Cloudy Jurisdiction: Foggy Skies in Traditional Jurisdiction Create Unclear Legal Standards for Cloud Computing and Technology

"We are on a shift that is as momentous and as fundamental as the shift to the electric grid[.] It's happening a lot faster than any of us thought."[1]

I. INTRODUCTION

By 2020, the cloud computing industry could be worth over $270 billion.[2] In 2012, this industry was worth only $100 billion.[3] Industry experts predict that cloud computing will make up roughly eighty to ninety percent of all data storage in the next five to ten years.[4] In October 2015, Dell purchased Egan Marino Corporation (EMC) "for $67 billion, making it the largest tech acquisition ever."[5] With such rapid growth, the boundaries that separate us will diminish, and the interconnectivity between us will be endless.[6]

Cloud computing is the act of "storing and accessing data and programs over the Internet instead of your computer's hard drive."[7] As cloud computing continues to grow, so will its technological capabilities and the way users interact with the technology.[8] Presently, cloud computing relies on "sharing

1. Quentin Hardy, *Active in Cloud, Amazon Reshapes Computing*, N.Y. TIMES (Aug. 27, 2012), http://www.nytimes.com/2012/08/28/technology/active-in-cloud-amazon-reshapes-computing.html [https://perma.cc/DP2F-2JBG] (quoting Andrew R. Jassy, head of Amazon Web Services).

2. Eric Griffith, *What Is Cloud Computing?*, PCMAG (Apr. 17, 2015), http://www.pcmag.com/article2/0,2817,2372163,00.asp [https://perma.cc/A7CD-6MTP] (providing prediction for future cloud computing market).

3. *Id.*

4. Xath Cruz, *Cloud Computing and Its Legal Implications*, CLOUD TIMES (Dec. 3, 2012), http://cloudtimes.org/2012/12/03/cloud-computing-and-its-legal-implications (discussing legal issues deriving from widespread cloud computing).

5. Eric Levenson, *Dell Buys Local Data Storage Company EMC for Record Tech Price*, BOSTON.COM (Oct. 12, 2015), https://www.boston.com/news/innovation/2015/10/12/dell-buys-local-data-storage-company-emc-for-record-tech-price (describing Dell's monumental purchase of Boston-based EMC).

6. *See* Betsy Rosenblatt, *Principles of Jurisdiction*, CYBER.HARVARD.EDU, http://cyber.law.harvard.edu/property99/domain/Betsy.html (last visited Mar. 27, 2017) [https://perma.cc/UQ2S-FUEW] (discussing how traditional jurisdiction interacts with Internet).

7. Griffith, *supra* note 2 (contrasting cloud computing from local computer storage).

8. *See* Vincent O'Keeffe, *Jurisdictional Issues Associated with a Move to the Cloud*, ACADEMIA 3, http://www.academia.edu/6174499/Jurisdictional_issues_.academia.edu/6174499/Jurisdictional_issues_associated_with_a_move_to_the_Cloud (last visited Mar. 27, 2017) [https://perma.cc/4WNK-97XK] (discussing issues with applying law to cloud).

computer resources" instead of utilizing a local server or host to handle operations, such as applications, e-mail, and storage.[9]

While cloud computing experiences continuous technological growth and widespread use across the world, the law has been playing catch up.[10] Data can reside in many different data centers around the world, which can result in jurisdictional dilemmas.[11] Cloud computing acquired its name because when it comes to identifying the current jurisdiction, "[t]here is much cloudy thinking—much shade and little light."[12] For example, corporations like Google have placed data centers on ships in international waters, raising significant and complex jurisdictional issues.[13]

This Note will examine historical jurisdictional doctrines and how they interact and conflict with cloud computing.[14] Part II provides an overview of traditional and Internet-based jurisdiction in the United States.[15] Part II further defines cloud computing, and provides an overview of this technology and how it impacts today's society.[16] Part II concludes with addressing the relationship between cloud computing and the Privacy Shield, previously known as the Safe Harbor Agreement.[17] Finally, this Note, applying a two-part analysis, concludes that traditional jurisdiction rules are not well adapted to modern technology, and advocates for a change in jurisdiction law analogous to recent changes to the Privacy Shield.[18]

II. HISTORY

A. The Beginning of Jurisdiction

Jurisdiction derives its roots from the Fourteenth Amendment's Due Process Clause in the U.S. Constitution.[19] A court must have the authority and must

9. *See* Vangie Beal, *Cloud Computing (the Cloud)*, WEBOPEDIA, http://www.webopedia.com/TERM/C/cloud_computing.html (last visited Mar. 27, 2017) [https://perma.cc/9CJF-BKZ3] (discussing functions of cloud computing).

10. *See* O'Keeffe, *supra* note 8, at 3 (highlighting low legislation rate for laws surrounding cloud computing).

11. *See id.* at 3-4 (outlining reasons for jurisdictional dilemmas, including several misconceptions).

12. *Id.* at 4.

13. *See* Paul T. Jaeger et al., *Where Is the Cloud? Geography, Economics, Environment, and Jurisdiction in Cloud Computing*, FIRST MONDAY (May 4, 2009), http://pear.accc.uic.edu/ojs/index.php/fm/article/view/2456/2171 [https://perma.cc/AW3F-LKLM] (reviewing structure of cloud computing and where it exists).

14. *See infra* Part II.

15. *See infra* Parts II.A-B.

16. *See infra* Part II.C.

17. *See infra* Part II.D.

18. *See infra* Part III.

19. *See* U.S. CONST. amend. XIV, §1 (discussing "life, liberty, or property, without due process of law"). The Supreme Court has described the Due Process Clause as the basis for constitutional limitations on jurisdiction. *See* Pennoyer v. Neff, 95 U.S. 714, 733 (1877); *see also* Wendy Collins Perdue, *What's "Sovereignty" Got to Do With It? Due Process, Personal Jurisdiction and the Supreme Court*, 63 S.C. L. REV.

provide adequate procedural safeguards to require a defendant to appear.[20] In 1877, in *Pennoyer v. Neff*,[21] the U.S. Supreme Court established the nexus between personal jurisdiction and the Fourteenth Amendment's Due Process Clause.[22] Shortly after that, in *International Shoe Co. v. Washington*,[23] the Court defined the relationship that a defendant must have to the forum state to be subject to litigation: minimum contacts.[24]

Defendants are subject to general jurisdiction in their home state and any other state where they are served with process while physically present.[25] General jurisdiction attaches when a defendant is served physically within the forum or state where the defendant is "at home."[26] Over the years, the standard

729, 730 (2012) (acknowledging long established limits based on Due Process Clause and state sovereignty principles); Max Rheinstein, *The Constitutional Bases of Jurisdiction*, 22 U. CHI. L. REV. 775, 792-93 (1955) (noting pre-Fourteenth Amendment limitations based on similar principles of fundamental fairness). The Fifth Amendment's Due Process Clause has also been recognized as imposing a limitation on personal jurisdiction power, though the Supreme Court has thus far declined to decide how, if at all, its limits differ from those the Fourteenth Amendment imposes. *See* Wendy Perdue, *Personal Jurisdiction in the Internet Age: Aliens, the Internet, and "Purposeful Availment": A Reassessment of Fifth Amendment Limits on Personal Jurisdiction*, 48 NW. U. L. REV. 455, 460 (2004).

20. *See* Omni Capital Int'l, Ltd. v. Rudolf Wolff & Co., 484 U.S. 97, 104 (1987) (recognizing need for further procedural requirements beyond compliance with Due Process Clause for jurisdiction assertion); *see also* Murphy Bros., Inc. v. Michetti Pipe Stringing, Inc., 526 U.S. 344, 350 (1999) (stating courts ordinarily cannot exercise jurisdiction over any defendant absent service of process). There are differences in state and federal regulations that can create inconsistencies between which safeguards are required. *See* Charles W. "Rocky" Rhodes, *The Predictability Principle in Personal Jurisdiction Doctrine: A Case Study on the Effects of a "Generally" Too Broad, but "Specifically" Too Narrow Approach to Minimum Contacts*, 57 BAYLOR L. REV. 135, 137-38 (2005) (discussing different states' long-arm statutes' impact on establishing standards for jurisdiction).

21. 95 U.S. 714 (1877).

22. *See id.* at 722. The issue presented in *Pennoyer* was whether an Oregon state court could issue a binding ex parte judgment against a nonresident defendant who was not physically served with process in Oregon. *Id.* at 720-21. The Supreme Court held that it could not. *Id.* at 736. While the Court decided the case based on "well-established principles of public law" rather than constitutional grounds, it noted in dicta that the Due Process Clause of the Fourteenth Amendment limited the ability of state courts to "determine the personal rights and obligations" of nonresident defendants who are not physically served with process with the State and chose not to appear in court voluntarily. *See id.* at 722, 727.

23. 326 U.S. 310 (1945).

24. *See id.* at 316. *International Shoe* highlighted two points: first, jurisdiction is proper if a defendant's actions are continuous and systematic in the forum and the claim arises out of those actions; and second, jurisdiction is improper where a defendant is present in the forum but in a manner unrelated to the claim. *See id*. at 320; *see also An Overview of the Law of Personal (Adjudicatory) Jurisdiction: The United States Perspective*, KENT L., http://www.kentlaw.edu/cyberlaw/docs/rfc/usview.html (last visited Mar. 27, 2017) (reviewing jurisdiction in United States).

25. *See* Walden v. Fiore, 134 S. Ct. 1115, 1121 n.6 (2014) (distinguishing and contrasting specific and general jurisdiction); *see also* Alan M. Trammell & Derek E. Bambauer, *Personal Jurisdiction and the "Interwebs*,*"* 100 CORNELL L. REV. 1129, 1136 (2015) (comparing general and specific jurisdiction). Trammell and Bambauer note that specific jurisdiction is the more modern of the two categories, remaining unarticulated by the Supreme Court until *International Shoe* in 1945. *See* Trammell & Bambauer, *supra*, at 1137. A plaintiff can easily establish general jurisdiction in the defendant's home forum, regardless of whether the claim occurred in that forum. Cassandra Burke Robertson, *The Inextricable Merits Problem in Personal Jurisdiction*, 45 U.C. DAVIS L. REV. 1301, 1308 (2012).

26. *See* Trammell & Bambauer, *supra* note 25, at 1136 (highlighting similar "at home" requirement for

for general jurisdiction has developed into a clear set of metrics.[27] Specific jurisdiction, on the other hand, tends to be more allusive, and requires the defendant's activities give rise to the claim.[28] For a plaintiff to establish specific jurisdiction over a defendant, he or she must pass three thresholds: the defendant must have sufficient minimum contacts with the forum, the claim asserted against the defendant must arise out of those contacts, and the exercise of jurisdiction must be reasonable.[29] Federal appellate judges have criticized the minimum contacts portion of the test as being composed of "gestalt factors" that are "more [of] an art than science."[30]

The minimum contacts analysis has played a significant role in at least twenty Supreme Court decisions since *International Shoe*.[31] These cases focus on defining specific jurisdiction activities and contacts to determine whether jurisdiction is proper.[32] In *McGee v. International Life Insurance Co.*,[33] the Court held that the respondent insurer had sufficient minimum contacts, even though it did not have an office or agents located in California, because it engaged in activities that were directed to the petitioner's forum.[34] In *World-Wide Volkswagen Corp. v. Woodson*,[35] a products-liability case, the Court found Oklahoma jurisdiction improper after analyzing two prongs: whether the defendant's contact with the forum was sufficiently purposeful, and whether the court balanced the defendant's burden with other factors.[36] The Court

corporations' general jurisdiction determinations). For example, a defendant who lives in New York, but travels and causes a car accident in California, can be sued in his or her home state, New York. *Id.*

27. *See id.* For a business, general jurisdiction exists where its principal place of business is located or where it is incorporated. *Id.*

28. *See* Robertson, *supra* note 25, at 1308 (considering specific jurisdiction "plagued by ambiguity and incoherence").

29. *See* Bernadette Bollas Genetin, *The Supreme Court's New Approach to Personal Jurisdiction*, 68 SMU L. REV. 107, 115-16, 121-22 (2015) (analyzing Supreme Court's narrow construction of specific jurisdiction). The Court determined that defendants must "purposefully avail" themselves to the forum in the interest of Due Process Clause concerns. *See id.* at 115.

30. *See* Kevin C. McMungial, *Desert, Utility, and Minimum Contacts: Toward a Mixed Theory of Personal Jurisdiction*, 108 YALE L.J. 189, 189 (1998) (arguing "[a]mbiguity and incoherence have plagued the minimum contacts test for . . . more than five decades"); *see also* Ticketmaster-New York, Inc. v. Alioto, 26 F.3d 201, 209 (1st Cir. 1994) (discussing reasonableness factors in determining whether minimum contacts established). *But see* 4 FED. PRAC. & PROC. § 1067.1 (4th ed. 2017) (noting minimum contacts protect defendants from burdensome litigation and preserves state sovereignty).

31. Robert E. Pfeffer, *A 21st Century Approach to Personal Jurisdiction*, 13 U. N.H. L. REV. 65, 72 (2015) (analyzing Supreme Court's approach in cases post *International Shoe*).

32. *See* Carol Andrews, *Another Look at General Personal Jurisdiction*, 47 WAKE FOREST L. REV. 999, 1010-11 (2012) (highlighting Supreme Court's focus on specific jurisdiction over general jurisdiction).

33. 355 U.S. 220 (1957).

34. *See id.* at 223 (discussing business activities insurance company engaged in to establish minimum contacts in California).

35. 444 U.S. 286 (1980).

36. *See id.* at 297-99 (concluding plaintiff's car accident in Oklahoma did not meet purposeful availment standard); Andrews, *supra* note 32, at 1010-11. The Court concluded that minimum contacts had two policy rationales: to ensure defendants are not hailed into inconvenient forums, and to prevent the State from reaching beyond its limits. *World-Wide Volkswagen*, 444 U.S. at 292. The majority noted that the mere likelihood of

analyzed only one contract dispute, *Burger King Corp. v. Rudzewicz*,[37] where the parties neglected to insert a choice of forum clause in a franchise contract.[38] The Court determined that the defendants were subject to jurisdiction in Florida because they had a substantial connection to the forum, even though their franchise never operated in Florida.[39]

The Court subsequently established the stream of commerce doctrine in order to determine jurisdictional issues in an increasingly mobile society.[40] In *Asahi Metal Industry Co. v. Superior Court of California*,[41] the Court could not exercise personal jurisdiction because the foreign company defendant's mere awareness that their product could enter the forum through the stream of commerce did not establish sufficient contacts.[42] The Court crafted three separate approaches to determine when entering a product into the stream of commerce meets sufficient minimum contact requirements.[43] Justice O'Connor articulated the stream of commerce plus approach, which indicates there must be some activity directed at the forum, such as advertising or sending

foreseeability was not a dispositive factor, rather, the connection the defendant has with the forum and whether that connection creates a reasonable likelihood of being subject to the forum should be considered. *See id.* at 297.

37. 471 U.S. 462 (1985).

38. *See id.* at 465-67 (outlining business locations and law governing franchise).

39. *See id.* at 479-80 (discussing contracts with forum supports personal jurisdiction and does not offend due process). Justice Brennan relied on the defendant's entrance into a franchise agreement with the plaintiff from Florida. *See id.* Additionally, Justice Brennan noted that, although the defendant lacked any physical ties with the forum, the dispute grew out of "a contract which had a substantial connection" with Florida. *Id.* at 479.

40. *See* Martin F. Noonan, *Issues in the Third Circuit: Civil Procedure—Personal Jurisdiction: Evolution and Current Interpretation of the Stream of Commerce Test in the Third Circuit*, 40 VILL. L. REV. 779, 781-82 (1995) (acknowledging international economy's impact on jurisdiction). The evolution and growth of the stream of commerce demonstrates how the Court has developed proper jurisdiction. *See id.*

41. 480 U.S. 102 (1987).

42. *See id.* at 112, 116 (concluding exercise of jurisdiction "unreasonable and unfair"). *But see* Kim Dayton, *Personal Jurisdiction and the Stream of Commerce*, 7 REV. LITIG. 239, 270-71 (1988) (considering *Asahi* product distribution in California certain, not mere foreseeability, therefore capable of establishing jurisdiction). Professor Dayton argues that Justice O'Connor's *Asahi* plurality opinion was not limited to indemnity cases, which indicates that the Court's holding could create a substantial burden on plaintiffs in product liability cases. *See id.* at 272.

43. *See Asahi*, 480 U.S. at 105-16 (representing Justice O'Connor's plurality opinion); *id.* at 116-21 (Brennan, J., concurring in part and concurring in the judgment) (providing Justices Brennan, Marshall, and Blackmun's concurrence with modified reasoning); *id.* at 121-22 (Stevens, J., concurring in part and concurring in the judgment) (representing Justices Sevens, White, and Blackmun's additional concurrence and reasoning). The three *Asahi* opinions demonstrate the major differences between the Justices' application of purposeful availment in the context of minimum contacts. Dayton, *supra* note 42, at 268. For instance, in the Eastern District of Virginia, the court applied Justice O'Connor's stream of commerce plus approach in a trademark and copyright infringement case. *See* AESP, Inc. v. Signamax, LLC, 29 F. Supp. 3d 683, 690 (E.D. Va. 2014) (finding no personal jurisdiction when Pennsylvania corporation did not purposefully direct sales towards Virginia). Alternatively, the Fourth Circuit rejected Justice Brennan's *Asahi* approach, indicating that awareness that a product may be in the stream of commerce is not enough to establish jurisdiction. *See* Lesnick v. Hollingsworth & Vose Co., 35 F.3d 939, 945-46 (4th Cir. 1994) (applying *International Shoe* while acknowledging *Asahi* and *World-Wide Volkswagen*).

replacement parts.[44] Justice Brennan created the pure stream of commerce test, which provides that a defendant whose components are incorporated into a final product has sufficient contact with any forum where the defendant knows the final product is sold.[45] Justice Stevens argued for a middle ground, stating that there needs to be an assessment of volume and sales to determine whether the court has jurisdiction.[46]

B. When Jurisdiction Meets the Internet

The Internet began in 1969 as a military research project funded by the Advanced Research Projects Agency.[47] At the time, the computer network connected the military, defense contractors, and universities conducting research.[48] The modern Internet is now leveraged for storing personal information, various modes of communication, and a plethora of commercial transactions.[49] The word "Internet" first appeared in a judicial opinion in 1991.[50] In *Bensusan Restaurant Corp. v. King*,[51] Judge Van Graafeiland correctly stated that "attempting to apply established trademark law in the fast-

44. *See Asahi*, 480 U.S. at 112 (explaining Due Process Clause requires more than defendant's mere knowledge of products in forum to establish jurisdiction).

45. *See id*. at 117 (Brennan, J., concurring in part and concurring in the judgment) (emphasizing defendant's knowledge of product's final destination and where lawsuit occurred). Justice Brennan argued that, according to precedent, Due Process is not violated when jurisdiction is deemed proper based on the placement of a product in the stream of commerce. *Id.* Justice Brennan concluded that there were sufficient contacts when the *Asahi* defendant knew that the manufacturer was making sales in California. *Id.* at 121.

46. *See id*. at 121-22 (Stevens, J., concurring) (considering fairness aspect of jurisdiction). Justice Stevens disagreed with the distinction Justice O'Connor made between mere awareness of products entering the stream and defendants purposefully availing their activities to the forum. *See id.*

47. Carolyn Duffy Marsan, *The Evolution of the Internet*, PC WORLD (Feb. 12, 2009), http://www.pc world.com/article/159471/evolution_internet.html [https://perma.cc/VU6G-9JGC] (discussing growth of Internet since its inception).

48. *See id*. In 2001, there were just under roughly 200 million Internet users; by 2006 that number jumped to over 400 million. *Id.* In 2000, U.S. e-commerce sales totaled $27,467, with total sales close to $102,238, not including the fourth quarter of sales. *Id.*

49. *See* Michele N. Breen, Comment, *Personal Jurisdiction & the Internet: "Shoehorning" Cyberspace into* International Shoe, 8 SETON HALL CONST. L.J. 763, 764-66 (1998) (explaining evolution of rigid standards applied to new technologies). In the 1990s, personal jurisdiction became a big issue when national corporations began using the Internet for commerce. *See* 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, 560 (2009) (explaining tensions between physical location and Internet activity). The Internet and the term "globalization" have become intertwined because of the increasing mobility and limitless boundaries between people and organizations that the Internet has created. *See* Paul Schiff Berman, *The Globalization of Jurisdiction*, 151 U. PA. L. REV. 311, 314-15 (2002). Issues arise because actions with no physical connection to local communities may nevertheless impact those local communities. *See id.* at 319. As such, some scholars have argued that cyberspace should have its own jurisdiction. *Id.* at 315.

50. *See* United States v. Morris, 928 F.2d 504, 505 (2d Cir. 1991) (mentioning Internet for first time in federal opinion, considering it "worm or virus") (internal quotations omitted); Michael L. Rustad & Thomas H. Koenig, *Rebooting Cybertort Law*, 80 WASH. L. REV. 335, 364-66 (2005) (explaining America's technological shift with first 1991 cybertort case involving Internet).

51. 126 F.3d 25 (2d Cir. 1997).

developing world of the [I]nternet is somewhat like trying to board a moving bus."[52]

Circuit courts are currently split on how to determine whether sufficient contacts have been established on the Internet.[53] Emanating from *Zippo Manufacturing Co. v. Zippo Dot Com, Inc.*,[54] the *Zippo* Sliding Scale Test (Zippo Test) looks at the spectrum of the defendant's business activity on the Internet; at one end of the spectrum, the business clearly and knowingly transmits certain data, while at the other end, the business utilizes a passive website that merely provides information.[55] Similarly, *Calder v. Jones*[56] coined the *Calder* Effects Test (Calder Test), which considers whether the defendant intentionally directs harm at the forum state.[57] Lastly, in *Grand River Enterprises Six Nations, Ltd. v. Pryor*,[58] the court looked to the totality of the defendants' contacts with a forum state.[59]

Courts have begun to move away from the Zippo Test and are instead utilizing the Calder Test, a more traditional approach toward personal jurisdiction.[60] Courts have also turned to the Calder Test to determine issues involving Internet transactions and social media sites.[61] The Supreme Court

52. *See id*. at 27; *see also* Dunham, *supra* note 49, at 572 (analyzing courts' predominately passive or active measurements to determine Internet contacts).

53. *See* A. Benjamin Spencer, *Jurisdiction and the Internet: Returning to Traditional Principles to Analyze Network-Mediated Contacts*, 2006 U. ILL. L. REV. 71, 73-74 (2006) (reviewing approaches courts take to determine sufficient contacts).

54. 952 F. Supp. 1119 (W.D. Pa. 1997).

55. *See id.* at 1124 (reasoning sliding scale consistent with personal jurisdiction principles). The court discussed that when contacts fall within the middle ground, personal jurisdiction may be analyzed according to the extent of interactivity and type of commercial transactions that occurred. *Id. But see* Hy Cite Corp. v. Badbusinessbureau.com, L.L.C., 297 F. Supp. 2d 1154, 1160 (W.D. Wis. 2004) (criticizing use of interactive versus passive website in context of jurisdiction); Millennium Enters., Inc. v. Millennium Music, LP, 33 F. Supp. 2d 907, 922-23 (D. Or. 1999) (arguing plaintiff must actually direct conduct towards forum to meet jurisdiction threshold).

56. 465 U.S. 783 (1984).

57. *See id.* at 789 (stating plaintiff's tortious actions intentionally targeted California). Justice Rehnquist noted that the plaintiffs had knowledge that their conduct would injure the defendant where she lived and worked. *Id.* at 789-90. Additionally, Justice Rehnquist rejected the notion that the First Amendment should be a part of the jurisdictional analysis due to the libel and defamation claims. *Id.* at 790.

58. 425 F.3d 158 (2d. Cir. 2005).

59. *Id.* at 166 (reasoning single event will not determine establishment of sufficient contacts); *see also* CutCo Indus., Inc. v. Naughton, 806 F.2d 361, 365 (2d Cir. 1986) (opining totality of defendant's action determines proper jurisdiction).

60. *See* Michael A. Geist, *Is There a There There? Toward Greater Certainty for Internet Jurisdiction*, 16 BERKELEY TECH. L.J. 1345, 1371-72 (2001) (discussing shift away from Zippo Test toward effects-based test). For example, courts are more likely to examine the effect a website has in their jurisdiction rather than the website's particular characteristics. *Id*.

61. *See* Boschetto v. Hansing, 539 F.3d 1011, 1017 (9th Cir. 2008) (determining one contract for sale of goods insufficient connection to forum). The Ninth Circuit determined that a California Internet buyer of an antique car did not meet the threshold jurisdictional requirements because the buyer did not purposefully direct his actions towards Wisconsin where the sellers of the car resided. *See id.* Companies that have a social media presence do not automatically avail themselves to court even when the social media site, such as Facebook, is an interactive website. Evan Brown, *Business Facebook Page Did Not Support Personal Jurisdiction Out of*

has also recently recharged its interest in jurisdictional procedural matters.[62] In 2014, the Court issued two decisions in a two-month span, limiting the reach of personal jurisdiction over defendants.[63] First, in *Daimler AG v. Bauman*,[64] the Court held that general jurisdiction over a corporation exists where the corporation is at home, meaning its principal place of business, the state where it is incorporated, or other limited situations.[65] Second, in *Walden v. Fiore*,[66] the Court applied the Calder Test and determined that there was no jurisdiction, even though the defendant's actions affected the plaintiffs and were clearly connected to the forum.[67]

C. An Overview of Cloud Computing

Around 1955, John McCarthy, the computer scientist that created the term "artificial intelligence," also developed the idea of time sharing, which resembles cloud computing.[68] In 1997, University of Texas Professor Ramnath Chellappa coined the term "cloud computing" while discussing "new

State, INTERNETCASES (Apr. 14, 2013), http://blog.internetcases.com/2013/04/14/business-facebook-page-did-not-support-personal-jurisdiction-out-of-state [https://perma.cc/T8XA-9B9L] (stating advertising on Facebook does not amount to purposefully directed contacts to establish jurisdiction). Additionally, under the Calder Test, posting negative remarks on the Internet, specifically Facebook, where the commenter knows the defendant is in the forum state is not enough to establish personal jurisdiction. Eric Goldman, *No Personal Jurisdiction Over Nasty Facebook Post*—Burdick v. Superior Court, TECH. & MARKETING L. BLOG (Jan. 16, 2015), http://blog.ericgoldman.org/archives/2015/01/no-personal-jurisdiction-over-nasty-facebook-post-burdick-v-superior-court.htm [https://perma.cc/FL42-3V28] (discussing limitations Supreme Court placed on Calder Test).

62. Rodger Citron, Walden v. Fiore*: The Supreme Court Turns to Personal Jurisdiction Issues*, JUSTIA (Dec. 9, 2013), https://verdict.justia.com/2013/12/09/walden-v-fiore-supreme-court-turns-personal-jurisdiction-issues [https://perma.cc/7X7N-FBRF] (highlighting failed attempt at cohesive approach to personal jurisdiction).

63. *See generally* Walden v. Fiore, 134 S. Ct. 1115 (2014) (holding Nevada court had no jurisdiction over petitioner); Daimler AG v. Bauman, 134 S. Ct. 746 (2014) (concluding California not proper venue for defendant). In 2011, the Court sought to provide more guidance on personal jurisdiction, but ended up with an even more splintered approach. *See* Citron, *supra* note 62 (reviewing Supreme Court's non-uniform approach in *J. McIntyre Mach., Ltd. v. Nicastro*, 564 U.S. 873 (2011)).

64. 134 S. Ct. 746 (2014).

65. *See id.* at 760-62 (holding California not corporate plaintiff's home).

66. 134 S. Ct. 1115 (2014).

67. *See id.* at 1126 (concluding effect of defendant's conduct not enough for jurisdiction in plaintiff's forum). The Court's decision ultimately limited courts' abilities to exercise personal jurisdiction over defendants who reside out of state, but whose conduct reaches out-of-state plaintiffs. *See* Charles W. "Rocky" Rhodes & Cassandra Burke Robertson, *Toward a New Equilibrium in Personal Jurisdiction*, 48 U.C. DAVIS L. REV. 207, 208 (2014) (discussing plaintiffs' limited ability to determine where to file lawsuits). The growth of the Calder Test corresponds with the growth of the Internet. *Id.* at 227. The Internet gave individuals the ability to reach outside their forums more readily, and thus, made the Calder Test more prominent. *See id.* The Court's unanimous and brief *Walden* opinion indicated that its impact is not yet known and leaves room for ambiguity. *Id.* at 252.

68. John Patrick Pullen, *Where Did Cloud Computing Come From, Anyway?*, TIME (Mar. 19, 2015), http://time.com/3750915/cloud-computing-origin-story (discussing emergence of cloud computing with development of computers). Service bureaus emerged in the 1960s and 1970s, which gave users the ability to share their computers. *Id.*

paradigms in computing."[69] Simply, cloud computing provides users with an on-demand network for their computing services.[70] There are generally three different types of clouds: software as a service (SaaS), which is the most common because it is delivered to users in the form of software you can buy or install, such as Microsoft Word; infrastructure as a service (IaaS), which provides more control over the infrastructure and includes programs such as Amazon Web Services; and platform as a service (PaaS), which enables users to create their own applications, such as Google App Engine.[71]

Cloud computing is one of the most significant technological advances for businesses around the world: just as "PCs were to the 1970s," cloud computing is "a technological and societal leap that will change how businesses function, how cities are planned, how people carry out their work[,] and what citizens expect from online services."[72] The cloud offers many advantages to companies worldwide, including streamlining mergers and acquisitions, making individuals more productive, and significantly lowering information technology (IT) costs.[73] These advantages incentivize companies like

69. Keith Gill, *The History of "Cloud Computing" and "Cloud Storage*,*"* LINKEDIN (June 2, 2014), https://www.linkedin.com/pulse/20140602173917-185626188-the-history-of-cloud-computing-and-cloud-storage [https://perma.cc/J9U3-M99J]; *30 Years of Accumulation: A Timeline of Cloud Computing*, GCN (May 30, 2013), https://gcn.com/Articles/2013/05/30/GCN30-Timeline-Cloud.aspx [https://perma.cc/FL3T-P56F] (outlining growth of cloud computing over last three decades). A majority of the American public remains unaware of what cloud computing actually is, with some believing it involves actual clouds. Damon C. Andrews & John M. Newman, *Personal Jurisdiction and Choice of Law in the Cloud*, 73 MD. L. REV. 313, 324 (2013) (explaining "[b]efore courts can adjudicate disputes . . . they must understand what cloud computing is").

70. *See* Kevin McGillivray, *Conflicts in the Cloud: Contracts and Compliance with Data Protection Law in the EU*, 17 TUL. J. TECH. & INTELL. PROP. 217, 218 (2014) (describing cloud computing aspects of providing users with immediate storage, software, and applications).

71. *See* J. Nicholas Hoover, Note & Comment, *Compliance in the Ether: Cloud Computing, Data Security & Business Regulation*, 8 J. BUS. & TECH. L. 255, 258-59 (2012). Clouds are offered in different "deployment models," including "private, public, and community clouds." *Id.* at 258. Private clouds and community clouds usually operate in a company's data center and are used by individual companies, while public clouds come in various forms accessible to the public, such as Salesforce and Google. *See id.* The three different types of clouds have also been metaphorically defined as "[p]izza as a [s]ervice." Albert Barron, *Pizza As a Service*, LINKEDIN (July 30, 2014), https://www.linkedin.com/pulse/20140730172610-9679881-pizza-as-a-service [https://perma.cc/D4E9-APZ6] (discussing difficulty of explaining cloud computing and simplifying it with pizza metaphor). IaaS is when you buy pre-packaged dough and some of the ingredients. *See id.* PaaS is when the pizza is delivered to your home. *See id.* Lastly, SaaS is when you get pizza at a restaurant. *See id.*

72. Honor Mahony, *EU Gets to Grips with Cloud Computing*, EU OBSERVER (Apr. 5, 2011), https://euobserver.com/news/32048 [https://perma.cc/C2LR-AZV2]; *see also* Nancy J. King & V.T. Raja, *What Do They Really Know About Me in the Cloud? A Comparative Law Perspective on Protecting Privacy and Security in Sensitive Consumer Data*, 50 AM. BUS. L.J. 413, 418 (2013) (providing overview cloud computing benefits for companies to serve public's digital needs). For the cloud to be successful, it must make security a top concern to gain users' trust who are providing sensitive data. *See* King & Raja, *supra*, at 418-19.

73. *See* Joe McKendrick, *5 Benefits of Cloud Computing You Aren't Likely to See in a Sales Brochure*, FORBES (July 21, 2013), http://www.forbes.com/sites/joemckendrick/2013/07/21/5-benefits-of-cloud-computing-you-arent-likely-to-see-in-a-sales-brochure (discussing cloud computing advantages not commonly cited); *see also* Andrew McAfee, *What Every CEO Needs to Know About the Cloud*, HARV. BUS. REV. (Nov.

Microsoft to leverage cloud computing services; Microsoft's cloud computing earnings increased $1.3 billion from the previous fiscal year, and were stronger than their mobile division earnings.[74] Furthermore, Amazon's Web Services division provides immense computing power with lower costs and higher accessibility.[75] Cloud computing also has pitfalls, including concerns about sensitive data security, limitations on storage, and inconsistent regulations.[76] Some of these issues derive from the complexities of cloud computing, and in some instances, the inability to pinpoint where the data resides.[77]

D. When Cloud Computing and Jurisdiction Collide

Data may travel long distances and intersect with various jurisdictional boundaries.[78] For example, a computer or other device is connected to the Internet, and then uploads data onto the cloud server.[79] That cloud server is

2011), https://hbr.org/2011/11/what-every-ceo-needs-to-know-about-the-cloud (describing cloud computing significance and long-lasting shift in computing power). The cloud also provides users with the ability to enter into a new industry or business. McKendrick, *supra*. It gives businesses more time and money to delve into new enterprises because the cloud's on-demand resources reduce the time needed for such endeavors. *Id*. Additionally, it gives chief technology officers the ability to act strategically rather than dealing with IT system repairs, which can tie up about eighty percent of their budget. *Id*. According to Microsoft, only eleven percent of a company's IT budget will go toward developing new and strategic applications and systems. McAfee, *supra*.

74. *See* Nick Wingfield, *For Microsoft, Cloud Business Looks More Promising than Mobile*, N.Y. TIMES (Oct. 21, 2014), http://bits.blogs.nytimes.com/2014/10/21/for-microsoft-cloud-business-looks-more-promising-than-mobile [https://perma.cc/6RH3-NN42] (discussing opening new data centers on global scale, enrolling over 10,000 customers on cloud offering platform). Cloud computing may also allow emerging economies to increase their economic development. *See* WORLD ECON. FORUM, EXPLORING THE FUTURE OF CLOUD COMPUTING: RIDING THE NEXT WAVE OF TECHNOLOGY-DRIVEN TRANSFORMATION 13 (2010), http://www3.weforum.org/docs/WEF_ITTC_FutureCloudComputing_Report_2010.pdf [hereinafter EXPLORING THE FUTURE OF CLOUD COMPUTING] [https://perma.cc/8KUG-7UCL] (noting reviewing data suggests important innovation for users instead of reducing costs).

75. *See* Hardy, *supra* note 1 (explaining companies rent computer server time from Amazon to meet their business objectives). For example, Climate Corporations performs weather simulations for one million locations in the United States; such capacity is possible through Amazon's Web Services. *See id.* It is estimated that these cloud services earn Amazon $1 billion in revenue. *Id.*

76. *See* EXPLORING THE FUTURE OF CLOUD COMPUTING, *supra* note 74, at 9. Some of the largest roadblocks to successfully using the cloud to its fullest potential include security, privacy, and governance. *Id.* Service providers are concerned about the lack of governance, outdated laws, and users that do not adequately understand the technology. *Id.*

77. *See* Hoover, *supra* note 71, at 260-61 (noting difference from traditional outsourcing). Users no longer have the physical infrastructure of their data because cloud computing takes control out of their hands. *See id.* at 261. Such loss of control over physical data creates a need for transparency from cloud servicers for both businesses and individuals. *Id.*

78. *See* Urs Gasser, *Cloud Innovation and the Law: Issues, Approaches, and Interplay* 15-16 (Berkman Ctr. For Internet & Soc'y at Harvard Univ. Research Pub. No. 2014-7, 2014), http://ssrn.com/abstract=2410271 [https://perma.cc/PJ7M-7G5B] (discussing horizontal issues, including jurisdiction, compliance, and transparency). The first approach to solving legal problems in regards to technological innovation has been applying old laws to the new technology. *Id.* at 16-17. The second approach is creating new laws through legislation or regulatory intervention. *Id.* at 18.

79. *See* Reeta Sony et al., *Data Protection & Cloud Computing: A Jurisdictional Aspect* (Nat'l L. Univ.,

connected to a data center that may be located anywhere in the world—the data centers may be large rooms full of physical servers, or they may be virtual servers.[80] Large companies like Microsoft and Amazon determine the locations of their servers based on climate, political atmosphere, government friendliness to the United States, and population education.[81] Furthermore, the "Google Navy" and Pirate Bay's drones use sea and air as locations for their servers, ensuring even more complex jurisdictional dilemmas.[82]

U.S. courts have addressed issues relating to data servers located within state borders.[83] In *Aitken v. Communications Workers of America*,[84] the court declared jurisdiction was proper because the company's data server and some of its employees were located in Virginia.[85] In *MacDermid, Inc. v. Deiter*,[86] a defendant residing in Canada conducted illegal activity on servers located in Connecticut.[87] The court held that the defendant purposefully availed herself to Connecticut when she accessed a computer server located in Connecticut.[88]

New Delhi, Council of Sci. and Indus. Research, New Delhi Research Paper), https://www.academia.edu /7728622/Data_Protection_and_Cloud_Computing_a_Jurisdictional_Aspect (last visited Mar. 27, 2017) (describing cloud computing upload and data storage process).

80. *Id*.

81. *See* Ingrid Burrington, *The Strange Geopolitics of The International Cloud*, ATLANTIC (Nov. 17, 2015), http://www.theatlantic.com/technology/archive/2015/11/the-strange-geopolitics-of-the-international-cloud/416370 [https://perma.cc/QPA6-9XEB] (reviewing reasons large companies place data centers abroad). Ireland's cool climate, coupled with its 12.5% corporate tax rate, have led to an increase in large companies moving assets and headquarters to the country. *Id.*

82. *See* Sony et al., *supra* note 79 (explaining Google Navy and Pirate Bay's innovative drone use for cloud servers). One solution may be leveraging international laws for litigants to select the appropriate forum. *See id.* Google received a patent on a tide-powered floating data center, which the ocean cools. Chris Taylor, *Google May Be Launching Floating Data Centers Off U.S. Coasts*, MASHABLE (Oct. 25, 2013), http://mashable.com/2013/10/25/google-floating-data/#2ze9BwEbLmqJ [https://perma.cc/PM5F-YDP2] (discussing how storing data on floating servers can save Google millions). The Pirate Bay drones were built intending to avoid legal repercussions that their users could experience on land. *See* Eloise Lee, *The World's Biggest Internet Piracy Site Plans To Use Aerial Drones to Keep Its Servers Out of Reach*, BUS. INSIDER (Mar. 21, 2012), http://www.businessinsider.com/pirate-bay-server-drones-2012-3 [https://perma.cc/E4V9-84PN] (outlining Pirate Bay's approach toward new methods of delivering pirated materials to users).

83. *See* Sasha Segall, Note, *Jurisdictional Challenges in the United States Government's Move to Cloud Computing Technology*, 23 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 1105, 1121-22 (2013) (noting courts have held server location indicates valid State interest).

84. 496 F. Supp. 2d 653 (E.D. Va. 2007).

85. *See id.* at 659 (asserting use of computer within forum constitutes sufficient contacts). The court stated that the defendant purposefully availed himself to the forum when he sent targeted e-mails to Verizon Business, which had servers and employees in the forum. *See id.*

86. 702 F.3d 725 (2nd Cir. 2012).

87. *See id.* at 727, 730 (concluding defendant purposefully directed her conduct toward Connecticut). The court recognized the defendant was aware of confidential information and that the company's email system was stored on the servers in the forum. *See id.*

88. *See id.* (holding test for jurisdiction met because defendant knew Connecticut housed servers); *see also* Caro v. Fidelity Brokerage Serv., No. 3:14-CV-01028 (CSH), 2015 U.S. Dist. LEXIS 57116, at *51-52 (D. Conn. Apr. 30, 2015) (asserting no evidence proving defendant accessed servers in Connecticut). Plaintiffs did not present proper evidence to indicate that defendant used a server located in Connecticut; thus, the court found jurisdiction improper. *See Caro*, 2015 U.S. Dist. LEXIS 57116, at *51.

At the federal level, some argue that the Supreme Court has made the establishment of proper jurisdiction even more challenging through unclear and inconsistent decisions.[89] In *Riley v. California*,[90] the Court concluded that searching a cell phone requires a warrant, which changes the legal paradigm that cloud computing impacts.[91] In *American Broadcasting Co. v. Aereo, Inc.*,[92] the defendant allowed users to access free broadcast television that is stored remotely, mimicking the cloud's qualities.[93] The Court held similar copyright laws should apply because the defendant's technology was similar to an antenna television.[94] In his dissent, Justice Scalia argued that this technology was unlike antenna television, and to treat it as such creates a rule that is too broad to be effective.[95]

Larger issues arise when international stakeholders are involved, as illustrated, for example, by Microsoft's refusal to provide the U.S. government with e-mails located on its servers in Ireland.[96] Additionally, at the end of 2015, the European Court of Justice struck down the fifteen-year-old Safe Harbor Agreement (Agreement), which was the catalyst for data transfers between the United States and the EU.[97] In *Yahoo! Inc. v. La Ligue Contre Le*

89. *See* Margot Kaminski, *The Supreme Court's Cloud-Computing Confusion*, NEW REPUBLIC (June 26, 2014), http://www.newrepublic.com/article/118402/supreme-courts-cloud-computing-confusion [https://perma.cc/HU63-XDDP] (explaining two contradictory cases Court decided). One case demonstrated the Court's hesitation to make legal shifts in regards to technology, and the other showed the Court's openness to change as technological advances continue. *See id.*

90. 134 S. Ct. 2473 (2014).

91. *See id.* at 2478-79 (highlighting cell phones' significant storage capacity); Kaminski, *supra* note 89 (explaining "Supreme Court's [c]loud-[c]omputing [c]onfusion"). Justice Roberts concluded that the differences between cellphones and other objects on one's person are so significant that they must warrant a different search procedure. *See Riley*, 134 S. Ct. at 2493. Furthermore, data from a phone can be tracked for many years, and ninety percent of Americans who own cell phones keep "digital record[s] of nearly every aspect of their lives." *Id.* at 2479.

92. 134 S. Ct. 2498 (2014).

93. *See id*. at 2500 (considering defendant Aereo's technology combination of servers and antennas); *see also* Kaminski, *supra* note 89 (arguing majority refused to recognize paradigm-shifting technology). Furthermore, the Court did not address which rule would apply to technologies that were paradigm-shifting. *See id.*

94. *See Aereo*, 134 S. Ct. at 2507-07 (noting court's technology comparisons).

95. *See id.* at 2512-14 (Scalia, J., dissenting) (arguing majority opinion will cause confusion for many years). Justice Scalia argued that the majority made no clear rule that demonstrates when the "cable-TV-lookalike" rule applies. *See id*. at 2516.

96. Zoya Sheftalovich, *The Court Case That Could Sink Safe Harbor*, POLITICO (Jan. 4, 2016), http://www.politico.eu/article/the-court-case-that-could-sink-safe-harbor-microsoft-department-of-justice-data-protection-ireland [https://perma.cc/GWU5-WTPW] (discussing Microsoft's impact on European Union (EU) and U.S. relations regarding cloud data protections). In 2013, the U.S. Department of Justice served Microsoft with a criminal search warrant to attain records from a specific email account. *Id.* "When a person stores his or her most personal information in the cloud, it should be entitled to the same protection as the same information stored on paper in a desk drawer, or in a sealed letter, or on the hard drive of a computer," according to John Frank, Vice President of EU government affairs for Microsoft. *Id.*

97. *See* Natalia Drozdiak & Sam Schechner, *EU Court Says Data-Transfer Pact with U.S. Violates Privacy*, WALL STREET J. (Oct. 6, 2015), http://www.wsj.com/articles/eu-court-strikes-down-trans-atlantic-safe-harbor-data-transfer-pact-1444121361 (explaining Agreement infringes EU citizen's privacy rights). The

Racisme et L'antisemistisme,[98] two French civil rights organizations sued U.S.-based Yahoo! because it made available Nazi content on its website in France.[99] After the French Court found Yahoo! liable because the content was viewed in France, Yahoo! appealed in the United States, reaching the Ninth Circuit.[100] The Ninth Circuit reversed portions of the previous French holding.[101]

The United States approaches cloud computing through legislation and regulations.[102] Given the global nature of cloud computing, international regulations provide more guidance for individuals and businesses.[103] With that said, there is no single set of jurisdictional rules because there is no single applicable international law, and some countries—like Canada—are multi-jurisdictional.[104]

The former Agreement—now the Privacy Shield—between the United States and the EU exemplified the global approach, and was developed to help the United States comply with EU personal data security regulations and alleviate potential trade disruption.[105] The need for such an agreement developed when the EU adopted the Data Privacy Directive (Directive), which states: "personal data must be . . . processed fairly and lawfully"; it shall be "collected for specified, explicit and legitimate purposes"; the data must be "adequate, relevant and not excessive in relation to the purposes for which they

Agreement allowed 4,500 companies like Apple and Google to transfer data from the EU into the United States. *See id.*

98. 433 F.3d 1199 (9th Cir. 2006).

99. *See id.* at 1201-03 (discussing French court ordering Yahoo! to take all possible actions to remove Nazi content). The French court order stated that Yahoo! and Yahoo! France could both be fined 100,000 euros per day if the information was not removed. *Id.* at 1203. Yahoo! argued that there was no technology that would allow them to remove all of the content and comply fully with the French court order. *See id.* Yahoo! claimed that they could identify only seventy percent of French users from their website—meaning potentially thirty percent would not be blocked from using the Nazi content. *See id.*

100. *See id.* at 1204-05 (arguing unenforceability of French court order in United States).

101. *See id.* at 1211, 1224 (explaining personal jurisdiction due to French defendant's activities directed towards California). French defendants sent a cease and desist letter to Yahoo!'s headquarters in Santa Clara, California, served Yahoo! in California for the French suit, and served two French court orders on Yahoo! in California. *Id.* at 1205.

102. *See* O'Keeffe, *supra* note 8, at 3, 7 (discussing U.S. government's approaches seeking to mitigate legal risk of cloud computing).

103. *See id.* at 3-7 (listing various methods to determine jurisdiction).

104. *See id.* at 5-6 (providing overview of differences in various countries' jurisdictional rules).

105. *See* Max Metzger, *EU Privacy Shield Soon to Be Finalised*, SC MAG. (Feb. 12, 2016), http://www.scmagazine.com/eu-privacy-shield-soon-to-be-finalised [https://perma.cc/B9J2-M9KK] (discussing Agreement's transformation into Privacy Shield); *U.S.-EU Safe Harbor Overview*, EXPORT.GOV, https://build.export.gov/main/safeharbor/eu/eg_main_018476 (last updated Dec. 18, 2013) [https://perma.cc/VP3B-Z8MW] (outlining principles behind Agreement between EU and United States). The United States relies on self-regulation, legislation, and regulation for data privacy protection, while the EU implements comprehensive legislation. *U.S.-EU Safe Harbor Overview*, *supra*; *see also* Robert R. Schriver, Note, *You Cheated, You Lied: The Safe Harbor Agreement and Its Enforcement by the Federal Trade Commission*, 70 FORDHAM L. REV. 2777, 2780 (2002) (describing "astronomical" losses if U.S. companies ignore EU data privacy regulations).

are collected . . . [and] accurate"; and it must be "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed."[106] The Agreement permits U.S. corporations to self-certify, indicating that they will provide adequate protection to EU customers and organizations according to the Privacy Shield's terms.[107] Some argue that the Agreement was vital in growing digital commerce and encouraging innovation.[108] In a 2015 case, the EU's Court of Justice declared the Agreement invalid because the plaintiff, a Facebook user, successfully argued that in light of Edward Snowden disclosures, Facebook did not "adequately protect his personal information" pursuant to the EU Directive.[109] Around the time of the court decision, Amazon announced that it would open cloud services in the United Kingdom, and Microsoft indicated that it would add new Azure centers operating on Microsoft cloud services in Germany and the United Kingdom.[110]

In February 2016, the EU Commission and the U.S. Department of Commerce replaced the invalidated Agreement with the Privacy Shield, which requires U.S. companies to comply with EU privacy principles, and calls for the U.S. government to limit tapping into data for national security purposes.[111]

106. Directive 95/46/EC, of the European Parliament and of the Council of 24 Oct. 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data Directive 95/46/EC, 1995 O.J. (L 281) 9, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML (last visited Mar. 27, 2017) [https://perma.cc/L35T-42SQ] (outlining EU's process and movement for personal data).

107. *See Self-Certification Information*, PRIVACY SHIELD FRAMEWORK, https://www.privacyshield.gov/article?id=Self-Certification-Information (last visited Mar. 27, 2017) [https://perma.cc/C7X3-XMJM] (describing process to quickly complete self-certification).

108. *See* Bradley S. Shear, *A New US-EU Safe Harbor Agreement*, LAW 360 (Oct. 29, 2015), http://www.law360.com/articles/720191/a-new-us-eu-safe-harbor-agreement [https://perma.cc/78K8-TU4X] (arguing updated Agreement will provide guidance to companies conducting business overseas). In 2025, the value of the international digital economy is predicted to be $4.8 trillion. *Id.* Stronger legal protections for consumer privacy will lead to a higher probability that the digital economy will reach its full potential. *Id.* "When the [EU] adopted the . . . Directive, the United States could not meet the 'adequate protection' standards"; thus, negotiations for the Agreement began because U.S. businesses were potentially going to lose "billions of dollars in annual transactions," and enter into a potential trade war with the EU. *See* Edward R. Alo, Comment, *EU Privacy Protection: A Step Towards Global Privacy*, 22 MICH. ST. INT'L. L. REV. 1095, 1110 (2014) (discussing differences between EU and United States data security policies).

109. *See* Shear, *supra* note 108 (discussing student who initiated legal proceedings which ultimately struck down Safe Harbor protocols). The Agreement offered companies and consumers a more transparent and "accountable process enforced by a government regulat[ion]." *Id.*

110. Barb Darrow, *Tech Companies Are Seizing on the Collapse of the Safe Harbor Agreement*, FORTUNE (Nov. 17, 2015), http://fortune.com/2015/11/17/tech-providers-safe-harbor [https://perma.cc/36E6-AP88] (discussing technology companies announcing new international products, services, and data centers during Agreement's collapse). The head of partnerships for the United Kingdom-based Premiership Rugby previously stored data on U.S.-based providers, but switched to storing information in the United Kingdom because of its data protection policies. *Id.*

111. *See* Metzger, *supra* note 105 (stating half of certified Safe Harbor companies remained unaware of Agreement's invalidation in October 2015). Businesses will need to be more aware of the location of their data and which measures they are taking to protect it. *See id.* The Agreement did not include harsh provisions

The Privacy Shield intends to give EU citizens more protection over their data, including access to various avenues of dispute resolution forums.[112] One of these forums, the Judicial Redress Act, will grant EU citizens protection under the Privacy Act of 1974, and allow them to bring civil actions and obtain civil remedies in U.S. courts in a similar manner as U.S. citizens in such judicial proceedings.[113] The Judicial Redress Act passed with an amendment that requires the U.S. Attorney General to confirm that foreign countries' "policies regarding the transfer of personal data for commercial purposes . . . do not materially impede the national security interests of the United States."[114] Some technology industry leaders praise the Judicial Redress Act's passage.[115]

regarding compliance, but the Privacy Shield intends to incorporate more rigorous repercussions to those who break its obligations. *See id.* The Privacy Shield includes a commitment that public officials will not access private information without limitations and transparency. *See* Kevin L. Jackson, *Cancer, Cloud and Privacy Shield*, TECH. PAGE ONE, http://www.techpageone.co.uk/industries-uk-en/cancer-cloud-privacy-shield/ (last visited Mar. 27, 2017) [https://perma.cc/HXF4-72A8] (explaining uncertainty Privacy Shield will have on trans-Atlantic cloud computing); *see also Privacy Shield Program Overview*, PRIVACY SHIELD, https://www.privacyshield.gov/Program-Overview (last visited Mar. 27, 2017) [https://perma.cc/8F8G-F6SG] (highlighting key features of plan).

112. *EU-US Privacy Shield Fact Sheet*, COMMERCE.GOV (Feb. 2, 2016), https://www.commerce.gov/news/fact-sheets/2016/02/eu-us-privacy-shield [https://perma.cc/F9DM-WLVG] (outlining commercial oversight provided to EU citizens). The Department of Commerce stated that the new Privacy Shield will improve transparency and better inform EU citizens of their rights. *Id.* Furthermore, the Privacy Shield intends to incorporate more safeguards against data used for U.S. national security, including "constitutional, statutory, and policy safeguards[,] . . . with active oversight provided by all three branches of the U.S. government." *Id.* Lastly, the Department of Commerce stated that President Obama, through Presidential Policy Directive 28, enhanced privacy protections for U.S. and non-U.S. citizens, and increased review and oversight of intelligence activities. *Id.* On the other hand, some did not believe that the new Privacy Shield would pass muster. Paul Van den Bulck & Raphaël Krowicki, *EU-U.S. Privacy Shied: Better or Worse?*, LEXOLOGY (Feb. 15, 2016), http://www.lexology.com/library/detail.aspx?g=65a8c9b4-9a7d-407b-b7f4-461cafad9bff [https://perma.cc/KSR7-4YSY] (arguing several issues need resolution before Privacy Shield becomes effective). The European Court of Justice emphasized that when data is transmitted outside of the EU, the country that receives the data must have data projections equivalent to those of the EU. David Hoffman, *A Transatlantic Common Language for Privacy*, NEW EUROPE (Feb. 8, 2016), http://neurope.eu/article/a-transatlantic-common-language-for-privacy [https://perma.cc/W3MR-8YXZ] (discussing further legal challenges likely to arise regarding international data exchange). Additionally, the European Court of Justice did not include any robust treatment of the U.S. legal framework for data protection, making its standard unclear. *See id.*

113. Mark L. Krotoski et al., *Judicial Redress Act Would Extend Privacy Act Remedies to Citizens of Designated Foreign Nations*, NAT'L L. REV. (Feb. 8, 2016), http://www.natlawreview.com/article/judicial-redress-act-would-extend-privacy-act-remedies-to-citizens-designated [https://perma.cc/N9HN-EA5B] (discussing importance of Judicial Redress Act to negotiating new Privacy Shield). Under the Judicial Redress Act, a non-citizen can bring an action against a U.S. agency that: "intentionally or willfully violates the conditions for disclosing an individual's records without the individual's consent, . . . refuses an individual's request to amend his or her records, or . . . refuses to permit an individual to review" his or her records. *Id.*

114. Lisa Brownlee, *Judicial Redress Act 'National Security Interests' Amendment Could Affect US-EU Negotiations*, FORBES (Jan. 28, 2016), http://www.forbes.com/sites/lisabrownlee/2016/01/28/posted-judicial-redress-act-national-security-interests-amendment/#5723e4f0155d.

115. *See* Levi Sumagaysay, *Tech and Privacy: Judicial Redress Act, Internet Providers and User Data, ACLU Guide*, MERCURY NEWS (Feb. 11, 2016), http://www.siliconbeat.com/2016/02/11/102041 [https://perma.cc/V5N8-37AB] (outlining role of Judicial Redress Act within Privacy Shield negotiations). The senior Vice President of the Software and Information Industry Association's public policy stated, "[b]y allowing citizens of European nations and other designated U.S. allies procedural privacy protections similar to those offered to

The United States and EU have formally adopted the Privacy Shield, and companies have begun signing on.[116] While concerns linger, many hail the Privacy Shield as necessary to data transferring and trans-Atlantic commercial success.[117]

Additionally, Apple's conflicts with the Department of Justice regarding their encrypted devices demonstrate technology outpacing the development of new laws and regulations.[118] The Federal Bureau of Investigation (F.B.I.) requested that Apple develop custom software to break into an iPhone owned by one of the attackers in the San Bernardino, California mass shooting.[119] The F.B.I.'s legal argument was based on the All Writs Act, a law passed in 1789 that states judges should use "all writs necessary" to promote a case.[120] Apple refused to follow the court order requesting that it create such software, indicating that "the court order would have grave consequences for digital security and privacy"; the Department of Justice, however, believed "Apple's inability to get into its smartphones has created a system tailor-made for criminals."[121] Such a significant debate over privacy and security demonstrates how a retroactive approach to developing laws for new technologies can create

U.S. citizens in Europe, the United States can provide equal privacy rights to our allied trading partners and foster global economic progress." *Id.*

116. *See* Natalia Drozdiak, *U.S., EU Agree on Final Adjustments to Data 'Privacy Shield*,*'* WALL STREET J. (June 24, 2016), http://www.wsj.com/articles/u-s-eu-agree-final-adjustments-to-data-privacy-shield-1466764267 (outlining stakeholders' and countries' concerns). Generally, there were concerns regarding the United States engaging in bulk data collection, so the United States released a document indicating that it would only collect bulk data in limited circumstances. *Id.*; *see also* Nancy Scola, *Politico Pro Q&A: The U.S. Privacy Shield Negotiators*, POLITICO (July 15, 2016), http://www.politico.com/story/2016/07/politico-pro-q-a-the-us-privacy-shield-negotiators-225599 [https://perma.cc/G7X8-SWE5] (listing commonly asked questions regarding Privacy Shield).

117. *See* Amar Toor, *EU-US Privacy Shield Agreement Goes into Effect*, VERGE (July 12, 2016), http://www.theverge.com/2016/7/12/12158214/eu-us-privacy-shield-data-transfer-privacy [https://perma.cc/27MU-57CF] (highlighting positives and negatives of Privacy Shield); *see also* Drozdiak, *supra* note 116 (discussing concerns and questions of American public and commercial companies); Li Zhou, *U.S. Privacy Shield Negotiators Share Their Takes*, POLITICO (July 13, 2016), http://www.politico.com/tipsheets/morning-tech/2016/07/us-privacy-shield-negotiators-share-their-takes-215299 [https://perma.cc/DF89-5FHD] (detailing stakeholders' mixed reactions to Privacy Shield).

118. *See* Jim Kerstetter, *Apple, the F.B.I. and a Collection of Very Old Laws*, N.Y. TIMES (Feb. 26, 2016), http://www.nytimes.com/2016/02/27/technology/apple-the-fbi-and-a-collection-of-very-old-laws.html [https://perma.cc/JUG5-5X86] (discussing government's use of All Writs Act to receive customer information from Apple).

119. *See* Lev Grossman, *Inside Apple CEO Tim Cook's Fight with the FBI*, TIME (Mar. 17, 2016), http://time.com/4262480/tim-cook-apple-fbi/ [https://perma.cc/8PZH-9N5R] (outlining problems with accessing shooter's information on encrypted iPhone).

120. *See* 28 U.S.C. § 1651 (2012) (noting "all courts established by Act of Congress may issue all writs necessary"); *see also* Daniel Fisher, *Does a 1789 Law Really Force Apple to Write Encryption-Cracking Code Today?*, FORBES (Feb. 17, 2016), http://www.forbes.com/sites/danielfisher/2016/02/17/apple-goes-to-the-mat-over-1789-law-in-iphone-encryption-case/#6cf16ae352c2 (considering All Writs Act gap filler for judges).

121. Katie Benner & Eric Lichtblau, *Apple and Justice Dept. Trade Barbs in iPhone Privacy Case*, N.Y. TIMES (Mar. 15, 2016), http://www.nytimes.com/2016/03/16/technology/apple-court-filing-iphone-case.html (outlining strong debate over security and privacy in Congress and public).

significant issues for our society:

> This is an issue that extends far beyond Apple and the FBI. Today, we are arguing over an iPhone, and whether or not the government can compel a tech company to help it break into a device. Tomorrow's problems will be far more complex, involving science and technology the likes of which you've only ever read about in sci-fi books.[122]

III. ANALYSIS

A. The Weakness of Traditional Jurisdiction in a Cloud Computing World

The traditional notion of jurisdiction in a society that is increasingly mobile and technologically reliant is no longer a feasible option.[123] In an increasingly globalized society, the growing irrelevance of physical territory in jurisdictional considerations makes current jurisdictional practices more challenging to apply.[124] To further exacerbate the situation, judicial precedent and a circuit spilt declared sufficient contacts ambiguous and difficult to predict.[125] Circuit courts have moved toward the Calder Test, arguably making jurisdiction slightly more predictable for litigants.[126] On the other hand, strong inconsistencies remain in the Internet jurisdiction context, making it unlikely that a cohesive approach to jurisdictional dilemmas in cloud computing will

122. Amy Webb, *Apple vs. FBI Debate May Be the Least of Our Challenges*, CNN (Feb. 29, 2016), http://www.cnn.com/2016/02/25/opinions/when-technology-clashes-with-law-iphone-opinion-webb/ [https://perma.cc/5TQ5-7E74] (outlining reasons for fierce debate between Apple and F.B.I.). The debate that ignited between Apple and the F.B.I should be a wake up call to lawmakers that technology is growing and changing, and that they must play an "active role in how technology intersects with American society." *Id*.; *see also* Maura Dolan & Victoria Kim, *Apple-FBI Fight over iPhone Encryption Pits Privacy Against National Security*, L.A. TIMES (Feb. 18, 2016), http://www.latimes.com/business/la-me-fbi-apple-legal-20160219-story.html [https://perma.cc/Q75B-L3EX] (describing "unprecedented" situation where government wants Apple to create new software for security purposes); Sam Thielman & Spencer Ackerman, *Apple and FBI Look to Congress to Settle Battle over iPhone Encryption*, GUARDIAN (Feb. 29, 2016), http://www.theguardian.com/technology/2016/feb/29/apple-lawyer-fbi-bruce-sewell-more-crime [https://perma.cc/QJ67-U5PH] (describing both sides of debate urge Congress to take action).

123. *See* Breen, *supra* note 49, at 765-66 (highlighting courts' evolving jurisdictional analyses due to technological advances). The "[j]urisdictional analysis that seemed suitable for an advancing and mobile society now threatens to attain virtually limitless applications of a court[']s power over individuals who will never enter the foreign forum." Breen, *supra* note 49, at 766.

124. *See* Berman, *supra* note 49, at 325 (arguing territorial boundaries no longer constitute sufficient markers for legal jurisdictional purposes). Existing state laws governing jurisdictional practices are relics of a bygone era when geography mattered much more. *See id.* at 321.

125. *See* Spencer, *supra* note 53, at 79 (discussing "sliding scale" courts use to determine sufficient contacts); *see also* Calder v. Jones, 465 U.S. 783, 789-90 (1984) (stating plaintiffs had knowledge conduct would reach into forum); Zippo Mfg. Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119, 1124 (W.D. Pa. 1997) (discussing defendants' interactivity may establish sufficient contacts).

126. *See* Geist, *supra* note 60, at 1371-72 (explaining movement toward effects-based standard for sufficient contacts granting jurisdiction).

emerge.[127]

Courts have added ambiguity through vague decisions, making it challenging for businesses to develop strategies for technological advancement because they do not know where they could be open to litigation.[128] Such ambiguity is a significant issue for cloud computing users because the servers they use either store the data themselves or transmit it to other servers.[129] The Supreme Court's stream of commerce analysis exemplifies the lack of cohesion in an increasingly mobile society, with three different approaches explaining how defendants may purposefully avail themselves.[130] Justice O'Connor argued for sufficient contacts to be established with some activity directed toward the forum, stating that this approach is in line with the Due Process Clause.[131] Justice Brennan, however, advocated for a more lenient approach, arguing that "[t]he stream of commerce refers not to unpredictable currents or eddies, but to the regular and anticipated flow of products from manufacture to distribution to retail sale."[132] The Court established more defined rules for corporations for general jurisdiction—a corporation can be hailed to court in its principal place of business and where the corporation is incorporated.[133]

Although some circuit courts approach minimum contacts in much the same fashion as the Supreme Court, other approaches exist across the country.[134]

127. *See* Rhodes & Robertson, *supra* note 67, at 227 (discussing growth of Internet favors Calder Test expansion). The Court's conclusion in *Walden* limited courts' abilities to call a defendant to a forum in which they do not reside. *See id.* at 207-08 (listing four areas in which jurisdictional disputes will likely arise in litigation context); *see also* Citron, *supra* note 62 (arguing Supreme Court created more splintered approach to jurisdiction in *McIntyre*).

128. *See* American Broadcasting Co. v. Aereo, Inc., 134 S. Ct. 2498, 2512-14 (2014) (Scalia, J., dissenting) (arguing majority made unclear standard for when rule applies); Asahi Metal Indus. Co. v. Super. Ct. of Cal., 480 U.S. 102, 116 (1987) (summarizing majority opinion's different approaches toward stream of commerce); Dayton, *supra* note 42, at 268 (discussing discrepancies between Justices' purposeful availment and minimum contacts applications); Kaminski, *supra* note 89 (describing Supreme Court's different approaches to technological advances); *see also* Yahoo! Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme, 433 F.3d 1199, 1203, 1225 (9th Cir. 2006) (explaining French court order demanded Yahoo! remove Nazi content, yet Ninth Circuit considered order unenforceable); Lesnick v. Hollingsworth & Vose Co., 35 F.3d 939, 945-56 (4th Cir. 1994) (demonstrating usage of Justice O'Connor's stream of commerce approach in intellectual property case); Segall, *supra* note 83, at 1122 (describing valid State interest in computer location); Sheftalovich, *supra* note 96 (describing Microsoft's dilemma of protecting user data in EU).

129. *See* O'Keeffe, *supra* note 8, at 3 (discussing law's inability to keep pace with advances in cloud technology); Hoover, *supra* note 71, at 258-59 (describing various services offered by cloud); *see also* Barron, *supra* note 71 (comparing cloud services through simplified pizza metaphor).

130. *See Asahi Metal Indus. Co., Ltd.*, 480 U.S. at 110-11 (describing three different approaches in determining sufficient contacts).

131. *See id.* at 112-13 (arguing defendant unfairly subjected to jurisdiction).

132. *Id.* at 117 (Brennan, J., concurring in part and concurring in the judgment) (describing defendant's knowledge of production market sufficient availment to forum).

133. *See* Daimler AG v. Bauman, 134 S. Ct. 746, 761-62 (2014) (concluding defendant's insufficient contacts fail to make them at home in California).

134. *See* Spencer, *supra* note 53, at 73-74 (discussing different approaches courts use to determine sufficient contacts); *see also* Calder v. Jones, 465 U.S. 783, 790 (1984) (stating knowledge plaintiff had of conduct reaching into forum sufficiently established jurisdiction); Zippo Mfg. Co. v. Zippo Dot Com., Inc., 952

The Supreme Court has used the Calder Test, which looks to the intentionality of defendants' conduct to limit the forums where they can be summoned.[135] In *Walden*, the Supreme Court concluded insufficient contacts existed because "[t]he proper question is not where the plaintiff experienced a particular injury or effect but whether the defendant's conduct connects him to the forum in a *meaningful way*."[136] While the *Walden* approach may provide corporations more jurisdictional predictability, a defendant's actions can still impact a community even when that defendant has no significant connection to the forum.[137]

B. The Promise of the Privacy Shield

International cooperation may be the catalyst that creates a more stable and secure climate for cloud computing.[138] The services the cloud offers transcend international borders to the point that borders no longer exist.[139] Cloud services for Amazon alone generate a total of $1 billion in revenue, and the value of the digital economy is estimated to reach $4.8 trillion by 2025.[140] With companies of all sizes relying more on cloud services, roadblocks such as security, privacy, and governance, need to be eliminated to allow companies to take full advantage of cloud capabilities.[141] Furthermore, individuals and companies that leverage cloud services lose control of their data, creating a strong need for clear regulations and more transparency.[142]

The new Privacy Shield has the potential to be the facilitator that establishes more stability for companies and individuals leveraging cloud-computing

F. Supp. 1119, 1124 (W.D. Pa. 1997) (discussing defendant's activity directed toward forum could establish contacts).

135. *See* Walden v. Fiore, 134 S. Ct. 1115, 1125-26 (2014) (determining defendant's conduct did not sufficiently reach into plaintiffs' forum based on Calder Test); *Calder*, 465 U.S. at 790 (stating defendant knowingly inflicted injury in plaintiffs' forum).

136. *Walden*, 134 S. Ct. at 1125 (emphasis added) (establishing insufficiency of mere injury to plaintiffs in their home forums to create sufficient contacts).

137. *See* Berman, *supra* note 49, at 319 (arguing non-local actions impact local communities).

138. *See* Sony et al., *supra* note 79 (highlighting importance of international cooperation; Shear, *supra* note 108 (discussing companies receiving transparency and accountability from Agreement).

139. *See* Darrow, *supra* note 110 (describing companies opening new transnational services and data centers during Agreement's collapse); Shear, *supra* note 108 (arguing for modernized Agreement to provide direction to companies conducting business internationally).

140. *See* Hardy, *supra* note 1 (describing cloud businesses seeking Amazon's business given its global expansion with cloud computing); Shear, *supra* note 108 (describing cloud's impact on Amazon's business model and need for stronger protections for digital economies).

141. *See* EXPLORING THE FUTURE OF CLOUD COMPUTING, *supra* note 74, at 9, 11 (discussing global concerns of privacy, security, and governance of cloud computing). Users' data security can be a significant issue in users' ability to trust their data in the cloud. *See* King & Raja, *supra* note 72, at 418-19 (highlighting benefits cloud provides companies, but keeping security top priority).

142. *See* EXPLORING THE FUTURE OF CLOUD COMPUTING, *supra* note 74, at 11 (describing providers' concerns for outdated laws and lack of governance for cloud computing).

benefits.[143] The Privacy Shield's predecessor, the Agreement, was ineffective in initiating long-term solutions between the United States and the EU.[144] The importance of the Agreement's benefit to United States companies, however, cannot be undermined: 4,500 companies transferred data between the EU and the United States as a result.[145] Additionally, the absence of such an agreement between the United States and EU could cost companies billions of dollars, and even cause a trade war.[146] A syncretic approach is challenging, however, given that the EU relies heavily on comprehensive regulations while the United States emphasizes a combination of self-regulation and legislation.[147]

Proponents of the new Privacy Shield are optimistic that it will increase compliance due to its more rigorous repercussions and harsh disciplinary actions.[148] Furthermore, the Department of Commerce stated that oversight from all three branches of government would create more safeguards for privacy.[149] Arguably, the United States took an affirmative step toward giving the Privacy Shield the command that EU stakeholders requested when it passed the Judicial Redress Act.[150] Nevertheless, there was a last-minute amendment, which included broad language for national security interests.[151]

Given the lack of consistency on jurisdictional issues related to technology already within U.S. courts, the Judicial Redress Act may create problems rather than solve them.[152] On the other hand, the Judicial Redress Act provides

143. *See* Metzger, *supra* note 105 (discussing Privacy Shield's more rigorous provisions than Agreement's); Shear, *supra* note 108 (stating Agreement can provide guidance to companies conducting international business); *see also* Alo, *supra* note 108, at 1110 (highlighting billions of dollars in trade loss); Jackson, *supra* note 111 (discussing Privacy Shield's commitment to transparency of accessing data).

144. *See* Darrow, *supra* note 110 (discussing companies taking advantage of collapse of Agreement's); *see also EU-US Privacy Shield*, *supra* note 112 (outlining new terms of Privacy Shield adding more levels of accountability and enhanced protections). *But see* Hoffman, *supra* note 112 (discussing how countries outside of EU using data from EU must have comparable data protections). The EU Court of Justice made an unclear standard for data protections in outside companies. *See* Hoffman, *supra* note 112.

145. *See* Alo, *supra* note 108, at 1111 (discussing "adequate level of protection" for EU); Drozdiak & Schechner, *supra* note 97 (discussing access granted by Safe Harbor Agreement to U.S. companies).

146. Alo, *supra* note 108, at 110 (describing significant losses to U.S. trade if EU privacy laws ignored).

147. *See* Schriver, *supra* note 105, at 2778-79 (explaining EU citizens consider privacy rights fundamental); *see also U.S.-EU Safe Harbor Overview*, *supra* note 105 (outlining EU's and United States's various approaches to data privacy). Furthermore, U.S. corporations "do not see privacy as a normal cost of doing business." Schriver, *supra* note 105, at 2779.

148. *See* Metzger, *supra* note 105 (explaining Privacy Shield incorporates harsher disciplinary actions against non-compliers than Agreement); *EU-US Privacy Shield*, *supra* note 112 (outlining new transparency and oversight provisions to Privacy Shield).

149. *See EU-US Privacy Shield*, *supra* note 112 (explaining multi-level government involvement in providing protections from potential infringers).

150. *See* Krotoski et al., *supra* note 113 (outlining importance of Judicial Redress Act for Privacy Shield negotiations); Sumagaysay, *supra* note 115 (describing importance of Judicial Redress Act to Privacy Shield negotiations and for fostering economic progress).

151. *See* Brownlee, *supra* note 114 (outlining national security reasons for new amendment by U.S. Senate).

152. *See* Breen, *supra* note 49, at 765-66 (outlining changing standards for new technologies).

clearer remedies for EU citizens that strengthen the Privacy Shield and define regulations for U.S.-based companies that transfer data to the EU through cloud computing services.[153] When the law pertaining to technological advances is too ambiguous, it creates high-stakes controversies for governments, corporations, and individuals, who are left with a plethora of interpretations and uncertainties.[154]

There is no clearer demonstration of disjointed technology laws' consequences than the debate between Apple and the Department of Justice.[155] Individual privacy and national security are significant issues that should not be decided according to ambiguous laws or with minimal congressional guidance.[156] The All Writs Act should not be used to supplement a twenty-first century law that is rapidly changing.[157] Moreover, this dispute demonstrates the consequences that result from a reactive approach, rather than bringing together all stakeholders to create substantive and long-lasting laws and regulations.[158]

IV. CONCLUSION

Technology will continue to be an extremely fast-growing sector of our society. It will enable companies and individuals to reach heights that they would have never thought possible. But with that innovation comes a great responsibility for our lawmakers, our technology industry leaders—and even us.

It is important that lawmakers are not the only ones taking the helm in legal innovations for technology. Industry leaders, from key stakeholders like Google to smaller start-up companies that leverage cloud services to expand their markets, need to play a significant role in the conversation. They are the ones who understand how the technology works and where the technology is headed. Without them, lawmakers would be shooting in the dark, and their policies may have serious unintended consequences, like hindering competition

153. *See* Sumagaysay, *supra* note 115 (recognizing United States's opportunity to provide equal privacy rights to allies through Judicial Redress Act); *see also* Krotoski et al., *supra* note 113 (discussing Judicial Redress Act addresses EU Court of Justice's concerns).

154. *See* Breen, *supra* note 49, at 766 (outlining problems facing personal jurisdictional with growth in technology, including varying court interpretations); Trammell & Bambauer, *supra* note 25, at 1130 (stating many courts do not understand how to deal with new technology).

155. *See* Benner & Lichtblau, *supra* note 121 (explaining Department of Justice's viewpoint on Apple's "above the law" status); Kerstetter, *supra* note 118 (discussing battle between technology companies and Department of Justice).

156. *See* Fisher, *supra* note 120 (stating "government is pushing the limits of its authority under the All Writs Act"); Webb, *supra* note 122 (stating society should not wait for court decision to decide technology's future).

157. *See* Webb, *supra* note 122 (arguing discussion around new technology laws must happen before problems arise).

158. *See id*. (arguing congressional lack in technology lawmaking leads to dispute).

or stifling innovation. Jurisdiction plays a substantial role in legal predictably for corporations because they must understand where they can be hailed to court, and individuals must be able to bring suits against parties who leverage technology to harm them. A lack of clear jurisdictional guidance creates a system where those engaged in any technology can skirt the justice system through procedural technicalities.

The Privacy Shield is an example of how international cooperation can foster an environment for well-defined laws that allow corporations to participate in the international market. While the Privacy Shield is not foolproof, the Judicial Redress Act, which was a precursor to Privacy Shield negotiations, provides some jurisdictional guidance for international parties. When international actors negotiate the policy and legal implications of technological advances, like the cloud, businesses and individuals will benefit.

On the other hand, the recent dispute between Apple and the Department of Justice exemplifies how a lack of lucidity in policy and the law can create significant turmoil. Leveraging the All Writs Act from the 1700s is not a solution for twenty-first century technology problems. The debate is also a strong indicator that there are deep gaps in the laws that are used when technological issues arise. Cloud computing and technology are reshaping our society, and we need a progressive, rather than retroactive, approach to jurisdiction.

Elma Delic