PERSONAL JURISDICTION IN THE DATA AGE: *MACDERMID V. DEITER*'S ADAPTATION OF *INTERNATIONAL SHOE* AMIDST SUPREME COURT UNCERTAINTY

Ryan Almy

PERSONAL JURISDICTION IN THE DATA AGE: *MACDERMID V. DEITER*'S ADAPTATION OF *INTERNATIONAL SHOE* AMIDST SUPREME COURT UNCERTAINTY

Ryan Almy[*]

In *MacDermid, Inc. v. Deiter*,[1] the Second Circuit held that a Connecticut court may exercise personal jurisdiction over a defendant who allegedly used a computer in Canada to remotely access a computer server located in Connecticut in order to misappropriate proprietary, confidential electronic information belonging to a Connecticut corporation.[2] This Note argues that, given the factual elements before the court, *MacDermid* was an unsurprising, orthodox, and proper holding in the context of personal jurisdiction jurisprudence.[3] However, the facts in *MacDermid*, and the corresponding limits inherent in the Second Circuit's holding, reveal potentially gaping holes in our modern personal jurisdiction framework and its ability to respond to the realities of modern commerce and technology.

This Note first analyzes the *MacDermid* opinion and, after briefly summarizing the history of jurisdictional jurisprudence, argues that the Second Circuit's holding is an example of a court's appropriate adaptation of the traditional personal jurisdiction framework to the data age. Next, this Note presents factual scenarios beyond those present in *MacDermid* and explores potential responses to these issues under both the modern United States Supreme Court approach and the Second Circuit's *MacDermid* analysis. This Note will conclude by arguing that, while the *MacDermid* approach exemplifies the proper exercise of a state court's jurisdiction over a defendant whose only contact with the forum state is technological in nature, the Supreme Court's recent foot-dragging leaves domestic electronic data protection in a potentially dangerous limbo.

I. *MACDERMID*

MacDermid, Inc., ("MacDermid") is a "chemical company with its principal place of business in Waterbury, Connecticut."[4] It maintains computer servers that are physically located in Waterbury and on which MacDermid stores sensitive proprietary information.[5] Employees of MacDermid and its subsidiaries agree, as a condition of employment, to safeguard and properly use such information, which

* J.D. Candidate, 2014, University of Maine School of Law. For their respective integral contributions to this Note, the Author would like to extend his sincerest gratitude to Professors Martin Rogoff, Gerald Petruccelli, Melvyn Zarr, and Andrew Clearwater. The Author would also like to thank the editors and staff of the *Maine Law Review*.

1. 702 F.3d 725 (2d Cir. 2012).

2. *Id.*

3. *See, e.g.*, Asahi Metal Indus. Co. v. Superior Court, 480 U.S. 102 (1987); Burger King Corp. v. Rudzewicz, 471 U.S. 462 (1985); Calder v. Jones, 465 U.S. 783 (1984); World-Wide Volkswagen Corp. v. Woodson, 444 U.S. 286 (1980); Int'l Shoe Co. v. Wash., 326 U.S. 310 (1945).

4. *MacDermid*, 702 F.3d at 727.

5. *Id.*

includes an agreement by the employee to refrain from transferring such information to a personal email account.[6] Employees may access this information only by accessing the Waterbury servers.[7] Likewise, MacDermid's email system is housed by the Waterbury servers.[8] Furthermore, by the terms of MacDermid's employment contract, employees are privy to the storage and maintenance of the company email system and proprietary information in Waterbury, Connecticut.[9]

Jackie Deiter is a Canadian citizen who lives in Fort Eerie, Ontario, Canada.[10] Between May 2008 and April 2011 she worked, in Canada, as an account manager for MacDermid's Canadian subsidiary, MacDermid Chemicals, Inc.[11] As an account manager, her responsibilities included managing customer accounts, obtaining new customers, and providing customer technical support.[12] Deiter has never been to Connecticut.[13]

For reasons irrelevant to the analysis, MacDermid had opted to terminate Deiter's employment, effective April 2011.[14] Aware of her impending termination, Deiter used her work computer to send MacDermid's allegedly confidential and proprietary data from her MacDermid employee email account to her personal email account for use on her personal computer.[15]

MacDermid then brought suit against Deiter in the United States District Court for the District of Connecticut, alleging unauthorized access and misuse of a computer system and misappropriation of trade secrets in violation of Connecticut's computer crimes and trade regulations statutes.[16] The District Court's jurisdiction[17] was based on diversity of citizenship and Connecticut's long-arm statute.[18] Deiter subsequently moved to dismiss the action for lack of personal

---

6. *Id.*

7. *Id.*

8. *Id.*

9. *Id.*

10. *Id.*

11. *Id.*

12. MacDermid, Inc. v. Deiter, No. 3:11-CV-00855-WWE, 2011 WL 6001625, at *1 (D. Conn. Nov. 30, 2011).

13. *Id.*

14. *MacDermid*, 702 F.3d at 727.

15. *Id.* Deiter admits sending the data to her personal email, but maintains she did so only because her work computer did not enable her to print documents, which she needed to do in preparation for a work-related presentation. *MacDermid*, 2011 WL 6001625, at *1.

16. *MacDermid*, 702 F.3d at 727.

17. *Id.*

18. *Id; see also* CONN. GEN. STAT. § 52–59b(a) (2005) ("[A] court may exercise personal jurisdiction over any nonresident individual . . . who in person or through an agent: (1) Transacts any business within the state; (2) commits a tortious act within the state, except as to a cause of action for defamation of character arising from the act; (3) commits a tortious act outside the state causing injury to person or property within the state, except as to a cause of action for defamation of character arising from the act, if such person or agent (A) regularly does or solicits business, or engages in any other persistent course of conduct, or derives substantial revenue from goods used or consumed or services rendered, in the state, or (B) expects or should reasonably expect the act to have consequences in the state and derives substantial revenue from interstate or international commerce; (4) owns, uses or possesses any real property situated within the state; or (5) uses a computer, as defined in subdivision (1) of subsection (a) of section 53-451, or a computer network, as defined in subdivision (3) of subsection (a) of said section, located within the state.").

jurisdiction pursuant to Fed. R. Civ. Pro. 12(b)(2).[19] The District Court granted her motion to dismiss, concluding that the long-arm statute did not reach Deiter's alleged conduct.[20] In so finding, the District Court relied on the view that Deiter had not accessed a Connecticut computer, but had merely sent an email "from one computer in Canada to another computer in Canada."[21] Thus, according to the District Court, Deiter's literal conduct was not within reach of Connecticut's long-arm provision[22] that establishes personal jurisdiction over a non-resident defendant who uses a computer, as defined by the state computer crime statute,[23] within the state.[24]

On appeal, the Second Circuit reversed. Applying the traditional two-step jurisdictional analysis, the Circuit Court found that the Connecticut long-arm statute did in fact confer jurisdiction, and that the state court's exercise of personal jurisdiction over Deiter was consistent with due process.[25]

While the District Court had reasoned that Deiter had not used a Connecticut computer, but rather had used a Canadian computer to send information to her personal Canadian email account, the Second Circuit pointed to the fact that "[i]n order to use [her] MacDermid e-mail account and to obtain said confidential data files, Ms. Deiter accessed computer servers located in MacDermid's offices in Waterbury, Connecticut."[26] Furthermore, the court held that a "computer server" is included within the Connecticut long-arm statute's incorporated definition of a "computer" because it is:

> An electronic . . . device . . . that, pursuant to . . . human instruction . . . can automatically perform computer operations with . . . computer data and can communicate the results to another computer or to a person [or is a] connected or directly related device . . . that enables the computer to store, retrieve or communicate . . . computer data . . . to or from a person, another computer or another device.[27]

Thus, the court found that, by accessing MacDermid's server, Deiter had "used a computer in Connecticut" for the purposes of the state long-arm statute, despite

---

19. *MacDermid*, 702 F.3d at 727.

20. *Id.*

21. *Id.* at 728 (internal quotation marks omitted).

22. *Id.*; s*ee also* CONN. GEN. STAT. § 52–59b(a)(5).

23. CONN. GEN. STAT. § 53-451(a)(1) (2012) ("'Computer' means an electronic, magnetic or optical device or group of devices that, pursuant to a computer program, human instruction or permanent instructions contained in the device or group of devices, can automatically perform computer operations with or on computer data and can communicate the results to another computer or to a person. 'Computer' includes any connected or directly related device, equipment or facility that enables the computer to store, retrieve or communicate computer programs, computer data or the results of computer operations to or from a person, another computer or another device.").

24. MacDermid, Inc. v. Deiter, No. 3:11-CV-00855-WWE, 2011 WL 6001625, at *3 (D. Conn. Nov. 30, 2011) ("That the information was originally obtained over the internet from a network of computers in Connecticut does not mean that the defendant used a computer network located within the state, as defined in [the computer crimes statute] . . .").

25. MacDermid, Inc. v. Deiter, 702 F.3d 727 (2d Cir. 2012).

26. *Id.* at 728 (internal quotations omitted).

27. *Id.* at 728-29.

the fact that the "use" was remote.[28] The court found this statutory interpretation reinforced by the fact that this particular long-arm provision was enacted as part of a broader statutory scheme aimed at combating unauthorized interference with computer programs or electronic data.[29] The integration of this provision must have been intended to reach precisely these instances of remote access that would not otherwise be within the scope of the long-arm statute, the court reasoned.[30]

Having found the Connecticut court's jurisdiction over Deiter proper under the state long-arm statute, the Circuit Court turned its attention to the second step in personal jurisdiction analysis: whether such exercise of jurisdiction is within the bounds of due process.[31]

Citing *International Shoe*,[32] the court first examined whether sufficient minimum contacts existed between Deiter and the state of Connecticut such that "maintenance of the suit [would] not offend traditional notions of fair play and substantial justice."[33] Stemming from the fact that MacDermid had specifically alleged that "Deiter knew that the email servers she used and the confidential files she misappropriated were both located in Connecticut," the court reasoned that Deiter had purposefully availed herself of the "privilege of conducting computer activities" within Connecticut's borders.[34] While noting that this may not be the case for the average internet user, the court found that, by the terms of her employment contract, Deiter specifically knew "of the centralization and housing of [MacDermid's] email system and the storage of [MacDermid's information] in Waterbury, Connecticut" such that she invoked the benefits and protections of Connecticut state law when she used her MacDermid email to transfer MacDermid information.[35] Additionally, the court invoked *Calder*[36] and found that Deiter had at least directed allegedly tortious conduct toward a Connecticut corporation.[37]

The Second Circuit next considered whether the exercise of personal jurisdiction in this instance would be reasonable.[38] In light of the factors set forth in *Asahi*,[39] the court found Connecticut's exercise of personal jurisdiction over Deiter

---

28. *Id.* at 729 ("It is not material that Deiter was outside of Connecticut when she accessed the Waterbury servers. The statute requires only that the computer or network, not the user, be located in Connecticut. The statute reaches persons outside the state who remotely access computers within the state . . . ").

29. *Id.*

30. *Id.* ("Extending the statute to reach a nonresident who committed any of the above activities while present in Connecticut would not have been necessary because that person would already have been subject to jurisdiction under § 52-59b(a)(2). Further, it cannot be said that Deiter's conduct is covered by § 52-59b(a)(3) because she is not alleged to have regularly conducted business in Connecticut, or to have derived revenue from her conduct.").

31. *Id.*

32. Int'l Shoe Co. v. Wash., 326 U.S. 310, 316 (1945).

33. *MacDermid*, 702 F.3d at 730 (internal quotation marks omitted).

34. *Id.*

35. *Id.* (internal quotation marks omitted).

36. Calder v. Jones, 465 U.S. 790 (1984) (Finding the proper exercise of personal jurisdiction in California when a Floridian defendant had directed defamatory conduct toward a California resident).

37. *MacDermid*, 702 F.3d at 730.

38. *Id.*

39. Asahi Metal Indus. Co. v. Superior Court, 480 U.S. 102, 113-14 (1987). *See also MacDermid*, 702 F.3d at 730 ("A court must consider [1] the burden on the defendant, [2] the interests of the forum

to be within the bounds of due process reasonableness.[40] Specifically, the court found that both the state of Connecticut and MacDermid had significant interests in resolving this dispute in Connecticut—MacDermid being a Connecticut corporation and the state having an interest in the proper interpretation of its laws.[41] The court also emphasized the sound public policy of establishing identity between the forum state and the state from which electronic data has been misappropriated.[42] Finally, and ironically, the court cited the conveniences of modern technology as sufficient abatement of any burden placed upon Deiter in having to defend her actions in Connecticut.[43]

In conclusion, the Second Circuit held that the Connecticut District Court's exercise of personal jurisdiction in this matter was both proper with respect to the state long-arm statute and consistent with the constitutional fairness and reasonableness afforded a non-resident defendant.[44]

II. *PENNOYER* TO *MCINTYRE*: 135 YEARS OF PERSONAL JURISDICTION JURISPRUDENCE

Placing *MacDermid* within the context of the prevailing personal jurisdiction framework will require a brief digression to explore the history of jurisdictional jurisprudence.

Pennoyer v. Neff[45] set the framework for modern personal jurisdiction doctrine with an emphasis on the limited power of sovereign states to reach defendants outside of their borders.[46] Here, Justice Field invoked principles of international law to define the scope of the state's sovereign authority.[47] Thus, while the *Pennoyer* personal jurisdiction inquiry centers on the scope of the state's sovereign authority over non-consenting, non-resident defendants, the defendants' Fourteenth Amendment rights also lurk within the opinion.[48] Concerned that the Full Faith and Credit Clause may not adequately protect against the intrastate enforcement of a judgment that is void as violative of sovereignty principles, Justice Field pointed to the Due Process Clause as a defendant's shield against jurisdiction-less judgments.[49] In sum, *Pennoyer* established the scope of state power as the appropriate starting point for answering questions of jurisdictional reach, and drew upon due process as a basis for resisting in-state judgments in excess of the state's authority.[50]

State, and [3] the plaintiff's interest in obtaining relief. It must also weigh in its determination [4] the interstate judicial system's interest in obtaining the most efficient resolution of controversies; and [5] the shared interest of the several States in furthering fundamental substantive social policies.").

40. *MacDermid*, 702 F.3d at 731.

41. *Id.*

42. *Id.*

43. *Id.*

44. *Id.* at 727.

45. 95 U.S. 714 (1877).

46. *Id.* at 722.

47. *Id.* at 729.

48. *Id.* at 733.

49. *Id.*

50. Wendy Collins Perdue, *What's "Sovereignty" Got to Do with It? Due Process, Personal Jurisdiction, and the Supreme* Court, 63 S.C. L. REV. 729, 732 (2012).

In 1945, however, *International Shoe v. Washington*[51] established due process as the constitutional norm by which the legitimacy of personal jurisdiction was to be measured.[52] It was here that the Supreme Court constructed a constitutional framework for modern jurisdictional jurisprudence that, for most, would be a touchstone[53] for the next century:

> [D]ue process requires only that in order to subject a defendant to a judgment *in personam*, if he be not present within the territory of the forum, he have certain minimum contacts with it such that the maintenance of the suit does not offend "traditional notions of fair play and substantial justice."[54]

Thus, now it was due process itself that provided the criterion for determining the legitimacy of a particular state's assertion of judicial power over a non-resident defendant.

As a threshold matter, there must be sufficient minimum contacts established between the non-resident defendant and the forum state.[55] Without such relation or ties, an exercise of jurisdictional authority by the state would offend the defendant's constitutionally guaranteed right to due process.[56] Accordingly, *International Shoe* established an unambiguous shift in personal jurisdiction analysis from state-centric to defendant-centric.

Subsequent case law endeavored to further define just how much process is due a foreign defendant in the context of personal jurisdiction by developing the test alluded to in *International Shoe* and demanded by the Fourteenth Amendment.[57] Out of these refinements arose new verbal formulations that are standard fixtures in modern jurisdictional jurisprudence: a requirement that there be "some act by which the defendant purposefully avails itself of the privilege of conducting activities within the forum [s]tate,"[58] including circumstances where tortious activity is directed at or has an effect within the forum state,[59] and a requirement that the claim arise out of or relate to forum-based activities.[60] Additionally, courts will consider a number of factors to determine whether the exercise of personal jurisdiction would be "reasonable" in light of competing interests, potential burdens, and public policy.[61] These reasonableness factors include:

---

51. 326 U.S. 310 (1945).

52. *See* Perdue, *supra* note 50, at 733 ("Under the *Pennoyer* approach, the due process violation consisted of enforcing a judgment rendered by a court that lacked legitimate authority, but the standards for determining legitimacy were derived separately from that clause. In contrast, *International Shoe* suggests that the Due Process Clause itself embodies certain criteria for legitimacy.")

53. Burger King Corp. v. Rudzewicz, 471 U.S. 462, 474 (1985).

54. *Int'l Shoe*, 326 U.S. at 316.

55. *Id*. at 319.

56. *Id*.

57. *See, e.g.,* Asahi Metal Indus. Co. v. Superior Court, 480 U.S. 102 (1987); Burger King Corp. v. Rudzewicz, 471 U.S. 462 (1985); Calder v. Jones, 465 U.S. 783 (1984); World-Wide Volkswagen Corp. v. Woodson, 444 U.S. 286 (1980); Hanson v. Denckla, 357 U.S. 235 (1958).

58. *Id.* at 253.

59. *See Burger King*, 471 U.S. at 475; *Calder*, 465 U.S. at 789.

60. *Burger King*, 471 U.S. at 472.

61. *See also id.* at 477; *World-Wide Volkswagen*, 444 U.S. at 292.

> [1] [T]he burden on the defendant, [2] the interests of the forum State . . . [3] the plaintiff's interest in obtaining relief . . . [4] the interstate judicial system's interest in obtaining the most efficient resolution of controversies; and [5] the shared interest of the several States in furthering fundamental substantive social policies.[62]

Thus, the trajectory of modern jurisdictional jurisprudence has had its origins not in *Pennoyer*, but in *International Shoe* and its defendant-driven approach.[63] Despite the Court's repeated implicit repudiation of the rationale set forth in *Pennoyer*, the state sovereignty theme has laid dormant in personal jurisdiction jurisprudence, occasionally erupting in tumultuous concurrences or dissents and injecting uncertainty into the jurisdictional landscape, much to the chagrin of Civil Procedure students everywhere.[64]

The most recent recurrence of the state sovereignty-centric analysis was confounding indeed. In 2011, *J. McIntyre Machinery Ltd. v. Nicastro*,[65] a plurality opinion by Justice Kennedy, invoked 1878's *Pennoyer* and appeared to place federalism at the heart of a personal jurisdiction analysis involving modern commerce.[66] However, unlike *Pennoyer*, and despite the plurality's emphasis on state sovereignty as the proper starting point for determining the state's jurisdictional reach, the opinion seems to define the scope of state authority not by principles of international law, but rather in reference to the defendant's actions.[67] Justice Kennedy explains, "it is the defendant's actions . . . that empower a State's courts to subject him to judgment"[68] – specifically, whether such actions "manifest an intention to submit to the power of a sovereign."[69] Thus, the *McIntyre* plurality's effective holding can be surmised as: a state court may not properly exercise jurisdiction over a defendant *unless* that defendant has purposefully availed itself of doing business in the forum state or placed goods in the stream of commerce with

---

62. *Asahi*, 480 U.S. at 113.

63. Indeed, in 1982's *Insurance Corp. of Ireland*, the Court explicitly recognized the reality of modern personal jurisdiction doctrine and its defendant-centric approach. Ins. Corp. of Ir. v. Compagnie des Bauxites de Guinee, 456 U.S. 694, 702 (1982). The Court specifically confronted the tug-of-war between federalism and individual liberty in personal jurisdiction precedent, ultimately siding with due process as the proper standard:

> The restriction on state sovereign power . . . must be seen as ultimately a function of the individual liberty interest preserved by the Due Process Clause. That Clause is the only source of the personal jurisdiction requirement, and the Clause itself makes no mention of federalism concerns. Furthermore, if the federalism concept operated as an independent restriction on the sovereign power of the court, it would not be possible to waive the personal jurisdiction requirement: individual actions cannot change the powers of sovereignty, although the individual can subject himself to powers from which he may otherwise be protected.

Id. at 703 n.10.

64. *Cf.* Perdue, *supra* note 50, at 734-40 (discussing the majority opinions in favor of a due process-centric analysis, the dissenting, concurring and sometimes majority opinions emphasizing due process, and the resulting confusion).

65. McIntyre Machinery Ltd. v. Nicastro, 131 S. Ct. 2780 (2011).

66. *Id.* at 2785-89.

67. Perdue, *supra* note 50, at 742-43.

68. *McIntyre*, 131 S. Ct. at 2789.

69. *Id*. at 2788.

the expectation they would be purchased in the forum state.[70] In this case, the plurality found that the foreign business had not purposefully availed itself of the privilege of conducting business in any U.S. state in particular by targeting the U.S. market in general.[71]

Dissenting, Justice Ginsburg replied: "the constitutional limits on a state court's adjudicatory authority derive from considerations of due process, not state sovereignty."[72] Thus, true to the trajectory set forth in 1945, Justice Ginsburg set out to reaffirm that the proper personal jurisdiction inquiry is grounded in considerations of due process, fairness and individual rights.[73] Despite her apparent reassertion of *International Shoe* fundamental fairness canons, however, Justice Ginsburg's rationale did not mirror the defendant-centric approach of *International Shoe*'s progeny.[74] Rather, Justice Ginsburg's analysis asked to what extent states are reasonably empowered to provide redress for injuries occurring within their borders, particularly in the broad context of modern commerce.[75] Accordingly, Justice Ginsburg concluded: "it would undermine principles of fundamental fairness to insulate the foreign manufacturer from accountability in court at the place within the United States where the manufacturer's product caused injury."[76]

Though it may seem that these discrepant jurisdictional formulations are really only getting at the same idea by way of varying terms of art, the point from which a justice begins his or her analysis can affect the ultimate terminus of the litigation—a prime example being the plurality's declining to find jurisdiction in *McIntyre* as opposed to the result the dissent would have returned. The plurality focused on state sovereignty but defined it by way of individual liberty, resulting in a limited view of a state's sovereign authority.[77] The dissent, on the other hand, emphasized the individual's due process rights, but framed the question as one of the "sensible . . . allocation of adjudicatory authority."[78]

The most significant takeaway from *McIntyre*, then, is that personal jurisdiction jurisprudence is on shaky doctrinal ground while the realities of modern commerce and the increasing prevalence of remote data storage and access are creating a fertile environment for novel questions of sovereignty, purposeful availment, and fairness.

III. WHERE DOES *MACDERMID* FIT?

From a civil procedure standpoint, *MacDermid* is an orthodox, coherent, and transparent application of long-standing personal jurisdiction principles.

---

70. *See id.* at 2785.
71. *Id*. at 2790-91.
72. *Id.* at 2798.
73. *Id*. at 2798-2800.
74. Perdue, *supra* note 50, at 742-43.
75. *Id*. at 743.
76. *McIntyre*, 131 S. Ct. at 2801-02.
77. *Id.* at 742.
78. *Id*.

A. Statutory Interpretation: Just How Long is the Arm?

As a threshold matter, the Second Circuit properly found Deiter's conduct to be within the scope of Connecticut's long-arm statute. In so finding, the court showcased adaptability to the realities of modern computing both in its statutory construction analysis and its understanding of what is meant by "use" of a computer. This is best understood in contrast to the narrower position put forward by the district court.

In declining to extend the long-arm statute to the conduct in question, the lower court focused on the fact that the physical "use" was exclusively in Canada; that is, the use of the internet between two computers in Canada.[79] It found significance in the fact that the express statutory language makes no reference to use of the internet, but rather exclusively addresses the physical use of computers or computer networks within the state.[80] Therefore, for the lower court, that Deiter had used the internet to originally obtain information from a Connecticut server was insufficient to confer jurisdiction because she had not "used" a computer or a computer network within the state.[81] Furthermore, the district court placed significance on the fact that Deiter's initial server access was authorized because she was, at the time, a MacDermid employee and was using her MacDermid computer.[82] Again, it was only the subsequent transfer of the gathered information, which took place exclusively in Canada, that constituted the alleged tort.[83]

But, as the Second Circuit opinion points out, the in-state physical actions seen by the district court as the only actions reached by the "use of an in-state computer" provision would already be reached by § 52-59b(a)(2), the provision addressing "torts committed outside of the state that cause injury within the state."[84] Therefore, the addition of § 52-59b(a)(5) and its cross reference to the state computer crimes statute would be redundant and ineffective in reaching any additional conduct if circuit courts were to adopt the lower court's narrow approach. Furthermore, to find that a computer server is not a computer for the purposes of the cyber crime and long-arm statute would be to acknowledge the necessity of protecting electronic data while refusing to extend that protection to the actual devices on which such data is stored. Such an interpretation would ignore the realities of modern computing, where a dizzying mass of data is stockpiled in server rooms across the globe, and individuals can access, alter, or destroy that data via computing devices.[85] In short, extending the jurisdictional reach anticipated by the Connecticut long-arm statute only as far as the physical use of a typical computing device within the state would frustrate the purpose of both the long-arm statute and

79. MacDermid, Inc. v. Deiter, No. 3:11-CV-00855-WWE, 2011 WL 6001625, at *3 (D. Conn., Nov. 30, 2011).

80. *Id*. ("If the legislature had meant internet instead of computer network it would have said so." (internal quotation marks omitted)).

81. *Id*.

82. *Id*. at *4.

83. *Id*.

84. MacDermid, Inc. v. Deiter, 702 F.3d 725, 729 (2d. Cir 2012).

85. JONATHAN I. EZOR, PRIVACY AND DATA PROTECTION IN BUSINESS: LAWS AND PRACTICES 259-62 (2012).

the broader computer crimes statute: combating injurious remote access.[86]

Likewise, the district court's emphasis on the initial access being technically authorized fails to account for the mechanics of modern technology. Because MacDermid's email system is stored on the Waterbury servers, the very act of reading or sending an email necessarily involves accessing those servers.[87] In fact, every time Deiter viewed, changed, or deleted MacDermid customer accounts or other company information, the properties of a Waterbury server changed ever so slightly.[88] Taking these mechanisms into account, the district court's distinction here—where, so long as the initial access is lawful, any subsequent remote misuse is beyond the reach of the forum law—makes little sense.[89] Again, taking such a narrow view of "access" would acknowledge that certain electronic data deserves the protection of law, but fail to adequately protect the very substance of that data.

Accordingly, the Second Circuit's determination that Deiter had used a computer located within the state of Connecticut gives effect to the state's intent to protect electronic property harbored within its borders, and also exemplifies a cognizance of modern technology. The Second Circuit's job was not done yet, however, as it proceeded to apply constitutional principles of personal jurisdiction as set forth by Supreme Court precedent. Thus, the circuit court conducted a defendant-centric due process review.[90]

B. Due Process Analysis

First, the court found sufficient minimum contacts established by Deiter's actions.[91] Relying on MacDermid's allegation that Deiter had expressly acknowledged the physical whereabouts of MacDermid data systems in her employment contract, the court comfortably found that Deiter had purposefully availed herself of conducting computing activities in Connecticut.[92] Thus, the court took advantage of the rare opportunity presented by an express, memorialized knowledge of the location of electronic data. Deiter's transfer of MacDermid data and use of MacDermid's email system after explicitly recognizing the effect such behavior would have in Connecticut presents as clear an example of purposeful availment as a court can expect.

Due Process precedent requires more than minimum contacts, as we know.

---

86. *See, e.g.*, U.S. v. Ivanov, 175 F. Supp. 2d 367, 371 (D. Conn. Dec. 6, 2001) ("The fact that the computers were accessed by means of a complex process initiated and controlled from a remote location does not alter the fact that the accessing of the computers, i.e. part of the detrimental effect prohibited by the statute, occurred at the place where the computers were physically located, namely OIB's place of business in Vernon, Connecticut.").

87. *See* Marshall Brain, *How Web Servers Work*, HOWSTUFFWORKS, http://www.howstuffworks.com/web-server.htm (last visited Nov. 8, 2013).

88. *See id.*

89. *Ivanov*, 175 F. Supp. 2d at 372 ("The fact that [the defendant obtained the victim's] valuable data by means of a complex process initiated and controlled from a remote location, and that he subsequently moved that data to a computer located in Russia, does not alter the fact that at the point when [the defendant] first possessed that data, it was on [the victim's] computers in Vernon, Connecticut.").

90. *See* MacDermid v. Deiter, 702 F.3d 725, 729-31 (D. Conn., Nov. 30, 2011).

91. *Id*. at 730.

92. *Id*.

Accordingly, the court conducted a standard reasonableness review.[93] Here, the court properly refused to recognize any preclusive burden on Deiter.[94] After all, Deiter had no problem utilizing technology to penetrate Connecticut's borders in the first instance—what sense would it make to now find it unreasonable to pull her into Connecticut physically, given modern transportation advancements?[95] Furthermore, the court gave proper weight to the interest of the state in providing a safe environment for electronic property storage, and to the broad public policy against cyber crime.[96] In short, the court's rationale reflected the sound, logical public policy response to the international cyber crime issue: hackers should have to come to us, not the other way around.

MacDermid applied the proper analysis to reach the proper result in light of the realities of modern commerce and the policy considerations of providing adequate protection against hacking. To put it simply, *MacDermid* represents a proper adaptation of *International Shoe* to the data age. In fact, from a personal jurisdiction jurisprudence standpoint, *MacDermid* is quite uninteresting. It seems likely that even the divided *McIntyre* Court might well find "purposeful availment" and personal jurisdiction in unanimity in this case.

However, the *MacDermid* court's ability to rely on extremely narrowing circumstances—an explicit "knowing" contractual provision—begs for an examination of modern factual scenarios beyond the scope of *MacDermid*. The question then becomes, even though the Second Circuit got it right in *MacDermid*, just how well equipped are our courts to handle novel issues of personal jurisdiction in the data age? In other words, early personal jurisdiction jurisprudence asked: "can we, the states, reach outside of our boundaries to pull in non-resident defendants?" Subsequent jurisprudence responded "sometimes." Then, personal jurisdiction case law set out to define the mechanisms for figuring out the "sometimes." The *MacDermid* court applied these mechanisms and properly responded to the issue presented. Is our court system, as a whole, similarly well-equipped to figure out the "sometimes" in other cases involving technology?

IV. FIGURING OUT THE "SOMETIMES"

Short of a contractual acknowledgment as to the geographic location of electronic data, when does the fleeting nature of modern communication give rise to the proper exercise of personal jurisdiction? The answer depends on how far back into history we reach in order to inform our personal jurisdiction approach.

A. Most of Us

Most of us perhaps have no idea where our online actions produce effects, geographically. Thus, even when our actions constitute illegal activity, it is difficult to conclude that there has been purposeful availment sufficient to establish

93. *Id.*

94. *Id*. at 731.

95. *Id*. Though the Second Circuit cited modern travel conveniences "easing" any burdens upon Deiter, the author is not convinced by this reasoning; while airline travel is certainly easier than travel by horse and buggy, it does not follow that modern travel is unequivocally *easy* or convenient.

96. *Id*.

minimum contacts with any particular state. To use a throwback internet term, driving down the information superhighway is decidedly different from driving down I-95. When someone navigates a physical interstate highway in the direction of, say, Massachusetts, she continuously makes decisions that reaffirm her intent to go to, and be in, Massachusetts. This is clearly distinguishable from online navigation, where clicking one link may activate electronic processes in California, and clicking on the next dials up servers in Washington D.C.[97] Furthermore, in the latter context, this all happens instantaneously, with no commitment, let alone continuous re-commitment, by the individual. In short, establishing personal jurisdiction in a specific forum based on these fleeting electronic interactions would be a tall order for any plaintiff, whether analyzed from a due process or state sovereignty standpoint.

Perhaps adequate notice regarding the geographical implications of certain online activity would facilitate a finding of purposeful availment in regard to litigation arising out of that activity. Of course, the question would then become: "what is *adequate* notice,"[98] the consideration of which is beyond the scope of this Note. Suffice it to say that policy considerations against stifling electronic commerce may preclude any holdings that such notice confers jurisdiction.

In the employment context, however, contractual provisions like the one in *MacDermid* will likely become more commonplace as businesses act to protect their data in a particular forum. Playing into this consideration will be the availability of long-arm provisions, like Connecticut's, which confer jurisdiction based on computing activities. Again, these considerations, while interesting, are beyond the scope of this Note.

B. Hackers: Intentional Thieves

What is quite interesting is the scenario where a corporation has its principal place of business in, say, Connecticut, but stores its data on servers or a cloud service[99] located in, say, California. A claim arises out of an alleged intentional misappropriation of data files from the California server. Under the defendant-centric due process analysis of *MacDermid* and Justice Ginsburg's *McIntyre* dissent, there does not seem to be much justification for denying the corporation's ability to bring suit in California. California would be the site of the injury[100] and, perhaps more importantly, the defendant here may be akin to a burglar who travelled to California, broke into the company's building, stole its tangible

97. *See* Brain, *supra* note 87; *Email*, WIKIPEDIA, http://en.wikipedia.org/wiki/Email (last visited Oct. 14, 2013).

98. For example, a provision within a website's terms and conditions versus a flashing banner on the homepage.

99. *See generally* WINSTON MAXWELL & CHRISTOPHER WOLF, A GLOBAL REALITY: GOVERNMENTAL ACCESS TO DATA IN THE CLOUD (May 23, 2012), *available at* http://www.cil.cnrs.fr/CIL/IMG/pdf/Hogan_Lovells_White_Paper_Government_Access_to_Cloud_Data_Paper_1_.pdf; *Federal Guidance Needed to Address Control Issues with Implementing Cloud Computing*, U.S. GOV'T ACCOUNTABILITY OFFICE (May 27, 2010), *available at* http://www.gao.gov/assets/310/305000.pdf.

100. Arguably, the site of the injury is Connecticut, where the financial or other damages of the misappropriation are felt. However, the situs of the injury is commonly found to be where the original event that caused the injury occurred, not where the resultant damages were subsequently felt. MacDermid v. Deiter, No. 3:11-CV-00855-WWE, 2011 WL 6001625, at *3 (Dist. Conn. 2011).

property, and then fled the state.[101] Under the *McIntyre* plurality approach, however, California's authority to exercise jurisdiction would be limited by a rigid application of purposeful availment. It is entirely foreseeable that the *McIntyre* plurality, much like it did in *McIntyre* itself, would find the defendant here to not have sufficiently subjected itself of *either* state's authority.[102] Furthermore, taking the plurality opinion's sovereignty language at its word would require an inquiry into whether suit in California would infringe upon Connecticut's authority, or indeed, whether judgment in California would be valid at all.

In the same vein, consider a Connecticut corporation that maintains an intricate, multi-state system of servers to handle its data assets. The analysis and accompanying result would likely vary, as in the previous example, depending on whether one approaches the analysis from a due process or state authority point of view. Again, if due process is the standard, a state court's exercise of jurisdiction over a claim resulting from an intentional misappropriation from any one of these servers would likely be proper.[103] However, from a federalism starting point, even an eventual acute harm in one particular state may not indicate the defendant's submission to the authority of that state.

C. Hackers: Cyber Attacks

Much like an intentional misappropriation of proprietary data, a targeted, individualized cyber attack[104] would be likely to confer jurisdiction in the state that hosts the damaged server under a due process analysis.[105] This analysis asks what the defendant knew or reasonably should have known so that the exercise of personal jurisdiction in the forum state would not infringe upon her constitutional rights. Thus, a targeted cyber attack would permit a finding that the attacker purposefully availed itself of the state's benefits, or could reasonably anticipate being haled into court there.[106] A narrowly targeted attack may also confer jurisdiction under a state sovereignty analysis but, as described in the previous

---

101. This is of course assuming that sufficient minimum contacts, via either purposeful availment or "directed at" activity, could be found from the fact that the defendant intentionally stole property located in California.

102. J. McIntyre Machinery Ltd. v. Nicastro, 131 S. Ct. 2780, 2789 (2011); *see* Zach Vosseler, Note, *A Throwback to Less Enlightened Practices: J. McIntyre Machinery Ltd. v. Nicastro*, 160 U. PA. L. REV. PENNUMBRA 366, 372, 374 (2012) ("If the Court's reasoning in *J. McIntyre* holds, defendants could, by virtue of having sufficiently few contacts with any single state, could escape jurisdiction in *all* states.").

103. *See* United States v. Muench, 694 F.2d 28, 33 (2d Cir. 1982) ("The intent to cause effects within the United States . . . makes it *reasonable* to apply to persons outside United States territory a statute which is not expressly extraterritorial in scope.") (emphasis added)

104. *See generally* BRUCE SCHNEIER, BEYOND FEAR: THINKING SENSIBLY ABOUT SECURITY IN AN UNCERTAIN WORLD (2003); BRUCE SCHNEIER, SECRETS AND LIES: DIGITAL SECURITY IN A NETWORKED WORLD (Carol Long ed., 2000); Oona Hathaway et al., *The Law of Cyber-Attack*, 100 CAL. L. REV. 817 (2012).

105. Ford v. United States, 273 U.S. 593, 623 (1927) ("The principle that a man who outside of a country willfully puts in motion a force to take effect in it is answerable at the place where the evil is done, is recognized in the criminal jurisprudence of all countries. And the methods which modern invention has furnished for the performance of criminal acts in that manner has made this principle one of constantly growing importance and of increasing frequency of application.")

106. *See* Peridyne Tech. Solutions, LLC v. Matheson Fast Freight, Inc., 117 F. Supp. 2d 1366 (N.D. Ga. 2000); CompuServe, Inc. v. Patterson, 89 F.3d 1257 (6th Cir. 1996).

subsection, where the plaintiff's operation or data storage spans multiple sovereignties, the picture becomes less clear.

Ironically, the more widespread the attack and, consequently, the larger the radius of detrimental effects, the less certain *any* exercise of personal jurisdiction becomes.[107] For example, a massive attack waged by Russian or Chinese hackers upon U.S. servers in all 50 states would not be unlike J. McIntyre Machinery Ltd. targeting U.S. market penetration in general. Thus, whether the cyber attack is successful in all states or one, a court adhering to *McIntyre* principles may very well find that the hackers had not subjected themselves to the authority of any state in particular. A New Jersey corporation heavily damaged as a result of the attack may be out of luck in New Jersey, or anywhere else.[108] Furthermore, under a sovereignty analysis, a foreign hacker may enjoy immunities that a domestic hacker may not.[109]

D. Gray Areas: Digital Trespass, SPAM, and Diminishing Bandwidth

Somewhere between "hacker" and "average internet user" lies a bit of a gray area, which contains individuals who access restricted servers without authorization,[110] spammers who flood servers or inundate subscribers with unsolicited information,[111] and individuals who purposefully or innocently demand a server's limited bandwidth.[112] In-depth treatment of the jurisdictional considerations of each of these types of behavior is beyond the scope of this Note. But the extent to which we view the proper analysis as one that "ensures a defendant will not be haled into a jurisdiction solely as a result of 'random,' 'fortuitous,' or 'attenuated' contacts,"[113] as opposed to one regarding the scope of a sovereign's authority, will dictate how we come out on these issues, as we have seen in *McIntyre*.

V. CONCLUSION

MacDermid is a model for how state courts should respond to novel jurisdictional questions presented by the ambiguities of the data age. The traditional due process mechanism set forth in *International Shoe* and developed by subsequent case law provides the adaptability demanded of modern courts. This defendant-centric approach ensures a case-by-case-like analysis of each new nuanced set of facts involving increasingly interconnected technology. It necessarily involves consideration of the realities of modern commerce and communication, as it sets out to determine, as a threshold matter, whether sufficient

---

107. *J. McIntyre*, 131 S. Ct. at 2789; *See* Vosseler, *supra* note 102, at 372, 374.

108. *See* Vosseler, *supra* note 102, at 374.

109. J. *McIntyre*, 131 S. Ct. at 2789; *See* Vosseler, *supra* note 102, at 370.

110. *See, e.g., Peridyne*, 117 F. Supp. 2d at 1372 (finding the proper exercise of jurisdiction where the defendants actively entered a system they knew to be in Georgia, manipulated security rights, and viewed files).

111. *See, e.g.*, Verizon Online Services, Inc. v. Ralsky, 203 F. Supp. 2d 601, 604 (E.D. Va. 2002); United States v. Carlson, 209 Fed. Appx. 181 (3d Cir. 2006).

112. *See, e.g.*, Pulte Homes, Inc. v. Laborers' Int'l Union of N. Am., 648 F.3d 295 (6th Cir. 2011).

113. *J. McIntyre*, 131 S. Ct. at 2801 (Ginsburg, J., dissenting) (quoting Burger King Corp. v. Rudzewicz, 471 U.S. 462, 475 (1985)).

minimum contacts exist between the defendant and the forum state. Of course, these minimum contacts may be technological in nature.[114] Furthermore, in the required due process reasonableness test, courts necessarily must weigh the broader technological and commercial context in which the transaction that gives rise to litigation takes place.

In short, *MacDermid* showcases the Second Circuit's proper adaptation of *International Shoe* principles to reach the proper, logical, and desirable result in the data age. Conjuring up realistic scenarios outside of the scope of the convenient facts presented by *MacDermid* showcases the flexibility and appropriateness of the due process mechanism utilized by the Second Circuit. Upon consideration of the issues discussed in the previous section, the *MacDermid* approach consistently yields the proper result in the furtherance of individual liberty, public policy, data protection and, indeed, the state's interests.

There is turmoil in the broader jurisdictional landscape, however. Just how far back into history should we look to shape our modern jurisdictional framework? Though *McIntyre* does not appear to be a complete revivification of *Pennoyer*—the contacts analysis appears alive and well—the plurality opinion does direct us to begin the inquiry with sovereignty and the capacity of the state to render judgment over a non-resident defendant. As we have seen in the previous section, this approach seems to lead to inefficient and inconsistent results when the alleged behavior is ambiguous. And as we constantly push the frontier of technological innovation, our virtual actions are increasingly geographically ambiguous. The sovereignty-centric approach places ultimate significance on borders as borders become less significant.[115] This approach sacrifices proper consideration of the realities of the modern marketplace, and thus fails to account for the actual behavior of the defendant in this context. Thus, as the current personal jurisdiction jurisprudence is apparently in flux, it appears we are in danger of an inconsistent application and enforcement of data protection laws. The dangers of such inconsistency for those relying on sensitive proprietary data—individuals, businesses, and governments—are bad enough,[116] but such a patchwork approach has potentially disastrous implications for the state's ability to provide a safe haven for its citizen's sensitive and proprietary data.[117] That such hindrance upon a significant state interest has its roots in a revivification of the sovereignty-centric approach to personal jurisdiction analysis is, of course, ironic.

The state of our personal jurisdiction jurisprudence, then, provides little useful guidance for state courts faced with novel issues in the data age. Perhaps it is encouraging that state courts nonetheless seem prepared to adapt traditional

---

114. *See* CompuServe, Inc. v. Patterson, 89 F.3d 1257 (6th Cir. 1996); Zippo Mfg. Co. v. Zippo Dot Com, 952 F. Supp. 1119 (W.D. Pa. 1997); GTE New Media Services, Inc. v. BellSouth Corp., 199 F.3d 1343 (D.C. Cir. 2000); D.C. Micro Dev., Inc. v. Lange, 246 F. Supp. 2d 705 (W.D. Ky. 2003).

115. *See* MAXWELL & WOLF, *supra* note 99, at 2 (arguing that the physical location of data is an increasingly less significant barrier to government data access).

116. *See* BRUCE SCHNEIER, LIARS AND OUTLIERS: ENABLING THE TRUST THAT SOCIETY NEEDS TO THRIVE (2012); Mark Watts, *A Problem for Business: The Data Protection Patchwork*, WHO'SWHOLEGAL (Nov. 2012), http://www.whoswholegal.com/news/features/article/28696/a-problem-business-data-protection-patchwork.

117. *See generally* SCHNEIER, *supra* note 116.

jurisdictional principles to the electronic age.[118] But a lack of guidance breeds inconsistency,[119] and inconsistency begets unfairness and inadequate protection. Given modern commerce's increasing reliance upon data,[120] and the increasing amount of sensitive personal data accumulating on servers globally,[121] inadequate protection could pose serious dangers for businesses, governments, and consumers.

118. *See* MacDermid, Inc. v. Deiter, 702 F.3d 725, 729-30 (2d. Cir. 2012); Vosseler, *supra* note 102, at 384 (citing lower court cases that have "either explicitly stated that J. McIntyre has changed nothing or have *sub silentio* continued to use their pre-J. McIntyre tests for personal jurisdiction.").

119. *See* Vosseler, *supra* note 102, at 374.

120. *See generally* SCHNEIER, *supra* note 116.

121. Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1710 (2010); Omer Tene & Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics*, 11 NW. J. TECH. & INTELL. PROP. 239, ¶ 79 (2013).