Saint Louis University Law Journal

Volume 66
Number 2 *General Issue (Winter 2022)*

Article 7

2022

International Application of CFAA: Scraping Data or Scraping Law?

King Fung Tsang
Chinese University of Hong Kong, kftsang@cuhk.edu.hk

INTERNATIONAL APPLICATION OF CFAA: SCRAPING DATA OR SCRAPING LAW?

KING FUNG TSANG*

ABSTRACT

Web scraping has resulted in a growing number of civil litigations internationally, including claims under the Computer Fraud and Abuse Act ("CFAA") in the United States. With the Supreme Court's first ever decision on the CFAA, in Van Buren v. United States*, and its granting of LinkedIn's petition for certiorari in June 2021, the CFAA is expected to attract even more interest among scholars and practitioners. However, little attention has been given to its cross-border ramifications. Cases show that U.S. courts are more than willing to apply the CFAA extraterritorially, even though their analyses are often flawed. In addition, other conflict-of-laws rules, such as personal jurisdiction and* forum non conveniens*, impose few constraints on the CFAA's international effects. Given that CFAA claims are more likely to succeed than other causes of action, there is a strong motivation for website owners to enjoin scraping internationally by filing CFAA claims in U.S. courts. It is therefore argued that U.S. courts should consider the international impacts of the CFAA with care when interpreting its substantive provisions. Such due regard to comity will be in the national interest of the United States.*

* S.J.D. (Georgetown), LLM, J.D. (Columbia), Associate Professor, The Chinese University of Hong Kong. I would like to thank Dr. Han-wei Liu for his insight and comments on the initial idea for this Article.

INTRODUCTION

Web scraping, using software to gather information from a website in an automated manner,[1] has resulted in a growing number of civil litigations internationally.[2] In the United States, violation of the Computer Fraud and Abuse Act ("CFAA")[3] is the most controversial claim utilized by website owners against scraping. The CFAA prohibits the obtaining of information through intentional access to a computer "without authorization" or in a way that "exceeds authorized access."[4] Although originally a criminal statute, the CFAA also gives a private right of action.[5] The "without authorization" clause is often used by web owners in private actions against web scrapers.[6] Currently, federal circuits are split as to the interpretation of "without authorization."[7] A liberal interpretation suggests that scrapers may be subject to liabilities if they violate the website owner's terms of use ("TOU"). In June 2021, the Supreme Court ruled on the CFAA for the first time in history in *Van Buren v. United States* (hereinafter "*Van Buren*").[8] This was a criminal case concerning the "exceeds authorized access" clause; the Supreme Court opted not to rule on the "without authorization" clause.[9] Eleven days after *Van Buren*, in *LinkedIn Corp. v. hiQ Labs, Inc.* (hereinafter "*hiQ*"),[10] the Supreme Court vacated and remanded the

1. *See* Ticketmaster Corp. v. Tickets.com, Inc., No. CV 99-7654 HLH (BQRx), 2003 WL 21406289, at *2 (C.D. Cal. Mar. 7, 2003) (Defendant employed an electronic program software called a 'spider' or 'crawler' to review the internal web pages (available to the public) of Plaintiff. The 'spider' 'crawled' through the internal web pages to Plaintiff and electronically extracted the electronic information from which the web page is shown on the user's computer); eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1060 n.2 (N.D. Cal. 2000) ("Programs that recursively query other computers over the Internet in order to obtain a significant amount of information are referred to in the pleadings by various names, including software robots, robots, spiders and web crawlers.").

2. For U.S. cases, *see* Andrew Sellars, *Twenty Years of Web Scraping and the Computer Fraud and Abuse Act*, 24 B.U. J. SCI. & TECH. L. 372, 378–79 n.43 (2018) (finding sixty-one such cases). For non-U.S. cases, *see, e.g.*, Case C-30/14, Ryanair Ltd. v. PR Aviation BV, ECLI:EU:C:2015:10 (Jan. 15, 2015); Century 21 Canada L.P. v. Rogers Commc'ns Inc., 2011 BCSC 1196 (Can.); Trader v. CarGurus, 2017 ONSC 1841 (Can.); Ryanair Ltd. v. On The Beach Ltd., [2013] IEHC 124 (Ir.); Ryanair DAC v. SC Vola.ro sri, [2019] IEHC 239 (Ir.); Pub. Rels. Consultants Ass'n v. Newspaper Licensing Agency Ltd., [2013] UKSC 18 (UK).

3. 18 U.S.C. § 1030 (2018).

4. 18 U.S.C. § 1030(a)(2)(C) (2018).

5. 18 U.S.C. § 1030(g) (2018).

6. *See* Sellars, *supra* note 2, at 391.

7. *See* hiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985, 1000–01 (9th Cir. 2019) (highlighting the difference in approaches between the Ninth Circuit on one hand and the First and Eleventh circuits on the other), *cert. granted*, *vacated*, No. 19-1116, 141 S.Ct. 2752 (June 14, 2021) (mem.); Jacquellena Carrero, *Access Granted: A First Amendment Theory of Reform of the CFAA Access Provision*, 120 COLUM. L. REV. 131, 148–49 (2020).

8. No. 19-783 (U.S. June 3, 2021).

9. *Id.* at 5.

10. GVR Order, LinkedIn Corp. v. hiQ Labs, Inc., 141 S. Ct. 2752 (No. 19-1116).

Ninth Circuit's decision that had adopted a narrow interpretation of the "without authorization" clause in the context of web scraping.[11] This makes the interpretation of the "without authorization" clause the next big question as far as the CFAA is concerned.

Little attention, however, is given to the international application of the CFAA.[12] This is surprising, given that web scraping will almost always involve some international elements. Either the website owner or scraper can be based overseas. For example, in *Ryanair DAC v. Expedia* (hereinafter "*Expedia*"), the Ireland-based airline Ryanair sued U.S.-based Expedia for scraping under the CFAA.[13] Furthermore, it is easy nowadays to store data in overseas servers, potentially containing information belonging to anyone in the world.[14] Similarly, since websites are available worldwide, scraping can be conducted anywhere with an Internet connection.

With the CFAA considered the easiest cause of action against scraping,[15] website owners have motivation to "shop" for a CFAA claim. This is facilitated by the U.S. courts' consistent interpretation that the CFAA applies extraterritorially. Such extraterritoriality, however, could lead to substantial conflict between the United States and other countries, as witnessed in extraterritorial applications of U.S. antitrust and securities laws,[16] particularly since no other country has an equivalent piece of legislation granting website owners a private action with such straightforward prohibition.[17] The CFAA, despite being a U.S. law, will potentially regulate web scraping all around the world.

Given the vastness of the CFAA's international impacts, it would make sense for U.S. courts to take them into consideration in their interpretations of substantive provisions. This is because when the CFAA attaches liability to an act conducted in the United States, it will likely attach liability to the same act conducted in a foreign country. However, its international reach was not

11. *See hiQ*, 938 F.3d at 1003.

12. Only one article has touched on this aspect, however, it is limited to software outsourced to China and dates back to 2007, see Carrie Greenplate, *Of Protection and Sovereignty: Applying the Computer Fraud and Abuse Act Extraterritorially to Protect Embedded Software Outsourced to China*, 57 AM. U. L. REV. 129, 135, n.20 (2007).

13. Ryanair DAC v. Expedia Inc., No. C17-1789RSL, 2018 WL 3727599, at *2 (W.D. Wash. Aug. 6, 2018).

14. *Id.* at *4.

15. Christine D. Galbraith, *Access Denied: Improper Use of the Computer Fraud and Abuse Act to Control Information on Publicly Accessible Internet Websites*, 63 MD. L. REV. 320, 323–24 (2004).

16. *See* Hartford Fire Ins. Co. v. California, 509 U.S. 764, 797–98 (1993); Morrison v. Nat'l Austl. Bank Ltd., 561 U.S. 247, 255, 269 (2010).

17. *See* Han-Wei Liu, *Two Decades of Laws and Practice Around Screen Scraping in the Common Law World and its Open Banking Watershed Moment*, 30 WASH. INT'L L.J. 28, 31 (2020).

addressed by the Supreme Court in *Van Buren,* although the decision will certainly have international implications.[18]

This Article aims to bridge the gap between international web scraping and the CFAA, right before the Ninth Circuit is to interpret the "without authorization" clause post *Van Buren*. Part I provides the background to the CFAA and explains how it has been shaped by *Van Buren*. In particular, it highlights the interlocking nature of CFAA's three perspectives: criminal, civil, and international. Part II discusses the problems in U.S. courts' interpretation of the CFAA's extraterritoriality. Part III discusses how other conflict-of-laws rules put few constraints on the CFAA's international effects. Finally, Part IV shows the advantages of the CFAA over other causes of action under both U.S. and foreign laws. Part V concludes that U.S. courts should consider the CFAA's vast impacts on international comity when interpreting its substantive provisions. Meanwhile, the courts should also revisit the extraterritoriality of the CFAA to define its scope and limitations.

I. CFAA

A. Background & Nature

The original statute, first enacted in 1984,[19] was created to combat the then-rising problem of the hacking of "federal interest computers."[20] Private right of action was added to the CFAA in 1994.[21] Apart from compensating aggrieved individuals, the addition was also intended to stem the rising tide of cybercrime.[22] The 1996 amendment further expanded the protection provided from federal interest computers to any computers "used in interstate or foreign commerce or communication."[23] Henceforth, the CFAA has applied to "all information from all computers that connect to the Internet."[24] This expansion was "prompted in part by a growing concern over the amount of financial losses suffered by American companies from the breach of computer security systems."[25] Yet, sorting through the legislative history of these amendments and those that came after them, it is clear there has never been any discussion of the CFAA's applicability to web scraping. This is not surprising, as commercial data

18. *See infra* Part I.B.2.

19. As part of the Comprehensive Crime Control Act of 1984, see Van Buren v. United States, No. 19-783, slip op. at 2 (U.S. June 3, 2021). *See also* Galbraith, *supra* note 15, at 326.

20. Galbraith, *supra* note 15, at 327–28.

21. Pub. L. No. 103-332, § 290001, 108 Stat. 1796, 2097–99 (1994).

22. *See* Galbraith, *supra* note 15, at 329.

23. *See* S. REP. 104-357, at 7 (1996).

24. Van Buren v. United States, No. 19-783, slip op. at 2 (U.S. June 3, 2021).

25. Galbraith, *supra* note 15, at 330.

scraping as we understand it today did not exist at the time.[26] The challenge facing the courts is how to apply the CFAA to an act that was not contemplated by the original legislators.

Most scrapers are sued under Section 1030(a)(2)(C) of the CFAA, which makes it an offense for "[w]hoever . . . intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer." A person who suffers "damage or loss by reason of a violation" of these provisions may bring a civil action under Section 1030(g) if the loss exceeds $5,000 in value.[27]

This statutory language is extremely broad. Professor Kerr has said that it covers "everything with a microchip that can be regulated under the Commerce Clause, whether it is connected to the Internet or not."[28] A "computer" is defined broadly to include "any data storage facility."[29] As long as the unauthorized access is intentional, its purpose does not matter. "Information" seems to cover any information; the term "whoever" implies that anyone in the world may be subject to the offense; and loss is defined broadly to include "any reasonable cost to any victim."[30] The court has even accepted the working hours spent in "analyzing, investigating, and responding to [the scraper's] actions [of scraping]" as satisfying the $5,000 loss threshold.[31] A finding of violation opens up a wide range of remedies under the civil suit, including "compensatory damages and injunctive relief or other equitable relief."[32] In addition, Section 1030(b) provides for the liability of any conspirator. Therefore, a company cannot escape liability by engaging a third party to commit the offense.[33] Similarly, the scraper company's managers may be individually liable.[34] In short, any person accessing any information on any device with a chip could fall under the scope of the CFAA, provided that such access is prohibited by the

26. *See* Orin Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1602 (2003) ("Unauthorized access statutes are creatures of the 1970s, when the Internet remained the domain of a few scientists and engineers.").

27. *See* 18 U.S.C. §§ 1030(c)(4)(A)(i)(I), (g) (2018).

28. *See* Brief of Professor Orin S. Kerr as Amicus Curiae Supporting Petitioner at 9, Van Buren v. United States, No. 19-783 (U.S. June 3, 2021).

29. 18 U.S.C. § 1030(e)(1) (2018).

30. 18 U.S.C. § 1030(e)(11) (2018).

31. Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058, 1066 (9th Cir. 2016).

32. 18 U.S.C. § 1030(g) (2018).

33. *See In re* Lenovo Adware Litig., No. 15-MD-02624-RMW, 2016 WL 6277245, at *6 (N.D. Cal. Oct. 27, 2016).

34. *See* Christie v. Nat'l Inst. for Newman Stud., 258 F. Supp. 3d 494, 511 (D.N.J. 2017).

TOU and results in a minimum loss of $5,000, regardless of the purpose of access.[35]

Most importantly, there is no definition of "without authorization." Under the broad interpretation adopted by some circuits, a breach of TOU, unilaterally set by the website owner, will be sufficient to satisfy the requirement of the definition.[36] For example, in *Southwest Airlines v. Farechase*, it was held that the scraper had obtained unauthorized access since Southwest's TOU expressly prohibited scraping and Southwest had directly informed the scraper that its access was unauthorized.[37] This is so "[r]egardless of whether the Use Agreement creates an enforceable contract for purposes of a breach of contract claim."[38] Under this interpretation, all that is required is "any verbal restriction on how a computer can be used."[39] Thus, if the broad interpretation is to prevail, the CFAA will be applied in a way that sets a low floor for finding liability and a high ceiling for possible remedies, while casting a wide net against potential violators.

On the other hand, other circuits have taken a narrow interpretation of "without authorization."[40] This is most recently illustrated by the Ninth Circuit in *hiQ*. This case concerned hiQ's scraping of LinkedIn profiles that were publicly available on the Internet. Although access to the data did not require authorization from LinkedIn, there were express conditions on LinkedIn's website that specifically prohibited scraping.[41] In addition, LinkedIn sent a cease-and-desist letter to hiQ, asserting that its user agreement had been violated.[42] The crux of the case is therefore whether these contract-based measures by LinkedIn made hiQ's access "without authorization." After acknowledging the split among federal circuits as to the interpretation, the Ninth Circuit reiterated its own narrow interpretation.[43] For "without authorization," the court drew an analogy to "breaking and entering," such that only private information, i.e., "information delineated as private through use of a permission requirement of some sort," like a password portal, is subject to the application

35. *See* Appellant's Brief at 2, United States v. Gasperini, 729 F. App'x 112 (2d Cir. Nov. 16, 2017) (No. 17-2479) (complaining that "§ 1030(a)(2)(C) punishes *any* unauthorized access to *any* computer that leads to obtainment of *any* kind of information").

36. *See* Carrero, *supra* note 7, at 148–49.

37. *See* Southwest Airlines Co. v. Farechase, Inc., 318 F. Supp. 2d 435, 439–40 (N.D. Tex. 2004).

38. *Id*.

39. *See* Brief of Professor Orin S. Kerr as Amicus Curiae Supporting Petitioner at 5, Van Buren v. United States, No. 19-783 (U.S. June 3, 2021); *see also* Mark A. Lemley, *Place and Cyberspace*, 91 CALIF. L. REV. 521, 528 n.29 (2003).

40. *See* Carrero, *supra* note 7, at 149 (highlighting the narrow approach adopted by Second, Fourth, and Ninth Circuits).

41. *See* hiQ, Inc. v. LinkedIn Corp., 938 F.3d 985, 991 (9th Cir. 2019).

42. *Id.* at 992.

43. *Id.* at 1003.

of unauthorized access.[44] Public information, such as public LinkedIn profiles, however, is not. Accordingly, the court granted hiQ's motion for a preliminary injunction against LinkedIn, which barred LinkedIn from imposing barriers to hiQ's access to public LinkedIn profiles.[45] LinkedIn subsequently appealed to the Supreme Court to overturn the decision. In June 2021, the Supreme Court decided to vacate the Ninth Circuit's decision and remand it to the court for reconsideration in light of *Van Buren*.[46]

B. Van Buren

Van Buren did not relate to web scraping, nor did it result in a ruling on the interpretation of "without authorization." It also had no international element. However, as will be seen, the case has implications for both civil and international perspectives.

The case involved a police officer who ran a license plate search with the computer in his patrol car in exchange for money, in violation of police department policy.[47] The issue was whether the police officer's access "exceed[ed] authorized access" under the CFAA when he had obtained the data via a computer he clearly had authorization to access, but had misused the data for an illegitimate purpose.[48] As with the "without authorization" clause, a split also emerged over the interpretation of the "exceed authorized access" clause.[49] The majority sided with those circuits taking the narrow interpretation, holding that the "exceeds authorized access" clause only "covers those who obtain information from particular areas in the computer—such as files, folders, or databases—to which their computer access does not extend."[50] Therefore, misuse of information for improper motives is not covered by the clause.

The majority reached the decision mainly by relying on the language of Sections 1030(a)(2) and (e)(6).[51] Unlike the "without authorization" clause, "exceeds authorized access" is defined in Section 1030(e)(6), and so much of the discussion is not relevant for our purpose.[52] Specifically, since both parties agreed that Van Buren had authorization to access the computer in question,[53]

44. *Id.* at 1001.

45. *Id.* at 992, 1005.

46. GVR Order, LinkedIn Corp. v. hiQ Labs, Inc., 141 S. Ct. 2752 (No. 19-1116).

47. Van Buren v. United States, No. 19-783, slip op. at 1 (U.S. June 3, 2021).

48. *Id.* at 3–4.

49. *See* Ajuba Int'l, L.L.C. v. Saharia, 871 F. Supp. 2d 671, 685–86 (E.D. Mich. 2012) (referring to "a nationwide split of authority concerning the proper interpretation of the terms 'without authorization' and 'exceeds authorized access'").

50. *Van Buren*, slip op. at 1.

51. *Id.* at 13.

52. Note, however, that the majority did refer to both the "without authorization" clause and the definition of "damages" and "loss" in its interpretation of "exceeds authorized access." *See id.* at 5.

53. Van Buren v. United States, No. 19-783, slip op. at 5 (U.S. June 3, 2021).

the court declined to define what constitutes authorization: "For present purposes, we need not address whether this inquiry turns only on technological (or "code-based") limitations on access, or instead also looks to limits contained in contracts or policies."[54] Consequently, the interpretation of the term "without authorization" is still very much up in the air. However, the case is still relevant for our purpose because of the interlocking nature of the CFAA's criminal, civil, and international perspectives. The three perspectives create a three-way tie.

1. Criminal-Civil Tie

First, the same actions that attract criminal liabilities will also attract civil liabilities, and vice versa.[55] Thus, a civil claim by the police department against Van Buren under the "exceeds authorized access" clause will now fail. When the same conduct attracts both criminal and civil liabilities under the CFAA, courts often rely on the rule of lenity to opt for the more lenient interpretation: "Because we must interpret the statute consistently, whether we encounter its application in a criminal or noncriminal context, the rule of lenity applies."[56] In the context of the CFAA, courts have cited the rule to support the narrow interpretation.[57] On the other hand, courts adopting the broad interpretation tend to be those focusing on the "civil context with sympathetic facts" while neglecting the implications in the "criminal context [that] would criminalize a remarkable swath of conduct involving computers."[58]

Although the majority in *Van Buren* did not frame this reasoning in terms of the rule of lenity,[59] it was clearly influenced by a policy consideration of

54. *Id.* at 13 n.8.

55. Except that for civil liabilities to be attached, the claim must be based upon "conduct involv[ing] one of the factors set forth in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i)." 18 U.S.C. § 1030(g) (2018).

56. *See* Leocal v. Ashcroft, 543 U.S. 1, 12 n.8 (2004).

57. *See* hiQ, Inc. v. LinkedIn Corp., 938 F.3d 985, 1003 (9th Cir. 2019) ("[T]he rule of lenity favors our narrow interpretation of the 'without authorization' provision in the CFAA."); Ajuba Int'l, L.L.C. v. Saharia, 871 F. Supp. 2d 671, 687 (E.D. Mich. 2012); Bell Aerospace Servs., Inc. v. U.S. Aero Servs., Inc., 690 F. Supp. 2d 1267, 1272 (M.D. Ala. 2010).

58. *See* Kerr, *supra* note 26, at 1642 ("The second source of the difficulty is that many cases have interpreted "authorization" in the context of civil disputes rather than criminal prosecutions. The difference tends to push courts in the direction of expansive interpretations of new laws. It is one thing to say that a defendant must pay a plaintiff for the harm his action caused; it is quite another to say that a defendant must go to jail for it. Courts are more likely to hold a defendant liable under an ambiguous statute when the stakes involve a business dispute between two competitors than when the government seeks to punish an individual with jail time. As a result, civil precedents tend to adopt broader standards of liability than do criminal precedents. Because many unauthorized access cases have arisen in a civil context with sympathetic facts, courts have adopted broad approaches to authorization that in a criminal context would criminalize a remarkable swath of conduct involving computers.").

59. Van Buren v. United States, No. 19-783, slip op. at 17 (U.S. June 3, 2021).

leniency.[60] According to the court, to apply the broad interpretation would "attach criminal penalties to a breathtaking amount of commonplace computer activity,"[61] and "[i]f the 'exceeds authorized access' clause criminalizes every violation of a computer-use policy, then millions of otherwise law-abiding citizens are criminals."[62] In particular, referring to the context of TOU published on a website,

> Many websites, services, and databases—which provide "information" from "protected computer[s]," §1030(a)(2)(C)—authorize a user's access only upon his agreement to follow specified terms of service. If the "exceeds authorized access" clause encompasses violations of circumstance-based access restrictions on employers' computers, it is difficult to see why it would not also encompass violations of such restrictions on website providers' computers.[63]

This same policy consideration is likely to be transferable to the "without authorization" clause through the rule of lenity. This is particularly the case given that "the line between ['access' and 'misuse'] can be thin."[64]

2. Criminal-International Tie

Even though *Van Buren* did not involve any international element, given the extraterritoriality of the CFAA (see Part II below), a narrow interpretation of criminal liability in a domestic case means that the same interpretation will apply in an international case. Thus, just as Van Buren will not be subject to the CFAA's criminal liability now, nor will a foreign-based employee of a U.S.-based company. For example, in *Ajuba Intern., L.L.C. v. Saharia*,[65] the court, adopting a narrow interpretation of the "exceeds authorized access" clause, granted the motion of the defendant—a former employee residing in India—and dismissed the CFAA claim.[66] In this sense, the international perspective acts as a multiplier that has the effect of multiplying the effects of the substantive provisions.

3. Civil-International Tie

Similarly, when the Ninth Circuit decides on the *hiQ* case on remand, the precedent will have an international impact in the future despite both hiQ and LinkedIn being U.S. corporations. However, just as the rule of leniency brings criminal consideration into civil cases, it is argued that the international

60. *See id.* at 11 ("The majority ends with policy arguments. It suggests they are not needed ('extra icing on a cake already frosted'). Yet, it stresses them at length.") (internal citation omitted).

61. *Id.* at 17.

62. *Id.* at 17–18.

63. *Id.* at 18.

64. Van Buren v. United States, No. 19-783, slip op. 19–20 (U.S. June 3, 2021).

65. 871 F. Supp. 2d 671, 687 (E.D. Mich. 2012).

66. *Id.* at 688.

perspective should equally influence the court's interpretation of the substantive provisions. For example, if the Supreme Court is worried that "an employee who sends a personal e-mail or reads the news using her work computer has violated the CFAA,"[67] it should be more concerned by the possibility that all overseas employees of that U.S. company would be in violation of the CFAA were they to send the same e-mail or read the same news. While the Supreme Court did not take the international perspective into consideration (which will further strengthen the majority's policy argument), it is suggested that the Ninth Circuit should certainly consider the international implications in deciding whether web scraping was committed "without authorization." The extraterritoriality of the CFAA is further explained below.

II. EXTRATERRITORIALITY

In *Morrison v. National Australia Bank Ltd.*, the Supreme Court adopted a two-stage approach to determine the extraterritoriality of a U.S. statute.[68] The first stage begins with a presumption against extraterritoriality, unless "the statute gives a clear, affirmative indication that it applies extraterritorially."[69] It is not necessary for the statute to state that it applies extraterritorially—inference can be made from the context.[70] If there is no clear indication, there is no extraterritoriality.[71] However, it is still possible for the statute to apply if the court is satisfied that its "focus" is such that "the case involves a domestic application of the statute."[72] In *RJR Nabisco, Inc. v. European Cmty.* (hereinafter "*Nabisco*"), the Supreme Court further required each cause of action under the same statute to go through the two-stage analysis.[73] Thus, despite finding that the Racketeer Influenced and Corrupt Organizations Act's ("RICO") criminal provisions passed the first stage, it concluded that its civil provisions failed both stages of the analysis.[74]

A. Unclear Application of Stage One

As regards the CFAA, the first case to examine its extraterritoriality was *United States v. Ivanov*, where a Russian hacker was accused of infiltrating a Connecticut corporation's computer system.[75] Although the case preceded both *Morrison* and *Nicastro*, the court's approach was consistent with stage one. First, the court looked at the CFAA's plain language. It found that Congress intended

67. *Van Buren*, slip op. at 18.
68. Morrison v. Nat'l Austl. Bank Ltd., 561 U.S. 247, 266 (2010).
69. RJR Nabisco, Inc. v. Eur. Cmty., 136 S. Ct. 2090, 2101 (2016).
70. *Morrison*, 561 U.S. at 255, 265.
71. *Nabisco*, 136 S. Ct. at 2102.
72. *Id.* at 2101.
73. *Id.* at 2106.
74. *Id.* at 2111.
75. United States v. Ivanov, 175 F. Supp. 2d 367, 369 (D. Conn. 2001).

the CFAA to apply extraterritorially as the text defines "protected computer" as a computer used "in interstate or foreign commerce or communication."[76] In particular, the court was convinced that the term "foreign" denotes extraterritoriality, as "it must mean something other than 'interstate'" to be meaningful.[77] Second, the court considered its legislative history. The 1996 Senate Judiciary Report clearly showed concern over foreign hackers accessing computers located in the United States and referred to two instances involving English and Argentinean hackers.[78] However, the fact that the CFAA may apply extraterritorially in *some* scenarios does not mean that it will *always* apply. The scope of extraterritoriality post-presumption will still need to be defined.[79] Here, the court failed to notice that the statutory language and the legislative history point to two different scenarios.

The term "protected computer" is used in CFAA provisions setting out substantive offenses. For example, Section 1030(2)(C) makes it an offense for "whoever . . . intentionally accesses a computer without authorization or exceeds authorization . . . to obtain information from any protected computer." With a protected computer defined as one used "in or affecting interstate or foreign commerce or communication,"[80] it *only* supports extraterritoriality in scenario (1), accessing a computer located outside of the United States, but *not* (2), a foreign national accessing a computer in the United States. Yet, *Ivanov* falls into the second scenario, involving a Russian hacker who had accessed computers located in Connecticut. Instead, the court should have interpreted the term "whoever" to cover the foreign hacker, but it did not. The Senate report cited above would have supported such an interpretation. Meanwhile, there is nothing in the legislative history that supports extraterritoriality in the first scenario.

If there was any doubt about the first scenario, it shall be eliminated after the definition of "protected computer" was amended post-*Ivanov* to one that is "used in or affecting interstate or foreign commerce or communication, *including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States*."[81] This added wording is the basis on which the court decided in favor

76. *Id.* at 374 (emphasis omitted).

77. *Id*.

78. *Id.* at 374–75 (citing S. REP. NO. 104-357, at 4–5 (1996)).

79. *See* Maggie Gardner, RJR Nabisco *and the Runaway Canon*, VA. L. REV. ONLINE, Oct. 2016, at 134, 145.

80. 18 U.S.C. § 1030(e)(2)(B) (2018).

81. USA PATRIOT ACT, Pub. L. No. 107-56, § 814, 115 Stat. 272, 384 (2001) (emphasis added). *See* Patricia L. Bellia, *A Code-Based Approach to Unauthorized Access Under the Computer Fraud and Abuse Act*, 84 GEO. WASH. L. REV. 1442, 1463 (2016) ("In theory, the specific reference to computers located outside the United States would overcome any presumption that Congress did not intend for the CFAA to have extraterritorial reach.").

of extraterritoriality in *Expedia*. The case involved the first scenario—Ryanair was suing Expedia for scraping flight information from its website operated in Ireland. On extraterritoriality, the court quickly concluded that the definition's reference to "a computer located outside the United States" was "as clear an indication as possible short of saying 'this law applies abroad.'"[82] However, the court failed to discuss the latter part of the definition, stipulating that the computer must be "*used in a manner that affects interstate or foreign commerce.*"[83] This is the built-in restriction of the CFAA's scope. For example, even if Ryanair does not offer flights to or from the United States,[84] can selling tickets through its overseas website satisfy this condition? If so, it is hard to imagine what kind of computer would not, as almost all websites in the world are available to users in the United States. In the next extraterritoriality case, *In re Apple Inc. Device Performance Litig*., the court did consider this condition to have been satisfied, but this was not a scraping case, and the court did not provide any elaboration.[85]

B. Independent Analysis of Civil Provision

Since *Expedia* was a civil action under the CFAA, according to *Nabisco* it was necessary to apply the two-stage approach to Section 1030(g) independently, particularly as the penalties of the civil and criminal provisions are not coextensive, just like those in RICO.[86] Here, the court sought to distinguish the CFAA from RICO. First, the court pointed to the fact that the CFAA contains an explicit definition of "protected computer," whereas RICO does not.[87] Therefore, to conclude that the civil provision does not apply extraterritorially "would require excising words from the actual statute."[88] This would have been a convincing argument if the term "protected computer" were contained in Section 1030(g), but it actually appears in Section 1030(c)(2)(C). Like its counterpart in RICO,[89] Section 1030(g) only incorporates provisions that clearly indicate extraterritoriality.[90]

82. Ryanair DAC v. Expedia, Inc., No. C17-1789RSL, 2018 WL 3727599, at *2 (W.D. Wash. Aug. 6, 2018).

83. Mentioned as a limit, but without analysis; *see id.* at *1.

84. *See* Defendant Expedia, Inc.'s Motion to Dismiss for *Forum Non Conveniens* at 2, Ryanair DAC v. Expedia, Inc., No. C17-1789RSL, 2018 WL 3748377 (W.D. Wash. May 4, 2018).

85. *In re* Apple Inc. Device Performance Litig., 347 F. Supp. 3d 434, 449 (N.D. Cal. 2018).

86. *Expedia*, 2018 WL 3727599, at *6 n.4.

87. *Id.* at *2.

88. *Id.* at *3.

89. 18 U.S.C. § 1964(a) (2010).

90. *See also* RJR Nabisco Inc. v. Eur. Cmty., 136 S. Ct. 2090, 2106 (2016).

In addition, the court reasoned that "it makes sense" for the CFAA's civil provisions to apply extraterritorially given the nature of scraping.[91] In the court's view, scraping "happens simultaneously at the locations of the accessor and the accessed computer, with limitless possible locations that the transmitted data may pass through in between . . . Many data and cloud-computing services store customer data on servers around the globe."[92] As such, the "logic [of applying CFAA's criminal provision extraterritorially] applies just as forcefully to its civil provision."[93] Admittedly, this argument has a strong appeal, but it does not fit into *Nabisco*'s two-stage framework. Apart from the plain language of "protected computer" not being contained in Section 1030(g), nothing in the legislative history backs up this reasoning. As the Supreme Court stated in *Morrison*, the court's role is to "give the statute the effect its language suggests . . . not to extend it to admirable purposes it might be used to achieve."[94]

On the other hand, the court should have considered the potential for international friction. In *Nabisco*, the Supreme Court stated that extraterritoriality in the civil provisions "creates a potential for international friction beyond that presented by merely applying U.S. substantive law to that foreign conduct."[95]

C. Uncertainty in Stage Two

The most recent extraterritoriality case is *United States v. Gasperini*.[96] It involved the defendant's unauthorized access to 140,000 computers all over the world, including more than 2,000 in the United States, in a scheme to defraud an Italian company.[97] The District Court relied on *Ivanov*'s analysis to conclude that the first stage was satisfied.[98] Again, the court confused the two scenarios, stating that "[i]n adopting [the] definition of 'protected computer,' Congress was explicit in its purpose of ensuring that the law penalized 'hackers' based outside the United States."[99] Interestingly, however, the Second Circuit declined to decide the case on the first stage on appeal. Instead, while appreciative of *Ivanov*'s "strong argument," it opted to base its decision on the second stage,

91. Ryanair DAC v. Expedia, Inc., No. C17-1789RSL, 2018 WL 3727599, at *3 (W.D. Wash. Aug. 6, 2018).

92. *Id*.

93. *Id*.

94. Morrison v. Nat'l Austl. Bank Ltd., 561 U.S. 247, 255, 270 (2010).

95. *Nabisco*, 136 S. Ct. at 2106.

96. No. 17-2479, 729 F. App'x 112 (2d Cir. 2018).

97. *Id.* at 114; Appellant's Brief at 31, United States v. Gasperini, 729 F. App'x 112 (2d Cir. Nov. 16, 2017) (No. 17-2479).

98. United States v. Gasperini, 16-CR-441 (NGG), 2017 WL 2399693, at *19 n.9 (E.D.N.Y. June 1, 2017).

99. *Id*.

stating that "[the focus of the CFAA] is gaining access to computers and obtaining information from them."[100] Consequently, the defendant's hacking of more than 2,000 computers in the United States was sufficient for a domestic application of the CFAA.[101] Technically, therefore, the Second Circuit did not conclude that the CFAA is applicable extraterritorially.[102] More importantly, at no stage did the court discuss the fact that the 2,000 U.S. computers only constituted approximately 1.7% of all computers hacked by the defendant.[103] Professor Brilmayer analogized the second stage to "some sort of center of gravity" test, "such that if the focus is situated in the United States the fact pattern as a whole can be treated as domestic."[104] If that is the test to be adopted, it is tough to justify the claim that 1.7% constitutes a "center of gravity." By analogy, in the context of personal jurisdiction, the Supreme Court found that the fact that Daimler obtained 2.4% of its worldwide sales from California was insufficient to justify assuming general jurisdiction over the German car manufacturer.[105] Similarly, in *BNSF Railway Co. v. Tyrell* (hereinafter "*BNSF*"), the Supreme Court also found that BNSF was not "at home" in Montana and denied general jurisdiction to Montana court.[106] This was so notwithstanding that BNSF had six percent of its total track miles and five percent of its total work force in the state.[107]

United States courts' liberal approach in applying CFAA extraterritorially therefore seems to be contrary to the Supreme Court's effort in recent years to rein in its legislative jurisdiction (as seen in *Morrison* and *Nabisco*),[108] as well as judicial jurisdiction (as seen in *Daimler* and *BNSF*).[109] In summary, the precedents reveal the following uncertainties regarding the extraterritorial application of the CFAA:

100. *Gasperini*, 729 F. App'x at 114.

101. *Id.*; *see also* United States v. Harris, 991 F.3d 552, 560 (4th Cir. 2021) (citing *Gasperini* in approval).

102. United States v. Gasperini, No. 17-2479, 729 F. App'x 112, 114 (2d Cir. 2018).

103. Appellant's Brief at 31, United States v. Gasperini, 729 F. App'x 112 (2d Cir. Nov. 16, 2017) (No. 17-2479).

104. Lea Brilmayer, *The New Extraterritoriality:* Morrison v. National Australia Bank*, Legislative Supremacy, and the Presumption Against Extraterritorial Application of American Law*, 40 SW. L. REV. 655, 661 (2011).

105. Daimler AG v. Bauman, 134 S. Ct. 746, 752 (2014).

106. BNSF Railway Co. v. Tyrell, 137 S. Ct. 1549 (2017).

107. *Id.* at 1554. The court also stated that BNSF derived "less than 10% of its revenue" from Montana. Although the exact number is not stated, it still appears to be substantial.

108. *See also* Kiobel v. Royal Dutch Petrol. Co., 569 U.S. 108, 116 (2013) (finding that Alien Tort Claims Act does not apply extraterritorially).

109. Interestingly, the jurisdictional application on CFAA also appears to be very liberal despite the Supreme Court's tendency to rein in its jurisdiction. *See* discussion *infra* Part III.1.

1. With reference to foreign scrapers, courts have yet to interpret the relevant term "whoever;"
2. Regarding its application to foreign computers, courts have not clarified the limiting clause "*used in a manner that affects interstate or foreign commerce or communication of the United States*;"
3. The courts did not apply the independent two-stage analysis on civil provision properly in these cases; and
4. At the second stage, the courts did not elaborate on how to assess the CFAA's "focus."

Nevertheless, all of these cases clearly indicate a willingness to apply the CFAA extraterritorially.

III. CONSTRAINTS IN CONFLICT-OF-LAWS

Even if the CFAA is to apply extraterritorially, its international impacts are still subject to constraints imposed by the following conflict-of-laws rules.

A. Personal Jurisdiction

In *Nabisco*, Justice Ginsburg highlighted the possible limitations placed on extraterritoriality by personal jurisdiction rules, including the doctrine of *forum non conveniens*:

> To the extent extraterritorial application of [U.S. statute] could give rise to comity concerns . . . those concerns can be met through doctrines that serve to block litigation in U.S. courts of cases more appropriately brought elsewhere. Where an alternative, more appropriate forum is available, the doctrine of *forum non conveniens* enables U.S. courts to refuse jurisdiction. Due process constraints on the exercise of general personal jurisdiction shelter foreign corporations from suit in the United States based on conduct abroad unless the corporation's "affiliations with the forum in which suit is brought are so constant and pervasive 'as to render it essentially at home there.'" These controls provide a check against civil [U.S.] litigation with little or no connection to the United States.[110]

To successfully sue a foreign party under the CFAA, the court must also have personal jurisdiction, either general or specific.[111] General jurisdiction is found if the defendant's contacts with the forum are "continuous and systematic."[112] In *Daimler*, Justice Ginsburg substantially limited the scope of general jurisdiction by essentially relegating the place with "continuous and systematic contacts" to either the state of incorporation or the principal place of

110. RJR Nabisco, Inc. v. Eur. Cmty., 136 S. Ct. 2090, 2115 (2016) (internal citations omitted).

111. Ryanair DAC v. Expedia Inc., No. C17-1789RSL, 2018 WL 3727599, at *3 n.3 (W.D. Wash. Aug. 6, 2018).

112. Int'l Shoe Co. v. Washington, 66 S. Ct. 154, 159 (1945).

business.[113] This means that if the scraper is based in a state in the United States, it will be subject to that state's jurisdiction, but not in other cases, even if a substantial part of the scraper's business is conducted in that state. Nor does a server location constitute a forum with "continuous and systematic contacts."[114]

However, the high threshold for general jurisdiction against foreign scrapers has been compromised by the low threshold for specific jurisdiction. The key issue is whether a foreign scraper has purposefully directed his activities at the forum.[115] As the CFAA claim has been equated to trespass,[116] courts apply the "effect test" under *Calder v. Jones* to determine specific jurisdiction.[117] This test can be broken down into three parts: "(1) intentional actions (2) expressly aimed at the forum state (3) causing harm, the brunt of which is suffered—and which the defendant knows is likely to be suffered—in the forum state."[118] In *Facebook, Inc. v. Sluchevsky*, the court found that the Ukrainian scrapers had purposefully targeted California. First, an intentional act was found: the Ukrainians scraped Facebook users' data and placed unauthorized advertisements onto their News Feeds.[119] These acts were expressly directed at California, Facebook's principal place of business, where over 37,000 users were subject to the scrapers' intentional acts.[120] As a consequence, Facebook incurred expenses of $75,000 at its California headquarters to investigate and remediate the damage.[121] Similarly, in *Craigslist v. Naturemarket*, the defendants developed and sold programs which, *inter alia*, gathered email addresses of Craigslist users from its website.[122] Since Craigslist is based in California and maintains its website there, the court found that the defendants' actions had directly targeted California in the knowledge that Craigslist would suffer harm to "its reputation and goodwill in the online community and with its

113. Daimler AG v. Bauman, 134 S. Ct. 746, 761 (2014) (citing Mary Twitchell, *Why We Keep Doing Business with Doing-Business Jurisdiction*, 2001 U. CHI. LEGAL F. 171, 184 (2000)).

114. Pfister v. Selling Source, L.L.C., 931 F. Supp. 2d 1109, 1116 (D. Nev. 2013) ("[C]ourts within this circuit have rejected the contention that server location within the forum can constitute a basis for the exercise of personal jurisdiction. As a result, [defendant's] website and its server location do not establish the continuous and systematic contacts required for this court to exercise personal jurisdiction over it.") (internal citation omitted).

115. Craigslist v. Naturemarket, 694 F. Supp. 2d 1039, 1053 (N.D. Cal. 2010).

116. Verizon Online Servs. v. Ralsky, 203 F. Supp. 2d 601, 616 (E.D. Va. 2002); NetApp, Inc. v. Nimble Storage, Inc., 41 F. Supp. 3d 816, 825 (N.D. Cal. 2014); WhatsApp v. NSO Group Techs. Ltd., 472 F. Supp. 3d 649, 672 (N.D. Cal. 2020).

117. Calder v. Jones, 465 U.S. 783, 787 (1984).

118. Panavision Int'l, L.P. v. Toeppen, 141 F.3d 1316, 1321 (9th Cir. 1998) (internal citation omitted); *see also NetApp*, 41 F. Supp. 3d at 825.

119. Facebook, Inc. v. Sluchevsky, No. 19-cv-01277-JSC, 2020 WL 5823277, at *6 (N.D. Cal. Aug. 28, 2020).

120. *Id*.

121. *Id*.

122. Craigslist v. Naturemarket, 694 F. Supp. 2d 1039, 1048–49 (N.D. Cal. 2010).

users" there.[123] Accordingly, specific jurisdiction can easily be established against a foreign scraper in the home state of a U.S. website owner because (1) scraping is always an intentional act; (2) the scraper will always know where the website owner is based; and (3) harm will usually be suffered in the website owner's home state.

In addition, the TOU of U.S. websites usually contain a forum-selection clause that designates a U.S. state as having jurisdiction.[124] If the clause is clearly drafted,[125] courts will usually respect that selection.[126] As in the case of general jurisdiction, courts have paid little attention to server location.[127] If there is "evidence that a defendant in some way targeted residents of a specific state . . . the focus would . . . instead [be] on the deliberate actions by the defendant to target or direct itself toward the forum state."[128]

Given the low threshold for specific jurisdiction, courts almost always have personal jurisdiction against scrapers whether they are based in the United States or not.[129] Of course, if neither party has anything to do with the United States, U.S. courts will have no personal jurisdiction over the defendant.[130] However, it is also unlikely that the CFAA will apply extraterritorially to that case. Thus, rules on personal jurisdiction do not impose any additional constraints on the CFAA.

B. Forum non conveniens

The doctrine of *forum non conveniens* could also be invoked to dismiss cases that would otherwise apply the CFAA extraterritorially.[131] Yet, this doctrine imposes a "heavy burden" on the defendant.[132] The defendant needs to prove that (1) another adequate and available forum exists; and (2) the balance of private- and public-interest factors makes trial in an alternative forum unnecessarily burdensome.[133] *Expedia* illustrates the difficulties in establishing

123. *Id.* at 1050, 1053.

124. *Id.* at 1052.

125. WhatsApp v. NSO Group Techs. Ltd., 472 F. Supp. 3d 649, 668 (N.D. Cal. 2020).

126. M/S Bremen v. Zapata Off-Shore Co., 407 U.S. 1, 6 (1972); *see Craigslist*, 694 F. Supp. 2d at 1052.

127. *WhatsApp*, 472 F. Supp. 3d at 670, 671; *see* Christie v. Nat'l Inst. for Newman Stud., 258 F. Supp. 3d 494, 505 (D.N.J. 2017).

128. Advanced Tactical Ordnance Sys., L.L.C. v. Real Action Paintball, 751 F.3d 796, 803 (7th Cir. 2014); *see also Christie*, 258 F. Supp. 3d at 506.

129. *See* NetApp v. Nimble Storage, 41 F. Supp. 3d 816, 823 (N.D. Cal. 2014); *Christie*, 258 F. Supp. 3d at 497; *Craigslist*, 694 F. Supp. 2d at 1053; *WhatsApp*, 472 F. Supp. 3d at 673 n.7; Ajuba Int'l, L.L.C. v. Saharia, 871 F. Supp. 2d 671, 684 (E.D. Mich. 2012).

130. *See* Ryanair DAC v. Expedia Inc., No. C17-1789RSL, 2018 WL 3727599, at *3 n.3 (W.D. Wash. Aug. 6, 2018).

131. Daimler AG v. Bauman, 134 S. Ct. 746, 771 (2014) (J. Sotomayor, concurring).

132. Sinochem Int'l Co. v. Malay. Int'l Shipping Corp., 127 S. Ct. 1184, 1191 (2007).

133. Piper Aircraft v. Reyno, 454 U.S. 235, 258 (1981).

forum non conveniens in scraping cases. Although the court found that Ireland was an adequate and available forum, neither the private- nor public-interest factors favored dismissal.[134] For private-interest factors relating to availability of evidence and parties' convenience, evidence in scraping cases is usually available in electronic form, "which makes its 'location' much less salient a factor."[135] For public-interest factors relating to the forum's local interests, the court found such interest in "adjudicating alleged violations of federal law committed by local companies."[136] Furthermore, as the CFAA is a federal law, it would not burden the court with applying foreign law.[137] Where a U.S. website owner sues a foreign scraper in its home forum, the court will give greater deference to the choice as "it is reasonable to assume that this choice is convenient."[138] *Forum non conveniens* also failed in two other CFAA cases, although neither involved scraping.[139]

International comity is an alternative basis on which U.S. courts may decline jurisdiction, but with more focus on interests of foreign sovereignty.[140] In *Expedia*, the court focused on the location and nature of the conduct and the balancing of United States and foreign interests.[141] First, despite the fact that Ryanair's servers were located overseas, the court adopted a liberal interpretation and found that some of the defendant's actions, namely the data gathering, occurred in the United States.[142] On foreign interest, the court adopted the narrow view taken in *Hartford Fire Insurance Co. v. California*[143] on conflict with foreign law, limiting it to "situations when complying with two laws or judgments is impossible."[144] It thus concluded that "Ireland has no interest in an American company avoiding (or not avoiding) liability under an American statute" even if the conduct is legal under Irish law.[145] If future cases take the *Expedia* court's liberal interpretation of conduct and narrow view on foreign interest, dismissals on the grounds of international comity will be rare.

134. *Expedia*, 2018 WL 3727599, at *5.

135. *Id.*; *see also* Weisel Partners L.L.C. v. BNP Paribas, No. C 07-6198, 2008 WL 3977887, at *11 (N.D. Cal. Aug. 26, 2008).

136. Ryanair DAC v. Expedia Inc., No. C17-1789RSL, 2018 WL 3727599, at *5 n.3 (W.D. Wash. Aug. 6, 2018).

137. *Id*.

138. *Piper Aircraft*, 454 U.S. at 255–56; *Weisel*, 2008 WL 3977887, at *8.

139. *Weisel*, 2008 WL 3977887, at *9; *see* Ajuba Int'l, L.L.C. v. Saharia, 871 F. Supp. 2d 671, 685–88 (E.D. Mich. 2012).

140. *See* William S. Dodge, *International Comity in American Law*, 115 COLUM. L. REV. 2071, 2109 (2015).

141. Ryanair DAC v. Expedia Inc., No. C17-1789RSL, 2018 WL 3727599, at *5 (W.D. Wash. Aug. 6, 2018).

142. *Id.* at *3, *6.

143. 509 U.S. 764, 797 (1993).

144. *Expedia*, 2018 WL 3727599, at *6

145. *Id*.

C. Choice-of-law

TOU also often contain a choice-of-law clause. If the choice-of-law clause designates U.S. law as the governing law, it will have no impact on the application of the CFAA. But what if the choice-of-law clause provides for foreign law—as in *Expedia*, where Irish law was stipulated in the TOU?[146] Will that rule out the application of the CFAA? In *Expedia*, the court rejected that argument since the choice-of-law clause would only be applicable if the cause of action was breach of the TOU.[147] In that case, Ryanair cleverly only brought a CFAA claim in the United States.[148] Accordingly, choice-of-law rules can only limit the application of a state version of the CFAA, such as California's Comprehensive Computer Data Access and Fraud Act ("CCDAFA"),[149] or other state law claims,[150] but not the CFAA. Foreign website owners therefore do not have to worry about the foreign choice-of-law clause barring CFAA claims in U.S. courts, but can enjoy the benefit of such a clause when they sue scrapers overseas under a favorable governing law.

D. Enforcement of Foreign Judgments

The CFAA can award both damages and an injunction.[151] In most cases, due to the difficulty in proving large damages, injunctions are more effective.[152] However, most countries do not enforce foreign non-monetary judgments.[153] In particular, other countries have long been offended by the extraterritorial application of U.S. legislation in the area of antitrust and securities law,[154] so are unlikely to give effect to an injunction under the CFAA. The international effect of the CFAA will be limited in this sense.

The reverse is also true, however. Enforcement of foreign injunctions in the United States is uncertain at best.[155] This is why Ryanair particularly filed a CFAA proceeding against Expedia in Washington, despite having also filed

146. *Id.* at *3.

147. *See id*.

148. *Id.* at *1.

149. *See* Farmers Ins. Exch. v. Auto Club Grp., 823 F. Supp. 2d 847, 856–58 (N.D. Ill. 2011).

150. *See* Southwest Airlines Co. v. BoardFirst, L.L.C., No. 06-CV-0891-B, 2007 WL 4823761, at *3 (N.D. Tex. Sept. 12, 2007).

151. *See In re* Lenovo Adware Litig., No. 15-md-02624, 2016 WL 6277245, at *19 (N.D. Cal. Oct. 27, 2016).

152. *See* Trader Corp. v. CarGurus, Inc. (2017), 137 O.R. 3d 587, ¶ 72 (Can. Ont. Sup. Ct. J.) (awarding only CAD 305,064).

153. Canada is an exception, see Pro Swing Inc. v. Elta Golf Inc., 2006 SCC 52, 613–14 (Can.).

154. *See In re* Vitamin C Antitrust Litig., 837 F.3d 175, 193–94 (2d Cir. 2016).

155. *See* Lothar Determann & Saralyn M. Ang-Olson, *Recognition and Enforcement of Foreign Injunctions in the United States*, *in* 1 LAWS OF INT'L TRADE 98, at 98-5, 98-6 (Thomson/West 2007).

proceedings in Ireland.[156] In contrast, Ryanair was comfortable suing Vola, a Romanian company that also happens to be a third-party online travel agency, in Ireland instead of Romania,[157] probably because an Irish injunction, as a judgment rendered by a European Union member state, will automatically be given effect in Romania under the Recast Brussels Regulations.[158] Consequently, although enforcement rules limit the CFAA's international effect, they also force foreign website owners to file CFAA claims in the United States if they want to block scraping activities in the United States. Furthermore, considering the size of the U.S. market, in many cases there is no need to seek recognition of a U.S. injunction overseas. For example, in Ryanair's action against Booking Holdings, it also sued a number of Booking.com overseas subsidiaries, including Booking.com (the Netherlands) and Agoda.com (Singapore), both of which do business in the United States.[159]

IV. COMPARING THE CFAA WITH OTHER CAUSES OF ACTION

This section compares the CFAA with other causes of action, both under U.S. law and foreign laws. These include breach of contract, trespass, and copyright infringement.[160] It is observed that the CFAA claim is "far easier to prove."[161] This provides motivation for a website owner to take advantage of the CFAA's extraterritoriality.

Compared with the CFAA, other causes of action are more difficult to establish, whether under U.S. or foreign laws. In breach of contract, the main difficulty lies in the recognition of the TOU, which usually explicitly prohibit scraping, as a valid contract.[162] Common-law courts around the world agree that if the TOU are contained in a "clickwrap," i.e., the website user is required to click on an "I agree" box to indicate assent, a valid contract will be found.[163] However, on many websites, the TOU are instead contained in a

156. Ryanair DAC v. Expedia Inc., No. C17-1789, 2018 WL 3727599, at *5 (W.D. Wash. Aug. 6, 2018).

157. Ryanair DAC v. SC Vola.ro SRL [2019] IEHC 239, ¶ 1 (H. Ct.) (Ir.).

158. Regulation 1215/2012 of the European Parliament and of the Council of 12 December 2012 on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters 2012 O.J. (L 351) 6, 14, 15 (EU).

159. Complaint for Violation of the Computer Fraud and Abuse Act at ¶¶ 5, 11, Ryanair DAC v. Booking Holdings, Inc., No. 1:20-cv-01191-UNA (D. Del. Sept. 4, 2020).

160. *See, e.g.*, EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 580 (1st Cir. 2001); hiQ Labs, Inc. v. LinkedIn Corp., No. 17-cv-03301, 2021 WL 1531172, at *3, *11 (N.D. Cal. Apr. 19, 2021).

161. *See* Galbraith, *supra* note 15, at 323–24.

162. *See* Ryanair Ltd. v. On The Beach Ltd. [2013] IEHC 124, ¶¶ 42–43 (Ir).

163. *See* i.Lan Sys. v. Netscout Serv. Level Corp., 183 F. Supp. 2d 328, 338 (D. Mass. 2002). For foreign authorities, *see, e.g.*, Rudder v. Microsoft Corp., [1999] O.J. No. 3778, ¶¶ 14, 17 (Can. Ont. Sup. Ct. J.) (QL); Ryanair Ltd. v. On The Beach Ltd. [2013] IEHC 124, ¶ 42 (Ir).

"browsewrap,"[164] a separate page accessed via a link, usually at the bottom of the webpage.[165] Whether browsewrapped TOU constitute a binding contract depends on whether the user has actual or constructive knowledge of the terms.[166] Although there are some successful cases where scrapers have been deemed bound by terms contained in a browsewrap,[167] it is ultimately a question of fact as to whether the user had knowledge of the terms.[168] In contrast, at least under the literal interpretation of the CFAA, a court may find that a valid contract is unnecessary for a finding of unauthorized access.

Alternatively, website owners may pursue an allegation of copyright infringement.[169] However, copyright claims have failed in most cases.[170] The threshold elements in copyright infringement are (1) the ownership of a valid copyright; and (2) the copying of the original elements of the work.[171] Yet, many website owners, such as LinkedIn, do not own the data stored on their sites.[172] Even with ownership, in *Ticketmaster L.L.C. v. Prestige Entertainment, Inc*., it was held that the website owner had failed to establish the second condition since in the process of scraping the site the defendant had engaged in no more than automatic background copying.[173] In contrast, there is no requirement as to either ownership or type of information under the CFAA.[174] Another copyright hurdle to overcome is the defense of "fair use" under U.S. law.[175] One important factor is the amount of substantiality of the copying.[176] In *Associated Press v. Meltwater U.S. Holdings, Inc.*, the Associated Press sued Meltwater for scraping the content of its news articles.[177] Meltwater took between 4.5% and 61% of the articles, as well as the lede of every story.[178] The court found this factor to weigh

164. *See, e.g.*, *hiQ*, 2021 WL 1531172, at *6.

165. *See* Nguyen v. Barnes & Noble, 763 F.3d 1171, 1175–76 (9th Cir. 2014).

166. *Id.* at 1176 (citing Van Tassell v. United Mktg. Grp., L.L.C., 795 F. Supp. 2d 770, 790 (N.D. Ill. 2011)).

167. *See* Register.com v. Verio, 356 F.3d 393, 403 (2d Cir. 2004). For foreign authority, *see, e.g.*, Century 21 Canada Ltd. P'ship v. Rogers Commc'ns Inc., 2011 BCSC 1196, ¶ 108 (Can.).

168. *See* hiQ Labs, Inc. v. LinkedIn Corp., No. 17-cv-03301, 2021 WL 1531172, at *6 (N.D. Cal. Apr. 19, 2021).

169. *See, e.g.*, Associated Press v. Meltwater U.S. Holdings, Inc., 931 F. Supp. 2d 537, 541 (S.D.N.Y. 2013).

170. *See* Kathleen C. Riley, *Data Scraping as a Cause of Action: Limiting Use of the CFAA and Trespass in Online Copying Cases*, 29 FORDHAM INTELL. PROP., MEDIA & ENT. L.J. 245, 276 (2018).

171. *See Associated Press*, 931 F. Supp. 2d at 549.

172. *See hiQ*, 2021 WL 1531172, at *7.

173. 306 F. Supp. 3d 1164, 1171–72 (C.D. Cal. 2018).

174. *See* 18 U.S.C. § 1030 (2018).

175. *See id*.; *Associated Press*, 931 F. Supp. 2d at 550.

176. *Id.*

177. Associated Press v. Meltwater U.S. Holdings, Inc., 931 F. Supp. 2d 537, 541 (S.D.N.Y. 2013).

178. *Id.* at 558.

strongly against the defense of fair use.[179] However, the court also emphasized that there is no clear-cut rule as to how much copying exceeds fair use.[180] Under Canadian law, there is a similar defense of "fair dealing."[181] The CFAA, however, has no such defense. The purpose of the unauthorized access does not matter. Apart from copyright infringement, it is also difficult to bring a successful case for other types of intellectual property violations abroad. In Ryanair's suit against PR Aviation BV in the Netherlands, the Court of Justice of the European Union issued a preliminary ruling which found first that Ryanair's data set was not protected by the Dutch copyright law,[182] and second that there is no *sui generis* right to the data set under Directive 96/9 and the related Database Law, as Ryanair had not made the requisite "substantial investment."[183]

Another alternative is trespass to chattels. United States courts have adapted the offense of trespass in tort to scraping.[184] However, apart from the theoretical difficulty in fitting the age-old doctrine to cyberspace,[185] another practical difficulty is the burden on the plaintiff to show actual damage to its computers or operations.[186] In *Ticketmaster Corp. v. Tickets.com, Inc.*, the court held that neither the information obtained by scraping nor the expenses incurred in fending off the scraper's "spider" software were sufficient to constitute the required damage.[187] Comparatively, we have seen how similar expenses could constitute a loss under the CFAA,[188] and the threshold is only $5,000.[189] Using trespass in scraping cases is an approach that is rather unique to U.S. courts. For example, in England and Wales, trespass "has never been applied to electronic interferences and has scarcely been used in any other context."[190] Ryanair recently sought to apply trespass to chattel in its case against Skyscanner.[191]

179. *Id*.

180. *Id*.

181. *See* Trader Corp. v. CarGurus, Inc. (2017), 137 O.R. 3d 587, ¶¶ 35–40 (Can. Ont. Sup. Ct. J.).

182. Case C-30/14, Ryanair Ltd. v. PR Aviation BV, ECLI:EU:C:2015:10, ¶¶24–25 (Jan. 15, 2015).

183. *Id.* at ¶ 22.

184. *See* Ticketmaster Corp. v. Tickets.com, Inc., No. CV997645HLHVBKX, 2003 WL 21406289, at *3 (C.D. Cal. Mar. 7, 2003).

185. *See* Lemley, *supra* note 39, at 527.

186. *See Ticketmaster Corp.*, 2003 WL 21406289, at *3.

187. *Id.* at *3–4.

188. *See* Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058, 1066 (9th Cir. 2016).

189. *See* Appellant's Brief at 11–12, United States v. Gasperini, 729 F. App'x 112 (2d Cir. Nov. 16, 2017) (No. 17-2479).

190. Liu, *supra* note 17, at 44–45.

191. Ryanair DAC v. Skyscanner Ltd. [2020] IEHC 399, ¶ 74 (H. Ct.) (Ir.).

However, Ryanair admitted that trespass only applies to corporeal property, and the Irish court swiftly dismissed the claim.[192]

Lastly, as highlighted in Part III.C above, since the CFAA will be applied as federal law by U.S. courts without the need to undergo at times complicated choice-of-law analysis like state law claims, it could be an added advantage of suing scrapers under CFAA.

CONCLUSION

This Article demonstrates three facts and makes one advocation. The first fact is that U.S. courts have consistently applied the CFAA extraterritorially, despite the absence of comprehensive legal analyses. The second is that safeguards under conflict-of-laws provide few limitations on the CFAA's international effects. The third is that the CFAA sets a lower threshold for web scraping than other substantive causes of action under both U.S. and foreign laws, particularly when the court adopts a broad interpretation of "without authorization." The combination of these three facts makes the CFAA highly attractive to website owners. This will have a vast impact on the governance of web scraping worldwide. The author therefore suggests that U.S. court should consider the international impacts of its interpretation of the substantive provisions of the CFAA in upcoming cases.

In terms of conflict analysis, in Parts II and III we have seen that courts take account of international effects in considering extraterritoriality and personal jurisdiction. If a substantive law will conflict with a foreign law, U.S. courts will be less likely to apply the law extraterritorially or to assume jurisdiction. Similarly, international comity is another basis on which a court may decline to exercise personal jurisdiction. By the same token, U.S. courts should limit their interpretation of substantive law when that law is capable of applying extraterritorially. If the Supreme Court interprets "without authorization" to cover violations of TOU, it will cause vast disruption to web scraping internationally. In addition, in interpreting this phrase, the circuit courts have referred to the rule of lenity, as the interpretation affects both criminal and civil liabilities.[193] By analogy, courts should also interpret the term with care, since it has such a large potential impact internationally.

This is not just because the United States has to cling to the vague notion of comity, but because it is in its national interest. There is always a concern that other countries will retaliate. In elaborating the need to limit the extraterritoriality of the Alien Tort Statute, the Supreme Court expressed the concern that other countries "could hale our citizens into their courts for alleged

192. *Id*.

193. *See* hiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985, 1003 (9th Cir. 2019); Ajuba Int'l L.L.C. v. Saharia, 871 F. Supp. 2d 671, 687 (E.D. Mich. 2012); Bell Aerospace Servs., Inc. v. U.S. Aero Servs., Inc., 690 F. Supp. 2d 1267, 1272 (M.D. Ala. 2010).

violation of the law of nations occurring in the United States."[194] Extraterritorial applications of U.S. laws have already spawned defensive legislation from foreign jurisdictions in the area of antitrust.[195] In 2020, China revised its Securities Act to give it extraterritorial application.[196] China's Ministry of Commerce also recently promulgated a new measure to counter the extraterritorial application of foreign law to Chinese nationals.[197] Under the new measure, where any such national, including any legal person or other Chinese organization, is restricted by foreign legislation and other measures from engaging in normal economic, trade, and related activities with a third state or its nationals, it will have to file a report with the relevant Chinese department. It may in turn issue a prohibition order if it finds the foreign legislation to be an "unjustified extra-territorial application."[198]

Similarly, U.S. courts should also reexamine the CFAA's exterritoriality. This is not to say that the CFAA cannot apply extraterritorially. However, given that the CFAA was not originally designed to serve as a tool to regulate international web scraping,[199] a more conservative approach to its interpretation may be more appropriate. In the event that Congress identifies a need to expand the CFAA's international reach, it could make proper amendments to its extraterritorial aspects to minimize unnecessary conflicts.[200] We have seen similar amendments to the Securities Act to overrule part of the *Morrison* decision, so as to restore the extraterritorial application of the Securities Exchange Act in actions brought by the Securities Exchange Commission or the Department of Justice, but not those brought by private parties.[201] More recently, Congress has also shown, in the recent passing of the Clarifying Lawful Overseas Use of Data Act, that amendments can be made swiftly to the extraterritoriality of the Stored Communications Act.[202] Therefore, there is no urgency for the courts to unleash the CFAA's full extraterritorial reach until the

194. Kiobel v. Royal Dutch Petrol. Co., 569 U.S. 108, 124 (2013).

195. *See, e.g.*, Protection of Trading Interests Act (1980) (UK).

196. *See* Zhonghua Renmin Gongheguo Zhengquan Fa (《中华人民共和国证券法》) [Securities Law of the People's Republic of China], (promulgated Dec. 28, 2019, implemented Mar. 1, 2020), art. 2 (China).

197. *See* MOFCOM Order No. 1 of 2021 on Rules on Counteracting Unjustified Extraterritorial Application of Foreign Legislation and Other Measures, art. 1–2 (China), *available at* http://english.mofcom.gov.cn/article/policyrelease/questions/202101/20210103029708.shtml.

198. *See id.* at art. 5–7.

199. *See supra* Part I.1.

200. *See* Foreign Trade Antitrust Improvements Act, 15 U.S.C. § 6a (2018).

201. *See* Dodd-Frank Wall Street Reform and Consumer Protection Act (Reform Act), Title IX (Investor Protection Act), Pub. L. No. 111-203, § 929P, 124 Stat. 1376, 1865 (2010). *See also* Hugh B. Hamilton III, *At the Water's Hedge: International Insider-Trading Enforcement After* Morrison, 68 DUKE L.J. 1003, 1040 (2019).

202. *See* Sabrina A. Morris, *Rethinking the Extraterritorial Scope of the United States' Access to Data Stored by a Third Party*, 42 FORDHAM INT'L L.J. 183, 208–17 (2018).

pros and cons of international web scraping have been given more comprehensive discussion.