Santa Clara University
School of Law

Santa Clara Law Review

Volume 56 | Number 1 Article 1

2-4-2016

Justice for J-Law?

William Schildknecht

JUSTICE FOR J-LAW?

SPECIFIC PERSONAL JURISDICTION OVER INTERNET TORTS IN THE WAKE OF *WALDEN V. FIORE*

William Schildknecht*

TABLE OF CONTENTS

* Many thanks to Professor Kathryn Abrams for her advice and encouragement and Sarah Chai for her thoughtful and meticulous edits.

Respondents warn that if we decide petitioner lacks minimum contacts in this case, it will bring about unfairness in cases where intentional torts are committed via the Internet . . . [w]e leave questions about virtual contacts for another day.[1]

INTRODUCTION

On the morning of August 31, 2014, a collection of celebrities, including famous actresses, models, and athletes, awoke to discover that their intimate and often explicit images had been posted across Internet message boards and other websites.[2] All told, this widespread hack revealed the private lives of over 100 celebrities.[3] Besides causing extreme embarrassment for those affected, the theft and distribution of the photographs thrust the threat of Internet torts into the spotlight and revealed the importance of providing adequate remedies to injured parties. One of the affected, actress Jennifer Lawrence, described the hack as "disgusting," noting "[t]he law needs to be changed, and we need to change."[4]

Though the laws may not be changed quickly, this Article anticipates that celebrities who had their photos released will bring lawsuits against the hackers under current laws. However, no matter how robust our state or national data privacy regimes become, they will provide no relief if would-be defendants are beyond the jurisdiction of the American legal system. While a great deal of research has been devoted to the study of civil litigation arising out of Internet contacts (often in the context of e-commerce),[5] there is little research

---

1. Walden v. Fiore, 134 S. Ct. 1115, 1125 n.9 (2014).

2. *See, e.g.*, Rich McCormick, *Hack Leaks Hundreds of Nude Celebrity Photos*, THE VERGE (Sept. 1, 2014, 2:29 AM), http://www.theverge.com/2014/9/1/6092089/nude-celebrity-hack.

3. *See* McCormick, *supra* note 2.

4. Sam Kashner, *Both Huntress and Prey*, VANITY FAIR (Nov. 2014), http://www.vanityfair.com/hollywood/2014/10/jennifer-lawrence-photo-hacking-privacy.

5. *See, e.g.*, Sasha Segall, *Jurisdictional Challenges in the United States Government's Move to Cloud Computing Technology*, 23 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 1105 (2013); Allyson W. Haynes, *The Short Arm of the Law: Simplifying Personal Jurisdiction over Virtually Present Defendants*, 64 U. MIAMI L. REV. 133, 150–51 (2009); A. Benjamin Spencer, *Jurisdiction and the Internet: Returning to Traditional Principles to Analyze Network-Mediated Contacts*, 2006 U. ILL. L. REV. 71, 80–85 (2006); Michael A. Geist, *Is There a There There? Toward Greater Certainty for Internet Jurisdiction*, 16 BERKELEY

on the jurisdictional conditions precedent to making use of those laws in the tort context.[6] This Article breaks new ground by considering the Supreme Court's most recent pronouncement on specific personal jurisdiction in the case of *Walden v. Fiore*. Specifically, this Article analyzes how the *Walden* decision complicates civil actions—particularly against international defendants—arising out of torts committed through the Internet. This Article exposes these challenges through the lens of the 2014 celebrity photo hack. Because data theft in the age of cloud computing disregards traditional notions of sovereignty and strains the current legal framework, the problem this Article poses will vex lower courts until Internet jurisdiction issues are provided greater clarity.

In Part II, this Article introduces a hypothetical test case where one of the affected celebrities, Jennifer Lawrence,[7] attempts to press a tort claim in federal court in California for relief against an international defendant. In Part III, this Article considers the 2014 Supreme Court decision in *Walden v. Fiore*, where the Court unanimously reaffirmed its commitment to the "minimum contacts" test of specific personal jurisdiction as a threshold for permitting suit against out-of-state defendants.[8] The case recognized, but declined to resolve, the petitioners' concerns that the reinforced rules might have implications for intentional torts perpetrated through the Internet.[9] While the Court's restraint is laudable, this Article argues that the lack of clear guidance on how to define specific personal jurisdiction in Internet torts in light of *Walden* has created a potential zone of ambiguous or non-existent personal jurisdiction, especially in the context of a suit against international defendants. In Part IV, this Article applies the *Walden* decision to the facts of our hypothetical Lawrence case, revealing the weaknesses under the current jurisdictional framework. Ultimately, this

---

TECH. L.J. 1345, 1347–49 (2001).

6. *See, e.g.*, Catherine Ross Dunham, *Zippo-ing the Wrong Way: How the Internet Has Misdirected the Federal Courts in Their Personal Jurisdiction Analysis*, 43 U.S.F. L. REV. 559, 574–75 (2009).

7. *See, e.g.*, *Nude Photos of Jennifer Lawrence Leak*, PEOPLE (Aug. 31, 2014), http://www.people.com/article/jennifer-lawrence-nude-photos.

8. Walden v. Fiore, 134 S. Ct. 1115, 1123 (2014).

9. *Id.* at 1125, n. 9.

Article concludes in Part V by exploring potential remedies to this gap in the jurisdictional jurisprudence.

I. TEST CASE: 2014 CELEBRITY PHOTO HACK

In August 2014, hackers released to the public a cache of stolen images of over 100 celebrities on passive image hosting websites.[10] While there is no certain theory on how the images were stolen and the project is believed to be the work of many different individuals working independently,[11] it is widely accepted that hackers obtained the images remotely by accessing phone data over the Internet that was stored in Apple data centers.[12] One of those celebrities acutely affected by the hack was Jennifer Lawrence.[13] This Article considers a hypothetical (but very probable) sequence of events surrounding Lawrence's attempt to sue those who stole and shared her photographs for civil damages.

A. Data Storage in the Cloud: Locating the Source of the Theft

In order to develop this hypothetical, a working understanding of how Internet data in "the cloud" is stored and accessed is a fundamental first step. "The cloud" is an evolution in Internet usage towards centralized off-site computing systems and Internet-based storage.[14] This process permits devices with limited storage to access large amounts of data stored offsite.[15] Examples include Google Docs and Gmail[16] as well as Apple's iCloud,[17] the database

10. *See* McCormick, *supra* note 2.

11. *See, e.g.*, James Vincent, *Nude Celebrity Photo Hacks the Work of an "Underground Nude Trading Ring," Reports Claim*, THE INDEPENDENT (Sept. 2, 2014), http://www.independent.co.uk/life-style/gadgets-and-tech/naked-celebrity-photo-hacks-the-work-of-an-underground-nude-trading-ring-claim-reports-9706787.html.

12. *See Nude Photos of Jennifer Lawrence Leak*, *supra* note 7; *see also* Justin Worland, *How That Massive Celebrity Hack Might Have Happened*, TIME (Sept. 1, 2014), http://time.com/3247717/jennifer-lawrence-hacked-icloud-leaked/.

13. *See Nude Photos of Jennifer Lawrence Leak*, *supra* note 7.

14. *See* David Lametti, *The Cloud: Boundless Digital Potential or Enclosure 3.0?*, 17 VA. J.L. & TECH. 190, 195 (2012).

15. Maamar Ferkoun, *Top 7 Most Common Uses of Cloud Computing*, I.B.M. (Feb. 6, 2014), http://thoughtsoncloud.com/2014/02/top-7-most-common-uses-of-cloud-computing/.

16. Lametti, *supra* note 14, at 209.

from which the stolen photographs were drawn. Databases like these, which offer access over the Internet to stored content, depend on large, centralized storage "data centers."[18] The increased use of cloud services has led to a subsequent increase in the construction of large-scale data centers around the world to house that information.[19] Though the data is always accessible on mobile devices, it is stored locally at the data center (in addition to possibly being stored locally on the user's device).[20] By way of example, the music-streaming program Spotify provides users the option of downloading music for offline consumption.[21] Otherwise, the music is available over an Internet connection by streaming it directly through the company's program.[22] In either case, the music is accessed from physical storage on site at Spotify's data centers in Stockholm, London, Ashburn, or San Jose (whichever is closest to the location of the user.).[23] As a result, a person looking to access Spotify's music does so by tapping the physical information held in the nearest data

---

17. *iCloud Drive*, APPLE, https://www.apple.com/icloud/ (last visited Mar. 4, 2014) ("[W]ith iCloud Drive, you can safely store all your documents in iCloud and access them from your iPhone, iPad, iPod touch, Mac, or even PC.").

18. Paul Stryer, *Understanding Data Centers and Cloud Computing*, GLOBAL KNOWLEDGE WHITE PAPERS (2010), http://www.globalknowledge.nl/content/files/documents/White-Papers/Cloud-Computing-White-Paper-Understanding-Data-Centers ("A data center (sometimes called a server farm) is a centralized repository for the storage, management, and dissemination of data and information.").

19. *See, e.g.*, Vanessa Desloires, *IBM Opens Data Centre in Melbourne to Capture Cloud Demand*, FINANCIAL REVIEW (Aug. 26, 2014), http://www.afr.com/p/technology/ibm_opens_data_centre_in_melbourne_8EJHXPvO6ftTZmDYfahSYP; Penny Jones, *U.S. Cloud Providers Lead EU Demand for Data Centers*, DATA CENTER DYNAMICS (Mar. 7, 2014), http://www.datacenterdynamics.com/focus/archive/2014/03/us-cloud-providers-lead-eu-demand-data-centers; Rich Miller, *Cloud Growth Spurs Demand for Data Centers*, DATA CENTER KNOWLEDGE (Mar. 12, 2012), http://www.datacenterknowledge.com/archives/2012/03/12/cloud-growth-spurs-demand-for-data-centers/.

20. *See* Zuzanna Blaszkiewicz, *What You Need to Know About Syncing Photos in iCloud,* SOFTONIC (Oct. 22, 2014), http://features.en.softonic.com/what-you-need-to-know-about-syncing-photos-in-icloud.

21. *Listen Offline*, SPOTIFY, https://support.spotify.com/us/learn-more/guides/#!/article/Listen-offline (last visited Mar. 4, 2015).

22. Farhad Manjoo, *The World's Greatest Music* Service, SLATE (July 16, 2009), http://www.slate.com/articles/technology/technology/2009/07/the_worlds_greatest_music_service.html.

23. David Poblador I. Garcia, *Spotify: Data Center & Backend Buildout*, SPOTIFY (July 10, 2013), http://www.slideshare.net/davidpoblador/spotify-bcn2013slideshare.

center.

Some liberties must be taken with the hypothetical at this juncture. At the time that Jennifer Lawrence's photos were stolen, it appears that all of Apple's iCloud data was stored in U.S. data centers in California and North Carolina.[24] Were it the case that the data was stolen from a U.S. data-center, personal jurisdiction over the defendant would likely be proper in the state containing the breached data center.[25] However, foreign-based digital theft of American information is an increasing problem.[26] Companies like Google and Microsoft, which are also victimized by data theft, store their data in centers in other countries.[27] In addition, Apple has announced that it will be expanding its data center servers into other countries including Curacao, the Netherlands, and China.[28] Furthermore, it is hypothetically possible that some of the data at issue was stolen from foreign data servers owned by third party application providers who store data for Apple.[29] Therefore, it

---

24. *See, e.g.*, Apple Insider Staff, *Apple to Build Second "Tactical Datacenter" at Maiden, NC Facility*, APPLE INSIDER (Feb. 20, 2014), http://appleinsider.com/articles/14/02/20/apple-to-build-second-tactical-datacenter-at-maiden-nc-facility; Rich Miller, *Apple Buys California Data Center*, DATA CENTER KNOWLEDGE (Feb. 27, 2006), http://www.datacenterknowledge.com/archives/2006/02/27/apple-buys-california-data-center/.

25. *See* MacDermid v. Deiter, 702 F.3d 725, 731 (2d Cir. 2012) (finding that defendant was subject to jurisdiction in Connecticut because she accessed servers there to steal confidential information). However, this ruling does not mean that the question of who has jurisdiction is completely settled. *See* Damon Andrews & John Newman, *Personal Jurisdiction and Choice of Law in the Cloud*, 73 MD L. REV. 358, 361 (2013). The hypothetical in this article is stretched to focus on the international defendant because it presents unique challenges that are certain to arise in time even if they do not apply directly to Jennifer Lawrence's circumstances.

26. Martin Giles, *Defending the Digital Frontier*, THE ECONOMIST (July 12, 2014), http://www.economist.com/news/special-report/21606416-companies-markets-and-countries-are-increasingly-under-attack-cyber-criminals.

27. Google data center locations are available at: http://www.google.com/about/datacenters/inside/locations/; Microsoft centers are located at: http://www.microsoft.com/online/legal/v2/en-us/MOS_PTC_Geo_Boundaries.htm.

28. Neil Hughes, *Apple Reportedly Expanding Global Data Center Presence with New Facility in Curacao*, APPLE INSIDER (Aug. 16, 2014), http://appleinsider.com/articles/14/08/16/apple-reportedly-expanding-global-data-center-presence-with-new-facility-in-curacao.

29. According to Apple's privacy provisions, the company "shares personal information with companies who provide services such as . . . managing and enhancing customer data . . . ." "These companies are obligated to protect your information and may be located wherever Apple operates." *Apple Privacy Policy*,

is likely in the future—if it is not already true—that users who have had their data stolen will be forced to pursue their action against a foreign defendant who obtained the information from a foreign data center. This hypothetical will incorporate some of these developing trends to demonstrate the difficulties that will arise in bringing civil claims over breaches of foreign data centers.

B. Jennifer Lawrence's Hypothetical Litigation

Suppose that Jennifer Lawrence decides to bring legal action against those who injured her by stealing and releasing her photos.[30] Further assume that research by Lawrence's attorneys reveals that her stolen photographs were stored at Apple's data center in the Netherlands. The data was stored at the Netherlands data center because it was the nearest data center when the photos were uploaded to the cloud while Lawrence was on set in Europe for the filming of a new movie.[31] After taking the pictures and uploading them to the cloud (unbeknownst to Lawrence, to be stored at the Dutch data center), she returned home to California, and it was there that she became aware that the photos had been stolen in the intervening period. In addition, the lawyers discover that the individual who stole Lawrence's photos from iCloud committed his nefarious acts from a computer terminal in Russia.[32] The individual has never

---

APPLE, https://www.apple.com/legal/privacy/en-ww/ (last visited Mar. 2, 2015).

30. In fact Lawrence has already sought legal representation to remove images posted on the Internet pursuant to the Digital Millennium Copyright Act. *See, e.g.*, TMZ Staff, *Jennifer Lawrence Non-Selfie Nudes Could Pose Legal Hurdle*, TMZ (Sept. 3, 2014), http://www.tmz.com/2014/09/03/jennifer-lawrence-nude-photos-leak-hacked-copyright/.

31. Data is often uploaded and stored to servers that are nearest to the location of the uploader to facilitate quick data uploads and downloads. *See In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.*, 13 MAG. 2814, 2014 WL 1661004 (S.D.N.Y. Apr. 25, 2014), at *2 ("[W]here a particular user's information is stored depends in part on a phenomenon known as 'network latency'; because the quality of service decreases the farther a user is from the datacenter where his account is hosted, efforts are made to assign each account to the closest datacenter.").

32. Russia was chosen because of the limited international cooperation between the countries and because of the high incidence of cyber-theft in the country. *See, e.g.*, Jeremy Bender, *Report: Russian Cyber Crime Syndicate Linked to Neiman Marcus Theft*, BUSINESS INSIDER (Apr. 7, 2015), http://www.businessinsider.com/neiman-marcus-cyber-attack-russian-hackers-2014-4.

visited the United States and does not engage in any business with the United States. Though the pictures of Lawrence were accessible to Internet users in the United States and around the world, the thief hosted the images on Russian servers with a Russian domain name.

Because Lawrence is a California resident and the defendant is a foreign national, Lawrence's attorneys file suit in the Federal District Court for the Central District of California based on diversity jurisdiction.[33] Among other causes of action,[34] Lawrence's attorneys rely on: (1) California Penal Code section 502(e)(1), which provides civil remedies against any person who knowingly takes, makes use of, or copies data without permission from a computer or network;[35] and (2) a common law claim for invasion of privacy for the public disclosure of private events.[36]

---

33. "California's long-arm statute, Cal. Civ. Proc. Code § 410.10, 'is coextensive with federal due process requirements, [so] the jurisdictional analyses under state law and federal due process are the same'." CollegeSource, Inc. v. AcademyOne, Inc., 653 F.3d 1066, 1073 (9th Cir. 2011) (quoting Schwarzenegger v. Fred Martin Motor Co., 374 F.3d 797, 800–01 (9th Cir. 2004)).

34. For the sake of brevity, this Article focuses on two representative claims and does not investigate related questions about whether Lawrence has satisfied the requirements of subject matter jurisdiction or venue.

35. Section 502 reads in relevant part:

> § 502. Unauthorized access to computers, computer systems and computer data.
>
> (c) Except as provided in subdivision (h), any person who commits any of the following acts is guilty of a public offense:
>
> (2) Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.
>
> (e)(1) In addition to any other civil remedy available, the owner or lessee of the computer, computer system, computer network, computer program, or data who suffers damage or loss by reason of a violation of any of the provisions of subdivision (c) may bring a civil action against the violator for compensatory damages and injunctive relief or other equitable relief. Cal. Pen. Code § 502.

36. The elements of a claim of invasion of privacy based on the public disclosure of private facts are as follows: "(1) public disclosure (2) of a private fact (3) which would be offensive and objectionable to the reasonable person and (4) which is not of legitimate public concern." Catsouras v. Dep't of Cal. Highway Patrol, 181 Cal. App. 4th 856, 868 (2010), as modified on denial of reh'g (Mar. 1, 2010) (quoting Shulman v. Group W Productions, Inc., 18 Cal. 4th 200, 214 (1998)).

Lawrence's attorneys believe that the defendant has not had "such continuous and systematic contacts as to be at home in"[37] California—a threshold requirement to establish general personal jurisdiction—so they decide instead to focus their proof of personal jurisdiction on specific jurisdiction based on defendant's conduct in the forum state.[38] In their pleadings, Lawrence's attorneys maintain that personal jurisdiction is proper based on a number of arguments. First, the defendant targeted the district by accessing the digital information owned by Apple in that district. Second, the defendant directed his efforts at the district by operating a website which hosts her images and which is accessible to residents of that district. Third, the defendant knew that Lawrence resided in California and therefore the distribution of the pictures would cause harm to her in that state.

The defendant maintains that he is not subject to specific jurisdiction in the United States. First, he argues that the data was not stolen from Apple's data centers within the district but from a data center located outside of U.S. jurisdiction.[39] Second, he argues that the website through which he has made the pictures available was set up and is maintained in his home country and is accessible to anyone, anywhere with an Internet connection. Third, he claims that he did not specifically target Jennifer Lawrence with his efforts and that his distribution of the images was not intended to cause harm to her or anyone else but merely to make information available to people everywhere. Therefore, the defendant would argue that he has not targeted residents in the forum state of California nor the victim herself within that state.

---

37. *See* Daimler AG v. Bauman, 134 S. Ct. 746, 754 (2014) (citations omitted); *see also* CollegeSource, Inc. v. AcademyOne, Inc., 653 F.3d 1066, 1074 (9th Cir. 2011) ("AcademyOne's alleged misappropriation of CollegeSource's intellectual property does not support general jurisdiction because the misappropriation was not a 'continuous and systematic' forum activity, but was, rather, a few discrete acts over a relatively short period of time.").

38. "Opinions in the wake of the pathmarking *International Shoe* decision have differentiated between general or all-purpose jurisdiction, and specific or case-linked jurisdiction." Goodyear Dunlop Tires Operations, S.A. v. Brown, 131 S. Ct. 2846, 2851 (2011) (internal citations omitted).

39. *See infra* Section II.a.

II. JURISDICTION FOR INTERNET TORTS: EXISTING CASE LAW

"Absent one of the traditional bases for personal jurisdiction (presence, domicile, or consent), due process requires that the defendant have certain 'minimum contacts' with the forum state, 'such that the maintenance of the suit does not offend traditional notions of fair play and substantial justice.'"[40] There is no Supreme Court precedent governing the application of jurisdiction in Internet torts. In 2014, the Court was asked to visit this issue in *Walden v. Fiore* but declined to rule on the matter.[41] Nevertheless, *Walden* and a patchwork of related case law provide the analytical framework for determining how and where jurisdiction could be properly exerted over the data thief in Lawrence's hypothetical litigation. Part A of this section explores the *Walden* decision in detail, particularly how it re-asserted the primacy of the minimum contacts test as a defendant-friendly tool to obstruct aggressive application of personal jurisdiction.[42] Through its discussion of *Walden*, Part A also analyzes the Court's decision in *Calder v. Jones*, which articulated an alternative "effects test" for personal jurisdiction, but which may have been significantly cabined by the *Walden* decision.[43] Part B considers the role of another seminal personal jurisdiction decision based on Internet usage, *Zippo Manufacturing Co. v. Zippo Dot Com, Inc.*, which considered how the use of a website can create minimum contacts with a forum state.[44] While the unanimous nature of the *Walden* decision suggests a level of obviousness in the legal reasoning,[45] when the decision is weaved together with *Calder* and *Zippo*, the legal fabric fails to cover important Internet torts like the photo theft in our hypothetical.

---

40. Mainstream Media, EC v. Riven, C 08-3623 PJH, 2009 WL 2157641, at *5 (N.D. Cal. July 17, 2009) (quoting Int'l Shoe Co. v. Washington, 326 U.S. 310, 316 (1945)).

41. Walden v. Fiore, 134 S. Ct. 1115, 1125 n.9 (2014).

42. *Id.* at 1121–22.

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

44. *See* Zippo Mfg. Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119, 1124 (W.D. Pa. 1997).

45. William Baude, *Opinion Analysis: The Boundaries of Specific Jurisdiction*, SCOTUSBLOG (Feb. 26, 2014, 2:37 PM), http://www.scotusblog.com/2014/02/opinion-analysis-the-boundaries-of-specific-jurisdiction/.

A. Walden v. Fiore

In 2014, a unanimous Supreme Court ruled that in order to satisfy the minimum contacts test for personal jurisdiction a plaintiff must show that the defendant herself has established connections to the forum state.[46] The Court held that where the relevant conduct occurred outside of the forum state, the fact that a defendant's conduct affected a plaintiff connected to the forum state was insufficient to establish jurisdiction.[47]

1. Facts

In 2006, TSA agents at the San Juan airport searched the carry-on bags of Gina Fiore and her travel companion as they attempted to board a plane to Atlanta.[48] Drug Enforcement Administration ("DEA") agents detained the travelers after discovering $97,000 in cash in the luggage.[49] Fiore informed agents in San Juan that the cash was the winnings and bankroll for a gambling trip to a local casino, that the travelers were professional gamblers, and that they maintained residency in California and Nevada.[50] Fiore and her companion were allowed to board the flight but the San Juan agents contacted their counterparts in Atlanta, who subsequently detained the travelers upon their arrival in Atlanta.[51] In Atlanta, DEA agent Walden seized the cash and informed Fiore that the money "would be returned if they later proved a legitimate source for the cash."[52] The travelers subsequently boarded the last leg of their flight to Nevada.[53]

Following the seizure, agent Walden helped draft an affidavit showing probable cause for the forfeiture of the funds and forwarded the affidavit to the United States Attorney's Office in Georgia.[54] Ultimately, the Department of Justice did not seek forfeiture and returned the funds in

---

46. Walden v. Fiore, 134 S. Ct. 1115, 1122.
47. *Id.* at 1126.
48. *Id.* at 1119–20.
49. *Id.*
50. *Id.*
51. *Id.* at 1119.
52. Walden v. Fiore, 134 S. Ct. 1115, 1119.
53. *Id.*
54. *Id.*

2007.[55] Nevertheless, Fiore and her companion brought a *Bivens* action in federal court in Nevada alleging that they had been injured because: (1) the seizure lacked probable cause; (2) the DEA withheld the money after concluding that it was not drug-related; and (3) because Walden had drafted and forwarded an affidavit purportedly based on false statements.[56]

2. Procedural History

The District Court in Nevada granted Walden's motion to dismiss, reasoning that even if Walden caused harm to plaintiffs in Nevada while knowing that they were living in Nevada, this could not confer jurisdiction on its own.[57] However, the Ninth Circuit reversed, finding that while the seizure in Georgia could not form the basis of personal jurisdiction, the purportedly false affidavit could establish jurisdiction because it was expressly aimed at Nevada and Walden knew that it would affect persons with a significant connection to Nevada.[58]

3. Supreme Court Decision

The Supreme Court granted certiorari in *Walden v. Fiore* to address "the 'minimum contacts' necessary to create specific jurisdiction."[59] The Supreme Court emphasized two particular considerations in determining whether specific personal jurisdiction existed. First, "the relationship must arise out of contacts that the 'defendant *himself*' creates with the forum State."[60] Second, the minimum contacts test is based on the defendant's contact with the forum state itself, not with the persons who reside there.[61]

The Supreme Court held that the facts in *Walden* did not satisfy these standards:

> It is undisputed that no part of petitioner's course of conduct occurred in Nevada. Petitioner approached, questioned, and searched respondents, and seized the cash

55. *Id.*
56. *Id.*
57. Walden v. Fiore, 134 S. Ct. 1115, 1119.
58. *Id.* at 1120.
59. *Id*. at 1121.
60. *Id.* (quoting Burger King Corp. v. Rudzewicz, 471 U. S. 462, 475 (1985)).
61. *Id.* at 1122.

> at issue, in the Atlanta airport. It is alleged that petitioner later helped draft a "false probable cause affidavit" in Georgia and forwarded that affidavit to a United States Attorney's Office in Georgia to support a potential action for forfeiture of the seized funds. Petitioner never traveled to, conducted activities within, contacted anyone in, or sent anything or anyone to Nevada. In short, when viewed through the proper lens—whether the *defendant's* actions connect him to the *forum*—petitioner formed no jurisdictionally relevant contacts with Nevada.[62]

Respondents argued that the case was analogous to *Calder v. Jones*.[63] In *Calder*, the Supreme Court held that personal jurisdiction existed over Florida newspaper writers in California state court for libel.[64] The writers contributed to a national newspaper with a circulation greater than 600,000 in California, where the celebrity who was the subject of the article claimed injury.[65] The writers also contacted sources in the state of California and one of the defendants regularly traveled to California on business.[66] Ultimately, the Supreme Court held that jurisdiction over the Florida defendants was proper in California:

> The allegedly libelous story concerned the California activities of a California resident. It impugned the professionalism of an entertainer whose television career was centered in California. The article was drawn from California sources, and the brunt of the harm, in terms both of respondent's emotional distress and the injury to her professional reputation, was suffered in California. In sum, California is the focal point both of the story and of the harm suffered. Jurisdiction over petitioners is therefore proper in California based on the "effects" of their Florida conduct in California.[67]

However, the Court in *Walden* rejected this comparison.[68] The Court reinforced that "mere injury to a forum resident is

---

62. *Id.* at 1124. (citations omitted).
63. Walden v. Fiore, 134 S. Ct. 1115, 1124; Calder v. Jones, 465 U.S. 783 (1984).
64. *Calder*, 465 U.S. at 785.
65. *Id.*
66. *Id.*
67. *Id.* at 788–89.
68. *Walden*, 134 S. Ct. at 1125 ("This emphasis [on *Calder*] is likewise misplaced.").

not a sufficient connection to the forum."[69] Therefore, the "proper question" is not where the plaintiff experienced injury but instead whether the defendant's conduct connects him to the forum in a meaningful way.[70] The Court concluded that the seizure of goods in Georgia caused an injury that was forum-agnostic: "Respondents would have experienced this same lack of access in California, Mississippi, or wherever else they might have traveled and found themselves wanting more money than they had."[71] In fact, the Court intimated that the *Calder* test may be limited to claims like defamation where intentional harm in the forum state is a component of the cause of action.[72] For this reason, *Walden* may portend a more limited application of the *Calder* doctrine.

At the end of the opinion, the court provided addressed the respondent's concerns about the consequences of this decision on Internet torts:

> Respondents warn that if we decide petitioner lacks minimum contacts in this case, it will bring about unfairness in cases where intentional torts are committed via the Internet or other electronic means . . . we reiterate that the "minimum contacts" inquiry principally protects the liberty of the nonresident defendant, not the interests of the plaintiff. In any event, this case does not present the very different questions whether and how a defendant's virtual "presence" and conduct translate into "contacts" with a particular State. To the contrary, there is no question where the conduct giving rise to this litigation took place . . . [w]e leave questions about virtual contacts for another day.[73]

This reveals two important themes of the *Walden* opinion. First, it reinforces the Court's belief that personal jurisdiction is to be construed in favor of the defendant, not for the benefit of the plaintiff. Second, it shows that, if possible, the Court will look to the location where the conduct took place when determining jurisdiction rather than relying

---

69. *Id.*
70. *Id.*
71. *Id*.
72. *Id.* at 1124 ("The strength of that connection [to the forum] was largely a function of the nature of the libel tort. However scandalous a newspaper article might be, it can lead to a loss of reputation only if communicated to (and read and understood by) third persons.").
73. *Id.* at 1125, n. 9 (citations omitted).

on the location of the injured party. Both of these themes have important implications for data theft cases.

B. Zippo Mfg. Co. v. Zippo Dot Com, Inc.: *Publication to a Website as a Basis of Jurisdiction*

The "*Zippo* test" has been widely adopted by the circuits as a means to determine whether an Internet portal accessible in the forum state can create jurisdiction in the forum state.[74] In *Zippo*, the district court for the Western District of Pennsylvania held that whether a website can establish jurisdiction in a forum depends on the level of contacts that the website creates with the forum state.[75] The court held that "[a]t one end of the spectrum are situations where a defendant clearly does business over the Internet": these business transactions satisfy the requirements of specific jurisdiction.[76] Similarly, "[i]f the defendant enters into contracts with residents of a foreign jurisdiction that involve the knowing and repeated transmission of computer files over the Internet, personal jurisdiction is proper."[77] On the other hand, "where a defendant has simply posted information on an Internet Web site which is accessible to users in foreign jurisdictions," jurisdiction over that defendant is not proper.[78] Stated another way, "a passive Web site that does little more than make information available to those who are interested in it is not grounds for the exercise of personal jurisdiction."[79] This standard has provided jurisdiction in a wide range of cases where defendants only interaction with the forum state was through

---

74. *See* Michael A. Geist, *Toward Greater Certainty for Internet Jurisdiction*, 16 BERKELEY TECH. L.J. 1345, 1367–71 (2001) (collecting and discussing cases adopting *Zippo*); William H. Wynne, *Roads? Where We're Going We Don't Need Roads: Back to the Future and the Ninth Circuit's Use of Traditional Jurisdiction on the Internet Superhighway*, 47 NEW ENG. L. REV. 477 (2012). *See also* Best Van Lines, Inc. v. Walker, 490 F.3d 239, 251 (2d Cir. 2007); Toys "R" Us, Inc. v. Step Two, S.A., 318 F.3d 446, 452 (3d Cir. 2003); ALS Scan, Inc. v. Digital Serv. Consultants, Inc., 293 F.3d 707, 713 (4th Cir. 2002) (collectively adopting the *Zippo* standard).

75. *See* Zippo Mfg. Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119, 1123–25 (W.D. Pa. 1997).

76. *Id.* at 1124.

77. *Id.*

78. *Id.*

79. *Id.*

a website.[80]

III. APPLICATIONS AND AMBIGUITIES POST-*WALDEN*

Having established the present contours of specific personal jurisdiction for Internet torts, this section returns to the specific circumstances of the hypothetical. When a defendant is domiciled internationally, can he be subject to personal jurisdiction for the theft and distribution of a U.S. citizen's data? There are three potential sources of personal jurisdiction in the hypothetical case. First, as discussed in Part A, the availability in California of images of Jennifer Lawrence on a passive Internet site may establish jurisdiction in California. Second, as discussed in Part B, the underlying theft of the photo data from a foreign server creates jurisdiction in California because the plaintiff is a California resident. Third, as discussed in Part C, the theft and distribution of the images creates jurisdiction because the effect of the actions were knowingly targeted at California. The first question implicates the *Zippo* reasoning, which nevertheless must be viewed in light of the *Walden* decision. The second case also implicates *Walden* because there are strong comparisons to be made between the seizure in that case and the theft of Internet data which routinely travels between different repositories. Finally, the third basis is rooted in the *Calder* "effects" test. However, that test may no longer carry the same force following the *Walden* decision. Each of these bases will be considered in turn.

A. Internet Availability as Basis for Jurisdiction

Zippo's reliance on interactivity likely renders the rule unfit to litigate the publication of Jennifer Lawrence's photos. The *Zippo* sliding scale is based on the interactivity of the website.[81] But hackers initially posted the celebrity photos on passive image sites including 4chan and Reddit.[82] These sites

---

80. John J. Schulze, Jr., *Caveat E-Emptor: Solutions to the Jurisdictional Problem of Internet Injury*, 29 AM. J. TRIAL ADVOC. 615, 619–24 (2006) (listing applications of the *Zippo* test based on website contacts).

81. *See infra* Section III.B.

82. Harry Bradford, *Everything We Know About The Unnamed Celebrity Photo Hacker*, HUFFINGTON POST (Sept. 2, 2014), http://www.huffingtonpost.com/2014/09/02/celebrity-photo-hacker_n_5752642.html (noting that the photos are believed to have been first uploaded to the Internet via relatively obscure

are intentionally austere message boards with limited interactivity besides the ability to post content or to view comments or images posted by others.[83] Neither website is interactive in the sense contemplated by the court in *Zippo* because the sites do not provide any opportunity for viewers in California to purchase or engage directly with a product on the website.[84] More apropos than engaging with products, the *Zippo* standard excludes online advertisements as a basis for jurisdiction because of its passivity.[85] The hosting of the images in this case is even less interactive than many modern advertisements.[86]

The Supreme Court of California considered a close example to the our Lawrence hypothetical in *Pavlovich v. Superior Court*.[87] In that case, a website operator residing in Indiana posted a computer program which could decrypt DVDs produced by a California corporation.[88] After determining that Pavlovich did not himself have any connection to California,[89] the court employed the *Zippo* scale and found that the passive hosting website did not create jurisdiction in California.[90] Just as the code at issue in *Pavlovich* could be used to tortiously breach the security of the DVDs, those who download Jennifer Lawrence's pictures can use them to commit tortious conduct by causing her emotional distress and further invading her privacy. Nevertheless, *Pavlovich* seems to support the notion that even when content could be used for nefarious purposes, the

---

forums like 4Chan and AnonIB, but that they were shared more widely after the creation of a Reddit community).

83. *See, e.g.*, Revell v. Lidov, 317 F.3d 467, 472 (5th Cir. 2002) (affirming a district court ruling that a "*Zippo*-passive" website could not create specific personal jurisdiction).

84. *See, e.g.*, Wynne, *supra* note 74, at 491 (finding that the *Zippo* standard "encompasses direct commercial activity or the selling of a physical product to an end-user, but notably excludes Internet advertising.").

85. *See* Wynne, *supra* note 74. *But see* Mavrix Photo, Inc. v. Brand Techs., Inc., 647 F.3d 1218, 1227–31 (9th Cir. 2011) (rejecting the interactivity standard in favor of a focus on purposeful availment).

86. Hairong Li & John D. Leckenby, *Internet Advertising Formats and Effectiveness* (Oct. 2004), *available at* http://champtec.googlepages.com/ad_format_print.pdf (finding an increase in advertising based on rich media and keyword searches and a decline in passive banner and sponsorship advertising).

87. Pavlovich v. Superior Court, 29 Cal. 4th 262 (2002).

88. *Id.*

89. *Id.* at 274.

90. *Id.*

person hosting it is not subject to jurisdiction in the injured party's state just because they made the information available.

Even if a broad reading of interactivity might capture the conduct in our Lawrence hypothetical, the effect would swallow the rule and lead to unsatisfactory jurisdictional outcomes. As the Ninth Circuit noted in *Cybersell, Inc. v. Cybersell, Inc*., assertion of jurisdiction based on mere posting or hosting of content would establish precedent whereby "every complaint arising . . . on the Internet would automatically result in personal jurisdiction wherever the plaintiff's principal place of business is located."[91] Similarly, the Tenth Circuit has emphasized that the analysis should focus on the intentional direction of activities at the forum state rather than the mere accessibility of those activities in that state.[92]

The passive hosting as a basis for jurisdiction rejected in *Zippo* has similarly failed to catch fire in the European Union. While EU regulations "potentially subject all cloud services used by an EU resident to the EU's data protection law"[93] the European Court of Justice held in the case of *In re Lindqvist*, that the rule should not be read broadly to impose jurisdiction in every member state over a website that contained some private information.[94] The Court noted that if posting information on a website constituted a transfer of data to all countries where that webpage could be accessed then EU Member States would actually be discouraged from permitting any posting because information may be transferred to a country that will not adequately protect the posted data according to EU law.[95] The European Court's reasoning comports with the Ninth Circuit's reasoning in *Cybersell* finding that it would be absurd and incongruous to subject a website owner to jurisdiction in any location where the website was accessed.[96]

---

91. Cybersell, Inc. v. Cybersell, Inc., 130 F.3d 414, 420 (9th Cir. 1997).

92. *See* Shrader v. Biddinger, 633 F. 3d 1235, 1240 (10th Cir. 2011).

93. *See* Paul Schwartz, *Information Privacy in the Cloud*, 161 U. PA. L. REV. 1623, 1650 (2013).

94. In re Lindqvist, Case C-101/01, 2003 E.C.R. I-13020, *available at* http://curia.europa.eu/juris/showPdf.jsf?text=&docid=48382&pageIndex=0&doclang=EN.

95. *Id.* at I-13020.

96. *See* Schwartz, *supra* note 93, at 1650–51.

Whether or not an expansive *Zippo*-like test could lead to desirable legal outcomes, a viewpoint rejected by American and European courts, such an approach seems foreclosed by the Court's *Walden* decision, which required defendant-specific contacts and rejected incidental contacts with plaintiff's forum.[97]

B. Data Seizure as Basis for Jurisdiction

The seizure of the data itself presents a second avenue for obtaining jurisdiction over a defendant. One could argue that because the data was stored concomitant on Lawrence's phone and at Apple's data centers, that the theft of the data occurred on that phone and thus jurisdiction is found wherever that phone was at the time of the hack. However, "cloud computing is necessarily (and perhaps counter-intuitively) 'grounded' by aggregated servers on land or in water."[98] Therefore, when an individual like the hypothetical defendant breaks into a server, they are perpetrating an act at a physical location where the data is stored even if the fruit of those efforts is information otherwise contained on a person's private device. A few courts have grappled with the issue of personal jurisdiction where a person takes information from a remote data server.[99] In these cases, courts have generally held that minimum contacts exist in the state where the data was stolen.[100] While this viewpoint comports with both a *Calder* analysis and a traditional minimum contacts analysis, no court has faced this question with respect to non-U.S. data storage. Nevertheless, a few decisions have considered the legal implications of theft from

---

97. Walden v. Fiore, 134 S. Ct. 1115, 1125 (2014).

98. *See* Andrews & Newman, *supra* note 25, at 360.

99. *See, e.g.*, Rhapsody Solutions, LLC v. Cryogenic Vessel Alternatives, Inc., 2013 WL 820589, at *5 (S.D. Tex. Mar. 5, 2013) (finding jurisdiction in forum state based on non-resident defendant's access of a company's forum state servers); *see also* Watch Sys. LLC v. Sys. Design Solutions, Inc., Civ. A. No. 09–5821, 2009 WL 5217085, at *6 (E.D.La. Dec.31, 2009); Abatix Corp. v. Capra, No. Civ. A. 2:07–CV–541, 2008 WL 4427285, *4 (E.D.Tex. Sept.24, 2008); Flowserve Corp. v. Midwest Pipe Repair, L.L.C., No. 3:05-CV-1357-N, 2006 WL 265521, at *3 (N.D. Tex. Feb. 3, 2006); Info. Techs. Int'l, Inc. v. ITI of N. Fla., Inc., No. 01 C 4668, 2001 WL 1516750, at *7 (N.D.Ill. Nov.28, 2001); Peridyne Tech. Solutions, L.L.C. v. Matheson Fast Freight, Inc., 117 F. Supp. 2d 1366, 1369 (N.D. Ga. 2000).

100. Joel R. Reidenberg, *Technology and Internet Jurisdiction*, 153 U. PA. L. REV. 1951, 1955–56 (2005).

a server in an unknown location, a realistic problem considering the decentralized and cross-border nature of cloud storage and a challenge in light of the *Walden* Court's distaste for random or fortuitous jurisdictional hooks.[101]

In *MacDermid, Inc. v. Deiter*, the Second Circuit held that a Canadian employee of a Connecticut company was subject to specific jurisdiction in Connecticut after stealing company documents from a server physically located in Connecticut.[102] The court analyzed the data theft under the *Calder* "intentionally directed efforts" rather than treating the theft of data like the car accident in *Worldwide Volkswagen*. The Second Circuit found that while "[m]ost Internet users, perhaps, have no idea of the location of the servers through which they send their emails," this particular defendant "knew that the email servers she used and the confidential files she misappropriated were both located in Connecticut."[103] A district court in Kansas in *AgJunction LLC v. Agragrian Inc.* adopted the same logic in denying jurisdiction where a defendant did not know that the data he was stealing was specifically stored on servers in the forum state as opposed to other states in which the plaintiff had data centers.[104] The court in *AgJunction* went further, applying the holding in *Walden* and declaring, "the fact that the files were stored in Kansas is the type of 'random, fortuitous, or attenuated' contact that does not satisfy due process."[105]

Even within the same courtroom, defendant's knowledge of server location has prompted divergent dispositions. In two near identical cases, *Microsoft Corp. v. Mountain W. Computers, Inc.* and *Microsoft Corp. v. Communications & Data Systems Consultants, Inc.* in the Western District of Washington, contrary motion to dismiss resolutions turned on whether the defendant's knew they were targeting servers in Washington when committing alleged tortious acts.[106] In the

---

101. *See Walden*, 571 U.S. at 8.

102. MacDermid v. Deiter, 702 F.3d 725, 727.

103. *Id.* at 730.

104. AgJunction LLC v. Agrian Inc., 14-CV-2069-DDC-KGS, 2014 WL 3361728 (D. Kan. July 9, 2014).

105. *Id.* at *5.

106. Microsoft Corp. v. Mountain W. Computers, Inc., No. C14-1772RSM, 2015 WL 4479490 (W.D. Wash. July 22, 2015); Microsoft Corp. v. Commc'ns & Data Sys. Consultants, Inc., No. C15-0497 RSM, 2015 WL 5102587 (W.D. Wash.

first case, *Mountain W.*, the court found that it had specific jurisdiction over copyright infringement claims against a small IT company in Utah, because "Defendants affirmatively contacted Microsoft through internet contact with its servers" and "they knew Microsoft is located in Washington."[107] The court reached this conclusion "regardless of whether Defendants knew where Plaintiff's servers were located."[108] Two months later, the same court dismissed for lack of jurisdiction a claim against a small computer reseller in Indiana because "Plaintiffs have produced no evidence that the servers accessed by the instant Defendant are located in Washington."[109] As this Article has advised, and other courts, as in *AgJunction* have recognized, courts must take care to not conflate the location of the company itself with the location of its data servers. Failing to take heed, the *Mountain W.* court disregarded the prevalence of off-site (and out of state) data storage while smoothing over the challenge this disconnect poses for establishing specific jurisdiction.

Taken together, these decisions illustrate the significant challenges Lawrence would face in asserting jurisdiction over a foreign defendant based on the location of the data seizure. First, the defendant could argue that even if the data was stored on a server or on Lawrence's phone in California, that fact is merely fortuitous and cannot form the basis of jurisdiction because defendant, like those in *AgJunction* and *Communications and Data Systems, Inc.*, did not know the location of the targeted data.[110] Even if, as in *MacDermaid* and *Mountain W.*, the court found that the defendant knew or should have known of the location of the servers, he may still be able to argue that jurisdiction is *only* proper where the server is located, a conclusion supported by pre and post-*Walden* case law.[111] If the server were in another U.S. state,

---

Aug. 28, 2015); The court in *Mountain W.* also considered the defendant's purchase of Microsoft software from a third party vendor based in Washington to establish specific jurisdiction. *See Mountain W.*, 2015 WL 4479490 at *7. While such a fact could have been dispositive on its own, the court presents the server access as an independent basis for establishing jurisdiction. *Id.*

107. *Id.* at *7–8 .

108. *Id.*

109. *Commc'ns & Data Sys. Consultants, Inc.*, WL 5102587 at *7.

110. *See id.*; *see also AgJunction*, 2014 WL 3361728 .

111. *See, e.g.,* CompuServe, Inc. v. Patterson, 89 F.3d 1257, 1264 (6th Cir.1996) (pre-*Walden*); *AgJunction*, 2014 WL 3361728 (post-*Walden*).

jurisdiction and venue would likely be proper in that state (even if local law might be less favorable). But if the server is housed abroad, then jurisdiction would not be proper in any U.S. state. Furthermore, the notion that Lawrence should be drawn out of her favorable jurisdiction to litigate in North Carolina or some other state where Apple stored her data seems no more equitable than hailing the defendant into a forum in which he has no contacts.

C. Calder "Effects" Test as Basis for Jurisdiction

Walden may have significantly cabined the viability of the *Calder* doctrine and consequently reduced its usefulness in our hypothetical case. The Supreme Court suggested this very possibility when they ruled that *Calder* may be limited to the exceptional nature of the libel tort action, which requires a person to affect individuals in the jurisdiction.[112] Other courts have speculated that the *Walden* decision will limit the effectiveness of *Calder*.[113] If *Calder* is limited, its limitation is to tort actions that by their very nature require contacts with the forum state.[114] Lawrence's best argument may be that the release of private facts tort is analogous to libel in that it requires a recipient in order to have effect. The significance of the photo hack was a function of the many people (including those in California) who viewed the images. Because the hacker knew or should have known that the effect would be most pronounced in California where Lawrence lives, the *Calder* effects test would render this an appropriate basis for personal jurisdiction.

Nevertheless, there are marked differences between the facts in *Calder* and the circumstances in this hypothetical. In *Calder,* the court made note of the fact that the publication had its most extensive circulation in the state of California.[115] Therefore, the writers for the paper were on notice that the

112. *See* Walden v. Fiore, 134 S. Ct. 1115, 1123–24 (2014).

113. *See* Streamline Bus. Servs., LLC v. Vidible, Inc., No. 14-1433, 2014 WL 4209550, at *12 (E.D. Pa. Aug. 26, 2014) ("It appears that this ruling [*Walden*] could limit the *Calder* effects test."); *see also Mountain W.*, 2015 WL 4479490 at *5-6 (discussing competing rulings as to whether the *Walden* decision overruled the "purposeful direction prong" of the *Calder* test in the Ninth Circuit).

114. *See Walden*, 134 S.Ct. at 1123–24.

115. Calder v. Jones, 465 U.S. 783, 784 (1984).

paper would have a significant effect where it was read.[116] On the other hand, the passive website created by the defendant is available to anyone, anywhere, so long as there is an Internet connection. While it may be the case that there are more people viewing these images in California, and it may also be the case that the effects would be felt most strongly in California because Lawrence lives there, it is not the case that the defendant targeted California in any meaningful way compared to any other jurisdiction.[117] Rather, the language of *Walden* is illustrative: jurisdiction cannot be based merely on the fortuitous residence of the plaintiff.[118] If this basis for jurisdiction were sustained, then Lawrence could have alternatively brought suit in any other state in which she happened to reside and where individuals had viewed the images.[119] This expansive interpretation of jurisdiction is contrary to the reasoning in *Walden*.

Because no exception was made in *Walden* for Internet torts, and as the preceding considerations show, there is a real concern of at least inconsistent applicability of personal jurisdiction in cases like the hypothetical and at worst a finding that jurisdiction is not proper anywhere in the United States, leaving Lawrence without legal remedy. None of the available frameworks—the traditional minimum contacts analysis, the *Calder* effects test, or the *Zippo* standard—are a proper fit for an age of cloud computing. The reasoning in *Walden*, applied to the foregoing standards, strengthens the belief that jurisdiction will not be proper over the hypothetical defendant in this comment. At least one scholarly article anticipated this problem before the *Walden* decision.[120] The remainder of this Article assumes that the lack of a definite remedy is an undesirable outcome both because it may lead to inconsistencies and because it may lead to legitimate tort claims devoid of remedy.[121]

---

116. *Id.* at 789.

117. This is assuming that the website does not employ other interactivity that would make it especially targeted towards California. *See supra* Section III.B (discussing the application of the *Zippo* standard).

118. *Walden*, 134 S.Ct. at 1125.

119. *Id.* ("Respondents would have experienced this same lack of access in California, Mississippi, or wherever else they might have traveled and found themselves wanting more money than they had.").

120. *See generally* Andrews & Newman, *supra* note 25.

121. Marbury v. Madison, 5 U.S. 137, 147 (1803) ("It is a settled and

IV. SOLUTIONS

The inability to obtain civil remedies for theft of data is an important policy issue worthy of scrutiny for a number of reasons. First, the full range of the U.S. judicial system, including civil remedies, should discourage overt attempts to steal the data of U.S. citizens. Second, victims of Internet attacks are worthy of particular sympathy because of our dependence on Internet services and the omnipresent threat posed by nefarious actors across the world. Therefore, jurisdictional nets should be stretched to reach Internet tortfeasors. Finally, gaps in judicial remedies are unfair to victims per se and extended jurisdiction would resolve these inequities. Whatever the reason, there are a number of ways that the ambiguities or inadequate jurisdiction can be reduced or eliminated.

A. Jurisdictional Reforms

In 2013, two authors, Damon Andrews and John Newman, engaged directly with the application of personal jurisdiction to torts occurring in the cloud-computing sphere.[122] Though there are some flaws to their proposals, they are useful starting points for considering solutions to the jurisdictional deficiencies described above.

1. Caveat Maleficus *Standard*

Under Andrews and Newman's *caveat maleficus* approach, the location of Internet harm like data theft is based on the victim's location.[123] They root the reform in the tort notion of taking your victim "as they are" transformed to "taking the victim where they find him."[124] In our hypothetical example, this would mean that the defendant's theft of data from a foreign data server creates jurisdiction in California because the injury was perpetrated against a person in California.[125] The author's justify this per se

---

invariable principle, that every right, when withheld, must have a remedy, and every injury its proper redress.").

122. *See* Andrews & Newman, *supra* note 25, at 313–14.

123. *See* Andrews & Newman, *supra* note 25, at 362.

124. *See* Andrews & Newman, *supra* note 25, at 362, 364.

125. In the original hypothetical it was suggested that Lawrence returned home to California after uploading the photos. The *caveat maleficus* approach appears to be unavailing if the photos were stolen while Lawrence was still

jurisdictional hook because "cloud torts that involve the hacking of remote servers to obtain information are complex and sophisticated."[126] While this assertion is dubious in an age of cheap, accessible, and user-friendly data theft software,[127] there are even more significant legal challenges to this framework.

The foremost critique of this per se jurisdictional hook is that there is no basis for it in case law. As the court emphasized in *Walden* when it discussed Internet torts, "the "minimum contacts" inquiry principally protects the liberty of the nonresident defendant, not the interests of the plaintiff."[128] A per se jurisdictional hook would be exceedingly plaintiff friendly. In addition, such a broadly sweeping provision would allow for jurisdiction against the defendant based only on the plaintiff's connection to the forum state—an outcome entirely at odds with the Walden decision's rejection of fortuitous connections as a basis for jurisdiction.

2. The Cloud as a Jurisdiction

Andrews and Newman alternatively propose that the cloud could be established as its own area of jurisdiction with its own court.[129] This new court would be reserved for "torts and crimes that occur in the cloud."[130] The authors point to the existence of specific jurisdiction courts like the Federal Appeals Court, which only covers patent-infringement suits as a model.[131] This approach would remedy *Walden*'s rejection of plaintiff-based jurisdiction.[132] Rather, the jurisdiction for the dispute would be based on the type of conduct, giving

---

visiting Europe to film her new movie since the injury would then have occurred in Europe, despite the arbitrariness and inequity of this outcome. *See* Andrews & Newman, *supra* note 25, at 363 n. 296 (showing the problem of *caveat maleficus* if the person is traveling when accident occurs).

126. *See* Andrews & Newman, *supra* note 25, at 363.

127. Christina Warren, *How I Hacked My Own iCloud Account, for Just $200*, MASHABLE (Sept. 4, 2014), http://mashable.com/2014/09/04/i-hacked-my-own-icloud-account/.

128. Walden v. Fiore, 134 S. Ct. 1115, 1123.

129. *See* Andrews & Newman, *supra* note 25, at 364–65. Andrews and Newman drew their inspiration for a court of cloud jurisdiction from similar arguments in David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996).

130. *See* Andrews & Newman, *supra* note 25, at 364.

131. *See* Andrews & Newman, *supra* note 25, at 365.

132. *See Walden*, 134 S.Ct. at 1124.

sufficient notice to defendant that his activities would impose jurisdiction in the cloud court.[133]

However, it would be difficult to define "torts and crimes that occur in the cloud" in such a way that the court of cloud jurisdiction did not swallow the affairs of all other competent courts. Would such a standard capture all Internet activity that travels through an Internet company's data servers? In addition, would such a court necessarily create jurisdiction over actions occurring in foreign countries? The geographical indefiniteness of the cloud means that it extends not only over domestic jurisdictions but also over foreign locales. Recent Supreme Court precedent has strongly disfavored the extraterritorial application of U.S. law.[134] However, if jurisdiction were artificially constrained to not extend extraterritorially, then the hypothetical defendant in this case may escape jurisdiction and the cloud court will not have improved the outcome. If, on the other hand, the court does extend its reach to foreign activities, the cloud court risks becoming a haven for the sort of F-cubed[135] litigation—cases between foreign plaintiffs and defendants concerning events in foreign countries—that the Supreme Court has tried to discourage.[136]

3. Reform of the Stored Communications Act

Finally, Andrews and Newman propose reforms of the Stored Communications Act ("SCA") with updates for the modern digital age.[137] The law was originally passed in 1986[138] and other critics have challenged the law for failing to keep pace with changes in the digital landscape.[139] Andrews

---

133. *See* Andrews & Newman, *supra* note 25, at 365.

134. Morrison v. National Australia Bank Ltd., 561 U.S. 247, 255 (2010) ("[w]hen a statute gives no clear indication of an extraterritorial application, it has none").

135. Linda S. Mullenix, *Personal Jurisdiction Stops Here: Cabining the Extraterritorial Reach of American Courts*, 45 U. TOL. L. REV. 705 (2014) ("Basically, an F-cubed case involves a lawsuit brought in an American court by foreign plaintiffs suing foreign defendants, based on events that took place in some foreign country.").

136. *See*, *e.g.*, Kiobel v. Royal Dutch Petroleum Co., 133 S. Ct. 1659, 1669 (2013) (rejecting the use of the Alien Tort Statute for actions occurring outside of the territory of the United States).

137. *See* Andrews & Newman, *supra* note 25, at 366.

138. 18 U.S.C. §§ 2701–11 (2012).

139. Illana R. Kattan, *Cloudy Privacy Protections: Why the Stored*

and Newman argue that the law should be updated.[140] However, they provide no specific guidance on how it might be reformed.[141]

Despite the incompleteness of their argument and its dependence on legislative reform in an era of significant government recalcitrance, at least one judge has attempted to expand the scope of the SCA to reach foreign data centers.[142] In *In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.*, Magistrate Judge James C. Francis held that the government was permitted to execute a search pursuant to the SCA to obtain information held by Microsoft in a data center in Ireland.[143] Ordinarily, such orders would violate the presumption against extraterritorial application.[144] Absent authority pursuant to the SCA, the government would be required to obtain the fruits of the search pursuant to a Mutual Legal Assistance Treaty and no remedy would be possible in the absence of a treaty.[145] Francis rebutted this presumption by noting, "the nationality principle . . . supports the legal requirement that an entity subject to jurisdiction in the United States, like Microsoft, may be required to obtain evidence from abroad in connection with a criminal investigation."[146]

Though the *Microsoft* decision occurred in the context of warrants pursuant to the SCA for criminal actions, the reasoning could be reasonably extended to the civil context. Rather than determine jurisdiction based on the location of the data centers, the court could base jurisdiction on the location of the organization the defendant hacked. In our hypothetical case, this would permit jurisdiction in California because it is where Apple is located. Thus, a defendant hacking into Apple's servers could reasonably anticipate being hailed into court where Apple does its business even if

---

Communications Act Fails to Protect the Privacy of Communications Stored in the Cloud, 13 VAND. J. ENT. & TECH. L. 617, 645 (2011).

140. *See* Andrews & Newman, *supra* note 25, at 366.

141. *See* Andrews & Newman, *supra* note 26, at 366–67.

142. In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 15 F. Supp. 3d 466, 477 (S.D.N.Y. 2014).

143. *Id.*

144. *Id.*

145. *Id.* at 474–75.

146. *Id.* at 476.

it hosts its data servers outside of California.

Two problems remain. First, Microsoft and a number of other cloud storage companies and advocates have vigorously challenged Judge Francis's interpretation of the SCA.[147] The Second Circuit conducted oral arguments in the case in September 2015.[148] Even Congress has weighed in, proposing the Law Enforcement Access to Data Stored Abroad ("LEADS") Act,[149] which would only permit extraterritorial data seizures of information belonging to a U.S. citizen or corporation (and finding that the corporations do not own for these purposes the data on their servers). Even then, only if the seizure would not be in violation of the foreign country's laws.[150] Second, companies are increasingly outsourcing their storage to third party data centers.[151] As a consequence, it may not always be clear to a hacker-defendant that his hack targeted Apple, or any other particular company, when he hacked the servers of a third party host. Alternatively, the defendant may argue that he knowingly intended to hack the servers of the third party but not to hack Apple itself. Such an argument might limit jurisdiction to where the third party does business as opposed to all of the places where Apple does business.

---

147. *See In re Warrant for Microsoft Email Stored in Dublin, Ireland,* ELECTRONIC FRONTIER FOUNDATION, *available at* https://www.eff.org/cases/re-warrant-microsoft-email-stored-dublin-ireland (database containing amicus briefs filed by the Electronic Frontier Foundation, AT&T, and Verizon, in support of Microsoft); *see also* Larry Seltzer & Zack Whittaker, *Microsoft Refuses to Comply After Judge Revives Overseas Data Search Warrant*, ZDNET (Aug. 31, 2014), http://www.zdnet.com/judge-revives-microsoft-irish-data-search-warrant-7000033144/.

148. *Argument Calendar, Courtroom 1703,* United States Court of Appeals for the Second Circuit, http://ww2.ca2.uscourts.gov/calendar/index.php?eID=735 (last visited Oct. 25, 2015).

149. The Law Enforcement Access to Data Stored Abroad Act, S. 2871, 113th Cong. (as introduced in Senate, Sept. 18, 2014).

150. John Ribiero, *Senate Bill Would Limit Access to Emails Stored Abroad*, COMPUTERWORLD (Sept. 18, 2014), http://www.computerworld.com/article/2686099/senate-bill-would-limit-access-to-emails-stored-abroad.html.

151. Archana Venkatraman, *Enterprises Spend More on Third-Party Datacentres Than In-house Ones: Uptime Survey*, COMPUTER WEEKLY (Aug. 9, 2013), http://www.computerweekly.com/news/2240203364/Enterprises-spend-more-on-third-party-datacentres-than-in-house-ones-Uptime-survey.

B. Other Means of Establishing Jurisdiction

1. International Collaboration

International collaboration on a comprehensive jurisdictional framework may be the most ideal solution to our hypothetical. It could not only resolve questions of jurisdiction but also remedy related challenges of service of process and judgment collection against a foreign defendant. While those other facets of civil procedure are beyond the scope of this Article, it is important to acknowledge that even if Lawrence could establish personal jurisdiction over the defendant, it would be difficult to hail the defendant into court or exercise a default judgment if the defendant declined to appear (and potentially subject himself to jurisdiction) without a comprehensive international framework.

However, there are significant barriers to the adoption of a uniform international standard for data privacy. Countries operate in a patchwork of national rules governing data protection.[152] While the Organization for Economic Cooperation and Development agreed on a framework for cooperation in the enforcement of privacy laws in 2007,[153] countries continue to develop competing data privacy frameworks that are fundamentally at odds.[154] Consequently, international collaboration on data privacy rules represents more of an aspiration than a concrete solution to the increasing challenges of international Internet torts.

2. Fact-Specific Arguments

All of the previously suggested solutions to the personal jurisdiction gap in Internet torts have depended on

---

152. John J. Schulze, Jr., *Caveat E-Emptor: Solutions to the Jurisdictional Problem of Internet Injury*, 29 AM. J. TRIAL ADVOC. 615, 627–32 (2006) (reviewing the data privacy rules for a variety of different countries and how they relate to U.S. data privacy law).

153. *OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy*, OECD: INTERNET ECONOMY, http://www.oecd.org/internet/ieconomy/oecdrecommendationoncross-borderco-operationintheenforcementoflawsprotectingprivacy.htm.

154. Donald C. Dowling, Jr., *European Union data protection law and US-based multinational banks: a compliance primer*, WHITE & CASE CLIENT ALERT, http://www.lexology.com/library/detail.aspx?g=056dbb01-0a69-46b6-85f1-ac7b8868b18f (last visited Oct. 25, 2015) ("The European approach in effect prioritizes privacy over free speech, while the U.S. in effect does the reverse.").

interventions in the law-making process, greater cooperation between nations, or debatable judicial interpretation. Therefore, the most favorable option may be a careful construction of facts that allow the *Calder* or *Zippo* tests to serve as a basis of jurisdiction.

The *Calder* test may be applicable if Lawrence can show two things: (1) that the torts she alleges are, like libel, dependent on the experience of harm in the forum state;[155] and (2) that the defendant intended or should have known that the effects of his tort would be felt in the forum state.[156] Therefore, a court could find that the privacy torts in our hypothetical fall within a special class, like the claims in *Calder*, which justify a unique jurisdictional treatment.

The *Zippo* test may be used to reinforce the assertion that the defendant knew that he was targeting California or as a standalone basis for establishing jurisdiction.[157] In this case, the key factual considerations will be the extent to which the author monetized the product through interaction with California residents or specifically interacted with residents of that state.[158] If, for instance, the defendant uses the release of the images to extort Lawrence in exchange for removal of the images, then a court could find that the defendant had directed the claims at the forum state.[159] However, the targeting of the forum state must be evident in

---

155. *See* Calder v. Jones, 465 U.S. 783, 785 (1984); *see also* Myers v. Bennett Law Offices, 238 F.3d 1068 (9th Cir. 2001) (finding in a FCRA claim that mental distress is felt where plaintiff resides thereby establishing jurisdiction over defendant who induced the mental distress).

156. *See Calder*, 465 U.S. 783. *But see* Xcentric Ventures, LLC v. Bird, 683 F. Supp. 2d 1068 (D. Ariz. 2010) (finding no personal jurisdiction over defendants because knowledge of plaintiff's place of residence, without more, insufficient to satisfy express-aiming prong of *Calder* effects test).

157. In fact courts grapple with the difficult interplay between these two tests when it comes to intentional torts. *See, e.g.*, Revell v. Lidov, 317 F.3d 467, 472 n.30 (5th Cir. 2002) ("We need not decide today whether or not a '*Zippo*-passive' site could still give rise to personal jurisdiction under *Calder*, and reserve this difficult question for another time.").

158. *See* Zippo Mfg. Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119, 1126–27 (W.D. Pa. 1997) ("If Dot Com had not wanted to be amenable to jurisdiction in Pennsylvania, the solution would have been simple—it could have chosen not to sell its services to Pennsylvania residents.").

159. *See, e.g.*, Panavision Int'l v. Toeppen, 141 F.3d 1316, 1318–19 (9th Cir. 1998) (finding that a defendant targeted plaintiffs by squatting on a website using the plaintiff's name and then extorting the plaintiff in exchange for relinquishing the site).

addition to the online activity.[160] Lawrence could additionally argue that the thief established contacts with California by posting images on the Internet knowing that the person most affected (Lawrence) resided in the forum,[161] or that persons in California were particularly likely to make use of the images on the website. In *Pavlovich*, the California Supreme Court left the latter legal argument open when it relied in part on the fact that "there is no evidence that any California resident ever visited, much less downloaded the DeCSS source code from, the LiVid Web site."[162] If Lawrence could show that users in California most often downloaded the images of her, then she may be able to claim that the site was interactive vis-à-vis the forum state. Because one purpose of a passive image-hosting site is to encourage the distribution and downloading of those images, the "interactivity" would be the very encouragement for California residents to download the images for themselves.

CONCLUSION

Considering the prompt legal action by Jennifer Lawrence and other celebrities to limit harms suffered by the release of their private photographs, it is not unreasonable to believe that suits for damages will be forthcoming. When those suits come, the celebrities will face a difficult challenge establishing personal jurisdiction over the defendant(s), especially if the defendants are foreign citizens. Increased reliance on cloud-based Internet services has resulted in the storage of Internet data in locales around the world. In addition, Internet data theft can be effortlessly perpetrated without regard for traditional jurisdictional borders. In fact, the entire celebrity photo hack could have occurred without any contact with the U.S.

The challenges faced by victims of Internet torts are

---

160. Dinar Corp. Inc. v. Sterling Currency Grp., LLC, 2:13-CV-02106-APG, 2014 WL 4072023 (D. Nev. Aug. 15, 2014) ("[T]he cases finding 'something more' [connecting defendant's actions to the forum state] focus on actions targeted at the forum taken in addition to the online activity.").

161. *See, e.g.*, Brayton Purcell, L.L.P. v. Recordon & Recordon, 606 F.3d 1124, 1129 (9th Cir. 2010) (finding that jurisdiction was proper where the advertiser knew that they were infringing the work of a resident of the forum state); Panavision Int'l, L.P. v. Toeppen, 141 F.3d 1316, 1320–22 (9th Cir. 1998).

162. Pavlovich v. Superior Court, 29 Cal. 4th 262, 276 (2002).

exacerbated by the lack of clear judicial guidance. In *Walden v. Fiore* respondents advised the Supreme Court that their decision could have far reaching implications for jurisdiction in Internet torts. The Court's disregard for this concern leaves a figurative cloud of uncertainty hanging over personal jurisdiction in the digital cloud, especially for precipitating Internet tort cases like those posed in our hypothetical. Furthermore, the prior court tests established in *Calder* and *Zippo* are, following *Walden*, at best fraught with ambiguity, and at worst support a finding of no jurisdiction. Therefore, foreign citizens committing acts that affect the United States may leave victims of their crimes to depend on changes to national or international legal norms or particularly beneficial facts in order to avoid the pressing problems of obtaining relief from Internet torts.