Yet neither court was concerned with how the scraper technically operated.[124] Although the scraper was custom designed by a technical expert who relied on unique knowledge from a former EF Cultural Travel employee, was able to decode EF Cultural Travel's website's information that the public could not interpret, and systematically undercut EF Cultural Travel, the First Circuit found Explorica liable because, in designing the scraper, the former employee breached a confidentiality agreement that he had previously signed with EF Cultural Travel.[125] The court stated, "because of the broad confidentiality agreement appellants' actions 'exceed[ed] authorized access,' and so we do not reach the more general arguments made about statutory meaning, including whether use of a scraper alone renders access unauthorized."[126]

In *EF v. Explorica*, the court avoided discussing how scraping related to authorization and instead focused on the clear contract violation.[127] When the auxiliary case, *EF Cultural Travel BV v. Zefer*,[128] came up two years later, however, the problems with relying on a contract-based definition of authorization became apparent. Arising from the same set of events as *EF v. Explorica*, in *EF v. Zefer*, the defendant (Zefer) was the independent company that made the scraper that Explorica used to scrape EF Cultural Travel.[129] But because Zefer was not subject to any confidentiality agreement with Explorica, the court could not find an independent basis for Zefer's liability and narrowly upheld EF Cultural Travel's injunction against Zefer on the ground that Zefer was EF Cultural Travel's software maker.[130]

EF v. Zefer nicely illustrates the danger of reliance on a contract theory for liability because in any situation where a user or designer of a scraper is not bound by a direct contract with the data host, a court may not be able to find CFAA liability based on the *motive* with which the scraper is used.

---

121 *Id.*
122 *Id.* at 580.
123 *Id.* at 578-79.
124 *Id.* at 581-82.
125 *Id.*
126 *Id.*
127 *Id.* at 582.
128 EF Cultural Travel BV v. Zefer Corp., 318 F.3d 58 (1st Cir. 2003).
129 *Id.* at 58.
130 *Id.* at 64.

But the CFAA is a criminal statute that requires assessing a violator's mens rea. Thus, a criminal liability theory that circumvents the questions of how and why a scraper was used does not accord with criminal liability jurisprudence that requires specific intent.

2. Movement Towards a Code Requirement

Two similar cases, both involving Facebook, illustrate why, over time, courts required more than a contractual breach for scraping liability. In 2007, Facebook brought a claim against ConnectU LLC, alleging that ConnectU violated the CFAA by designing a scraper that collected millions of email addresses that were available to registered users of Facebook but not to the general public.[131] Facebook argued that the scraper violated Facebook's terms and conditions of use, which specifically prohibited users from collecting, copying, and using data found on its site without Facebook's permission.[132] ConnectU argued that since registered users voluntarily supplied their information to Facebook, its scraper had authorization to collect that information.[133] It also argued that it would be dangerous to allow a criminal standard to depend on terms that private parties set at their discretion.[134] The court, unpersuaded by both of ConnectU's arguments, found ConnectU liable under the CFAA.[135] It stated that the *statute* defines criminal offenses and that private parties only set the conditions upon which they grant authorization.[136]

The second Facebook case, *Facebook, Inc. v. Power Ventures, Inc.*, arose three years later in the same jurisdiction.[137] In that case, Facebook alleged that Power Ventures violated California Penal Code section 502, California's analogue to the CFAA, when Power Ventures used a scraper to access Facebook's website in violation of Facebook's Terms of Service.[138] This time, however, Facebook also alleged that the scraper violated several "cease and desist"

---

131 Facebook, Inc. v. ConnectU LLC, 489 F. Supp. 2d 1087, 1089 (N.D. Cal. 2007).

132 *Id.* at 1091.

133 *Id.*

134 *Id.*

135 *Id.*

136 *Id.*

137 Facebook, Inc. v. Power Ventures, Inc., No. C 08-05780 JW, 2010 WL 3291750 (N.D. Cal. July 20, 2010).

138 *Id.* at *7. Facebook's terms of use state: "[A Facebook user may] not collect users' content or information, or otherwise access Facebook, using automated means (such as harvesting bots, robots, spiders, or scrapers) without [Facebook's] prior permission." *Terms of Service*, FACEBOOK (Jan. 30, 2015), https://www.facebook.com/legal/terms [http://perma.cc/HPC3-84XT].

orders[139] and bypassed special *technical* barriers.[140] The court, relying on case law interpreting the CFAA, held that the scraper "did not act 'without permission' within the meaning of section 502."[141] Unlike its reasoning three years earlier in *Facebook, Inc. v. ConnectU LLC*, this time, the court discussed how imposing criminal liability on the basis of terms of use or a cease and desist letter would grant the data host the ability to define the scope of federal criminality, which it found "constitutionally untenable."[142]

In *Power Ventures*, the court was concerned with exactly what *ConnectU* had previously warned about—that a contract-based concept of authorization would effectively allow private parties to determine the scope of criminal liability. The court did note that to the extent that Facebook could prove that Power Ventures circumvented *technical* barriers, it could be liable for violating the statute.[143] In doing so, the court recognized that a key consideration for finding that a scraper's use exceeded authorization would be whether the scraper overcame a technical barrier.

Although Facebook lacked proof of a technical breach in both cases, in the second case, the court discussed the importance of a technical standard at length. It stated how access that violates a code barrier crosses a clear demarcation that the administrator has erected "to restrict the user's privileges within the system, or to bar the user from the system altogether."[144] The court further explained that when "a user gains access to a computer, computer network, or website" by overcoming technical barriers, the user has "eliminate[d] any constitutional notice concerns, since a person applying the technical skill necessary to overcome such a barrier will almost always understand that any access gained through such action

---

139 *Facebook, Inc. v. Power Ventures*, 2010 WL 3291750, at *10-11.

140 *Id.* at *5.

141 *Id.* at *12.

142

> By granting the computer owner essentially unlimited authority to define authorization, the contract standard delegates the scope of criminality to every computer owner. Users of computer and internet services cannot have adequate notice of what actions will or will not expose them to criminal liability when a computer network or website administrator can unilaterally change the rules at any time and are under no obligation to make terms of use specific or understandable to the general public.

Id. (citing Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1650-51 (2003)).

143 *Id.* at *12.

144 Facebook, Inc. v. Power Ventures, Inc., No. C 08-05780 JW, 2010 WL 3291750, at *11 (N.D. Cal. July 20, 2010).

is unauthorized."[145] The court correctly reasoned that such an instance is appropriate for criminal liability because if a scraper user utilized special knowledge to bypass a code barrier, it implies that the user intended to access an unauthorized source of information. Consequently, the court stated, "accessing or using a computer, computer network, or website in a manner that overcomes technical or code-based barriers is 'without permission,' and may subject a user to liability."[146]

These cases show why a technical breach requirement for CFAA liability would resolve important notice concerns. The requirement would ensure that regardless of the wording of data hosts' individual terms of service agreements and cease and desist letters, data hosts would at most only shape contractual liability. Criminal liability under the CFAA would only arise when a scraper user breaches a technical barrier with the knowledge that the user did not have authorization.

3. Emergence of a Code-Based Requirement

Two fairly recent scraping cases illustrate the trend of courts requiring a code-based breach to establish CFAA liability. The first is a 2010 case entitled *Cvent, Inc. v. Eventbrite, Inc.*[147] In that case, Cvent, an event-planning company, alleged that Eventbrite designed and used a scraper to collect information from Cvent's website, reformat it, and post it as its own.[148] Cvent asserted that the scraping deprived it of its monetary investment in the website and led to lost profits.[149] Eventbrite responded that because Cvent's website was publicly available on the Internet and did not require any login, password, or individualized grant of access, by definition, Eventbrite could not have exceeded its authority to access Cvent's data.[150] While Cvent did have a terms of use agreement that prohibited competitors from accessing information on its site,[151] the court sided with Eventbrite and condemned Cvent for not taking affirmative steps to block competitors from accessing its data.[152] The court stated that unless Cvent took *meaningful* protective steps, anyone, including direct

---

145 *Id.*
146 *Id.*
147 Cvent, Inc. v. Eventbrite, Inc., 739 F. Supp. 2d 927 (E.D. Va. 2010).
148 *Id.* at 930.
149 *Id.* at 930-31.
150 *Id.* at 932.
151 *Id.*
152 *Id.* at 932-33.

business competitors, could search and access Cvent's information at will.[153]

The second case that underscores the courts' movement towards a code-based rule is the 2013 case *Fidlar Technologies v. LPS*.[154] There, a technology company (Fidlar) partnered with a number of governmental entities and sold them a software program called Laredo, which those agencies used to let community members view county records—the idea being that if after previewing the county records, individuals wanted to obtain the records, they would have to purchase them from their local county offices.[155] As such, Laredo was designed to help generate county revenue.[156] The defendant (LPS), a competitor that relied on scraping, amalgamated a variety of real property data. Like individual users of Laredo, LPS used Laredo to view public records online.[157] LPS then developed a program to electronically capture the public records from Laredo and download them without having to pay fees to local counties.[158] LPS also sold the records to its own customers, undercutting Laredo's ability to help counties generate revenue.[159] While LPS had no contract with Laredo to prohibit such scraping,[160] as soon as Fidlar learned of LPS's scraping, Fidlar notified LPS that it was using its data unlawfully under the CFAA.[161] Fidlar also technically upgraded Laredo just to prevent further scraping.[162] The court held that LPS was liable under the CFAA because its scraper was designed to circumvent Laredo's intended functions and bypass various user controls.[163] Further, the scraper impaired Laredo's integrity, causing it significant damage.[164]

Fidlar Technologies was an important case because the court, in addition to analyzing why scrapers must violate a code barrier in order to exceed authorization, spent significant time determining Fidlar's damages.[165] While damages under the CFAA

---

153 *Id.* at 933.

154 Fidlar Techs. v. LPS Real Estate Data Sols., Inc., No. 4:13-cv-4021-SLD-JAG, 2013 WL 5973938 (C.D. Ill. Nov. 8, 2013).

155 *Id.* at *1.

156 *Id.*

157 *Id.*

158 *Id.* at *2-3.

159 *Id.* at *3.

160 *Id.* at *2-3.

161 Fidlar also communicated with each county that was affected by LPS's harvesting activities, and consequently, many of these counties unilaterally terminated their accounts with LPS or upgraded their Laredo software in order to hinder LPS's harvesting activity. *Id.* at *4-5.

162 *Id.*

163 *Id.* at *7-8.

164 *Id.*

165 *Id.*

have not been as contentious as the term authorization,[166] in *Fidlar*, the plaintiff brought a parallel claim of trespass to chattels.[167] Indeed, many scraping cases have been brought under this common law tort, and courts have increasingly applied it in the modern digital context. The jurisprudence of scraping cases brought under trespass to chattels is important to understand because it has allowed many data hosts to recover damages caused by harmful scrapers.

B. When Scrapers Do Not Breach Codes: Alternative Remedies in Trespass to Chattels

Liability for trespass to chattels arises when one intentionally takes or intermeddles with a chattel that is possessed by another.[168] Since the 1990s, this tort has been applied to cases involving devices that automatically overuse phone and email networks and diminish their functionality.[169] More recently, the tort has been used in scraping cases.[170] To establish a trespass to chattels claim, data hosts have to show that they were dispossessed of their chattel, that their chattel's condition, quality, or value was impaired, or that they were "deprived of the use of their chattel for a substantial time."[171]

---

[166] Catherine M. Sharkey, *Trespass Torts and Self-Help for an Electronic Age*, 44 TULSA L. REV. 677, 695 (2009) (discussing Patricia Bellia and Richard Epstein's similar opinions).

[167] *Fidlar*, 2013 WL 5973938, at *9-10.

[168] Sharkey, *supra* note 166, at 678 (citing RESTATEMENT (SECOND) OF TORTS § 217 (1965) ("A trespass to chattel may be committed by intentionally (a) dispossessing another of the chattel, or (b) using or intermeddling with a chattel in the possession of another.")).

[169] *See, e.g.*, Hotmail Corp. v. Van$ Money Pie Inc., No. C 98-20064 JW, 1998 WL 388389, at *2 (N.D. Cal. Apr. 16, 1998) (involving a device that automatically sent spam emails to thousands of Hotmail users); Am. Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444, 448 (E.D. Va. 1998) (involving a device that sent bulk unsolicited spam advertisements to AOL customers); Am. Online, Inc. v. IMS, 24 F. Supp. 2d 548, 549 (E.D. Va. 1998) (involving a device that sent bulk spam emails to AOL customers); Thrifty-Tel, Inc. v. Bezenek, 54 Cal. Rptr. 2d 468, 471 (Cal. Ct. App. 1996) (involving device that accessed Thrifty-Tel's telephone system and generated massive number of phone calls); CompuServe Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1017-18 (S.D. Ohio 1997) (involving device that sent substantial volume of unsolicited email advertisements to CompuServe subscribers).

[170] *See, e.g.*, Register.com, Inc. v. Verio, Inc., 356 F.3d 393, 396-97 (2d Cir. 2004) (involving device that scraped competitor's website to solicit additional business and engage in email and phone marketing); EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 579 (1st Cir. 2001) (involving scraping device that automatically gleaned pricing information from competitor's website); Fidlar Techs. v. LPS Real Estate Data Solutions, Inc., No. 4:13-CV-4021-SLD-JAG, 2013 WL 5973938, at *3 (C.D. Ill. Nov. 8, 2013) (involving scraper that aggregated nondownloadable data from software program); eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1062 (N.D. Cal. 2000) (involving scraper that aggregated auction data from competing website).

[171] RESTATEMENT (SECOND) OF TORTS § 218 (AM. LAW INST. 1965).

When trespass to chattels was first used in the digital context, courts were willing to apply the doctrine even when there was no physical damage to digital property.[172] As scholars began to warn about the dangers of applying the doctrine too expansively,[173] however, certain courts began to find that without showing physical harm, data hosts could not make out a claim.[174] Although a few courts adopted this view and dismissed trespass to chattels claims where there was no proof of tangible harm, in most courts, trespass to chattels is a viable alternate legal route for data hosts to pursue scraping claims. Adopting a code-based standard for scraping claims brought under the CFAA will not significantly prejudice data hosts that do not erect code barriers because data hosts that are victims of harmful scraping can still recover damages under trespass to chattels.

1. Early Digital Trespass: Phone and Email Cases

Before the emergence of scraping cases, trespass to chattels was applied in cases with telephone networks and email systems. In *Thrifty-Tel, Inc. v. Bezenek*,[175] phone hackers used computer software to hack into a phone and generate hundreds of thousands of calls that denied other users access to those phone lines. Thrifty-Tel alleged that Bezenek's conduct constituted trespass to chattels. The court agreed, finding that the computerized telephone network was a chattel, and by overburdening the network, Bezeneck intermeddled with Thrifty-Tel's *use* of its chattel, thereby causing it injury.[176]

---

[172] *See, e.g.*, *Thrifty-Tel*, 54 Cal. Rptr. 2d at 472, 475, 477 (holding that there was sufficient damage due to overburdening an electronic phone system, which caused a diminution of its quality, condition, or value); *CompuServe*, 962 F. Supp. at 1025-27 (finding that there was sufficient damage to an email network).

[173] *See, e.g.*, Sharkey, *supra* note 166 (proposing that self-help remedies be a precondition for data hosts to seek legal enforcement of cyberproperty rights, even though they are not required for land owners to seek enforcement of land property rights, in order to distinguish the two doctrines and cabin the expansiveness of the digital tort); Dan Hunter, *Cyberspace as Place and the Tragedy of the Digital Anticommons*, 91 CAL. L. REV. 439, 502 (2003) (identifying a trend towards increased private ownership in the Internet domain and warning that such increased private ownership could lead to a tragedy of the anticommons, whereby "multiple parties can prevent others from using a given resource so that no one has an effective right of use"); Greg Lastowka, *Decoding Cyberproperty*, 40 IND. L. REV. 23, 71 (2007) (advocating for less robust cyberproperty rights and noting that "[w]e have no reason to trust that creating broad legal rights of exclusion online will lead us to better social outcomes and good reason to believe that cyberproperty rights might well, under the cover of private property, lead to significant harms").

[174] *See, e.g.*, Ticketmaster Corp. v. Tickets.Com, Inc., No. CV997654HLHVBKX, 2003 WL 21406289, at *3 (C.D. Cal. Mar. 7, 2003).

[175] Thrifty-Tel, Inc. v. Bezenek, 54 Cal. Rptr. 2d 468 (Cal. Ct. App. 1996).

[176] *Id.* at 472-73.

In subsequent email spamming cases,[177] courts continued to apply a modern notion of trespass to chattels; in most instances, the plaintiff claimed that a digital device accessed its personal property without authorization.[178] For damages, these courts generally only required a modest showing that the email network suffered some diminution of its quality, condition, or value as a result of the spammer's conduct, even if the damages were not quantifiable.[179] For example, in *CompuServe, Inc. v. Cyber Promotions*, CompuServe, a major online provider of email services, brought a trespass to chattels claim against Cyber Promotions.[180] Cyber Promotions was a business that sent massive amounts of unsolicited email advertisements and used CompuServe's email database to send such advertisements to CompuServe's subscribers.[181] The court, after analyzing the evolution of trespass to chattels in the digital context, agreed with CompuServe and granted its request for a temporary injunction against Cyber Promotions.[182] Otherwise, the court found, CompuServe's email system would be at risk of irreparable damage, not only from the diminished physical disk space and processing power of CompuServe's systems,[183] but also from the threat to CompuServe's "business reputation and goodwill with its customers."[184] Thus, as in *Thrifty-Tel*, the court showed that it was willing to assess remedies based on nonphysical damage.

---

[177] *See, e.g.*, Hotmail Corp. v. Van$ Money Pie Inc., No. C 98-20064 JW, 1998 WL 388389 (N.D. Cal. Apr. 16, 1998); Am. Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444 (E.D. Va. 1998); Am. Online, Inc. v. IMS, 24 F. Supp. 2d 548 (E.D. Va. 1998); CompuServe Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015 (S.D. Ohio 1997).

[178] "Trespass to chattels has evolved from its original common law application, concerning primarily the asportation of another's tangible property, to include the unauthorized use of personal property." *CompuServe*, 962 F. Supp. at 1020.

[179] *Id.* at 1022.

[180] *Id.* at 1017.

[181] *Id.* at 1018-19.

[182] *Id.* at 1027.

[183]

> To the extent that defendants' multitudinous electronic mailings demand the disk space and drain the processing power of plaintiff's computer equipment, those resources are not available to serve CompuServe subscribers. Therefore, the value of that equipment to CompuServe is diminished even though it is not physically damaged by defendants' conduct.

Id. at 1022.

[184] *Id.* at 1023; Patricia L. Bellia, *Defending Cyberproperty*, 79 N.Y.U. L. REV. 2164, 2176 (2004).

2. Modern Digital Trespass: The Scraping Cases

The first major application of trespass to chattels in a scraping case was in 2000 in *eBay, Inc. v. Bidder's Edge, Inc.*[185] In that case, eBay, a well-known auction website, sought to enjoin Bidder's Edge (BE), a company that utilized a scraper to list eBay's auction items on its own site.[186] eBay based its trespass to chattels argument on its user agreement,[187] telephone conversations with BE,[188] cease-and-desist letters in which it told BE to discontinue scraping,[189] and attempts to block BE's IP addresses.[190] The court held that BE was liable under trespass to chattels for intermeddling with eBay's servers without authorization and free riding on the time, effort, and money that eBay had invested to create its system.[191] The court expressed concerned that "[i]f BE's activity . . . [were] allowed to continue unchecked, it would encourage other auction aggregators to engage in similar recursive searching of the eBay system such that eBay would suffer irreparable harm from reduced system performance, system unavailability, or data losses."[192]

Two subsequent cases that considered trespass to chattels in a similar manner were *Oyster Software v. Forms Processing, Inc.*[193] and *Southwest Airlines v. FareChase, Inc.*[194] In *Oyster*, a scraper copied data from Oyster's website, and Forms Processing used the data on its own site. Relying on *Bidder's Edge* and *CompuServe*'s standard that interference need not be more than negligible, a district court for the Central District of California declined to dismiss Oyster's claim against Forms Processing for misusing its data.[195]

Similarly, in *Southwest Airlines v. FareChase, Inc.*, Southwest Airlines alleged that it suffered damages from being scraped by a company (FareChase) that gleaned flight information from its website.[196] Even though Southwest did not

---

[185] eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058 (N.D. Cal. 2000); Fibbe, *supra* note 58, at 1014.

[186] *Bidder's Edge*, 100 F. Supp. 2d at 1058, 1063.

[187] *Id.* at 1060.

[188] *Id.* at 1062.

[189] *Id.*

[190] Indeed, "eBay had blocked a total of 169 IP addresses it believed BE was using to query eBay's system." But "BE elected to continue crawling eBay's site by using proxy servers to evade eBay's IP blocks." *Id.* at 1062-63.

[191] *Id.* at 1063, 1069-70.

[192] *Id.* at 1066.

[193] Oyster Software, Inc. v. Forms Processing, Inc., No. C-00-0724 JCS, 2001 WL 1736382 (N.D. Cal. Dec. 6, 2001).

[194] Sw. Airlines Co. v. FareChase, Inc., 318 F. Supp. 2d 435 (N.D. Tex. 2004).

[195] *Oyster Software*, 2001 WL 1736382, at *13.

[196] Sw. Airlines, 318 F. Supp. 2d at 436.

prove that it endured physical harm or deprivation, the court held that FareChase's use of a scraper to glean Southwest's flight information was unauthorized, as it deceived consumers who purchased tickets through FareChase's website but mistakenly believed that they had contracted with Southwest.[197] Thus, the court held that FareChase's scraping wrongfully interfered with Southwest's use and possession of its site.[198] Essentially, the court implied that because FareChase knowingly accessed Southwest's data without its consent, this alone was an adequate basis for damages.[199]

This line of modern trespass to chattels cases shows courts' openness to assessing damages based on harms that are difficult to quantify, such as data hosts' devalued investments in their websites, scraper users' ability to free ride on data hosts' investments, and data hosts' diminished ability to use their sites if they slow down or crash due to scraping. Although a few courts have refrained from flexible damages assessments, the majority of courts allow plaintiffs to plead and recover for trespass to chattels under a range of damages theories.

3. A Negligible Bump in the Road to Adopting a Code

In 2003, in light of a surge of scholarly criticism against applying trespass to chattels to digital property, courts began to find that scraper users could not be liable unless their scraper physically interfered with the use or operation of the computer.[200] For example, in *Ticketmaster Corp. v. Tickets.com, Inc.*, a district court for the Central District of California did not find a scraper liable for trespass to chattels and rejected the argument that "mere use of a spider to enter a publicly available web site to gather information, without more, is sufficient to fulfill the harm requirement."[201] Later that year, the Supreme Court of California reached a similar decision in *Intel v. Hamidi*.[202] There, a former employee sent numerous disruptive email messages to current Intel employees but did not circumvent any technical security or damage the computer

---

[197] *Id.* at 442.

[198] *Id.*

[199] *Id.* ("Additionally, the Court concludes Southwest has arguably alleged damage; the question of whether the damage is actual or physical, or whether the interference is for a substantial period of time, is a fact question and inappropriate for resolution in a motion to dismiss.").

[200] Ticketmaster Corp. v. Tickets.Com, Inc., No. CV997654HLHVBKX, 2003 WL 21406289, at *3 (C.D. Cal. Mar. 7, 2003); Intel Corp. v. Hamidi, 71 P.3d 296, 300 (Cal. 2003).

[201] *Ticketmaster*, 2003 WL 21406289, at *3.

[202] *Hamidi*, 71 P.3d at 300.

systems in any physical manner.[203] Even though *Hamidi* was not a scraper case, the court's reasoning in rejecting the trespass to chattels claim was the same as its reasoning in *Ticketmaster*—that in order for a plaintiff to successfully make out a trespass to chattels claim, the plaintiff would need to prove that the chattel was physically damaged.[204]

Although these two cases interpreted the damages requirement for trespass to chattels narrowly, neither substantially detracted from the viability of trespass to chattels for harmful scraping cases. In *Ticketmaster*, the court was dealing with a beneficial scraper, a price amalgamator, that was compiling public pricing information available on Ticketmaster's website without breaching any technical code or damaging the site. In fact, the price amalgamator was "deep linking" the prices, which means that after scraping ticket prices from Ticketmaster's site, it would provide users with a hyperlink and transfer them directly to the Ticketmaster site for purchase.[205] And in *Hamidi*, the court was not dealing with a scraper, but rather with an individual whose emails disrupted work productivity.

In *Register.com, Inc. v. Verio, Inc.*, a major decision in the Second Circuit in 2007, the court affirmed that trespass to chattels could still be used to bring a suit against harmful scrapers.[206] Register.com was an issuer of Internet domain names and a seller of web services, and Verio was a competitor that scraped Register.com.[207] Although Register.com shared its data with certain members of its site, it expressly prohibited members from using that data to solicit additional business.[208] Verio scraped and used Register.com's data for email and phone marketing.[209] Despite notices to cease such activities,[210] Verio continued scraping Register.com.[211] When Register.com sued Verio for trespass to chattels, Verio argued that its conduct never physically harmed Register's servers.[212] But the district court agreed that *use* deprivation could be considered harm under the tort.[213] Relying on *Thrifty-Tel* and older spamming cases, the

---

[203] *Id.* at 299.
[204] *Id.* at 300.
[205] *Ticketmaster*, 2003 WL 21406289, at *1.
[206] Register.com, Inc. v. Verio, Inc., 356 F.3d 393, 395-96 (2d Cir. 2004).
[207] *Id.*
[208] *Id.* at 396.
[209] *Id.* at 396-97.
[210] *Id.* at 397.
[211] *Id.* at 398.
[212] *Id.* at 404.
[213] "Verio's use of search robots, consisting of software programs performing multiple automated successive queries, consumed a significant portion of the capacity of Register's computer systems." *Id.*

Second Circuit reiterated the court's concern in *Bidder's Edge* that if such scraping were permitted, it would likely encourage other competitors to follow suit.[214]

The jurisprudence of scraping cases brought under trespass to chattels shows that, on the whole, courts have been flexible in constructing the damages requirement of this tort in the modern digital context. Over the years, courts have assessed damages, such as overburdened networks,[215] lost space,[216] threats to business reputation and goodwill with customers,[217] threats of similar future conduct,[218] intermeddling with servers without authorization,[219] "wrongful interference with . . . use or possession,"[220] and free riding on data hosts' investments.[221] Even though the *Ticketmaster* and *Hamidi* courts were less flexible in their damages determinations, those cases involved different considerations than most harmful scraping cases and therefore did not substantially detract from the viability of the trespass to chattels regime as an alternative remedy for certain data scraping cases.

Notably, trespass to chattels need not be considered a substitute for or equivalent remedy to the CFAA. Because only certain harmful scraping cases—those that involve a code breach—should be brought under the CFAA in the first place, trespass to chattels serves as a useful alternative legal avenue for situations involving less pervasive scraping that still damages data hosts. Since problems caused by scrapers will only proliferate as society becomes more technologically dependent, it is useful to have both the CFAA and trespass to chattels available to deter harmful scrapers' unlawful conduct.

CONCLUSION

In November 2014, the U.S. State Department became the fourth government agency to announce a breach of its computer systems in the span of just a few weeks.[222] The hack,

---

[214] *Id.*

[215] Thrifty-Tel, Inc. v. Bezenek, 54 Cal. Rptr. 2d 468, 475, 477 (Cal. Ct. App. 1996).

[216] CompuServe Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1022, 1027 (S.D. Ohio 1997).

[217] eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1066, 1072 (N.D. Cal. 2000).

[218] *Id.*

[219] *Id.* at 1064.

[220] Sw. Airlines Co. v. FareChase, Inc., 318 F. Supp. 2d 435, 442 (N.D. Tex. 2004).

[221] *Bidder's Edge*, 100 F. Supp. 2d at 1068, 1072.

[222] Nicole Perlroth, *State Department Targeted by Hackers in 4th Agency Computer Breach*, N.Y. TIMES (Nov. 16, 2014), http://www.nytimes.com/2014/11/17/us/politics/state-

believed to have originated from Russia, forced the department to temporarily shut down its email system and public websites.[223] The attack resembled one involving unclassified computer systems at the White House the month before, which also necessitated a temporary shutdown of its communications systems.[224] Although both of these government attacks were ultimately contained, data breaches pose an increasingly grave threat to our national security and privacy in all of its forms—further demonstrating the need for a cohesive jurisprudence of computer hacking laws.

The CFAA must be fortified if it is to remain Congress's premier antihacking computer fraud statute. The CFAA's original title and the initial Senate and House Reports indicate that the intent behind the act was to combat crimes akin to credit card theft, identity theft, grand fraud, larceny, false pretenses, embezzlement, and similar offenses.[225] All of these are crimes of specific intent, indicating that the drafters of the act desired for there to be a knowledge requirement. To fortify the act, courts must preserve the drafters' intent.

Users of beneficial scrapers are unlikely to intentionally harm data hosts or expose confidential, protected data because beneficial scrapers compile and reformat data that is already publicly available. Even if data hosts occasionally suffer damage from beneficial scrapers that did not intend to harm them, data hosts can still seek recourse under the tort of trespass to chattels. Since there are adequate remedies available to data hosts that are scraped by harmful or beneficial scrapers, a code-based rule derived from the narrow concept of authorization helps ensure that users of beneficial scrapers are not unnecessarily swept under the CFAA without having the requisite intent to access protected data and harm data hosts.[226] Such a rule would also provide clear notice to scraper users of when they are committing a federal crime, and it would create a workable standard for federal courts to apply consistently. Thus, a code-based rule is the best means to combat harmful scraping while protecting beneficial scraping.

Adopting a narrow, code-based rule also does not threaten unprotected data hosts if they are the victims of

---

department-targeted-by-hackers-in-4th-agency-computer-breach.html?_r=0 [http://perma.cc/K4X9-QECE].

[223] *Id.*

[224] *Id.*

[225] Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, 98 Stat. 2190 (codified as amended at 18 U.S.C. § 1030 (2008)); S. REP. NO. 99-432, at 9 (1986); H.R. REP. NO. 98-894, at 21 (1984).

[226] H.R. REP. NO. 98-894, at 21.

scraping abuse. This is due to the availability of trespass to chattels as an alternative claim when scraper users do not breach a code barrier or deprive a data host of some use of or value in its website. Because courts have flexibly construed damages theories in cases brought under this tort, it adequately fills the void in those situations where it would be inappropriate to apply the CFAA.

In 2013, reports indicated that scraping accounts for nearly a quarter of all Internet activity.[227] Since scraping can be both a beneficial and detrimental activity to society, its place in data hacking jurisprudence needs to be clear. President Obama announced to the nation in his 2015 State of the Union address that data hacking legislation must account for the modern security issues we face.[228] One of the best ways to make data hacking legislation more cohesive and effective is to clarify the meaning of the CFAA's ambiguous terminology once and for all and adopt a narrow standard of authorization, particularly in the scraping context. This will resolve a prolonged circuit split, ameliorate problems of adequate notice for users of scrapers, reduce the surplus of CFAA cases in federal courts, and allow the CFAA to more effectively hold harmful scrapers and perilous data hackers accountable, as it was originally intended to do.

Myra F. Din[†]

---

[227] Rubin & Hu, *supra* note 21.

[228] "And tonight, I urge this Congress to finally pass the legislation we need to better meet the evolving threat of cyber attacks, combat identity theft, and protect our children's information." President Barack Obama, State of the Union Address (Jan. 20, 2015), https://www.whitehouse.gov/the-press-office/2015/01/20/remarks-president-state-union-address-january-20-2015 [http://perma.cc/5BH7-TL56].

[†] J.D. Candidate, Brooklyn Law School, 2016; B.S., Cornell University, 2012. First and foremost, thank you to my incredible mother and brother for their unwavering support as I learned to love the law. Another thank you to my many mentors at Brooklyn Law School—particularly Professors Christina Mulligan and Lawrence Solan for their insight on this topic and Professors Michael Gerber, Maryellen Fullerton, Brian Lee, and Cynthia Godsoe for their constant guidance during the year I wrote this note. A special thanks to Lillian Smith, Michael Piacentini, Jonathan Myers, Taylor Dougherty, and the staff of the *Brooklyn Law Review* for their hard work in preparing this note for publication. And lastly, I dedicate this note to my father, Anees Din, whom I lost while I was writing it. His life and legacy continue to inspire all my academic endeavors.