Washington Journal of Law, Technology & Arts

University of Washington School of Law

VOL. 6 AUTUMN 2010 NO. 2

CONTENTS

Washington Journal of Law, Technology & Arts

University of Washington School of Law

VOL. 6 AUTUMN 2010 NO. 2

WASHINGTON JOURNAL OF LAW, TECHNOLOGY & ARTS
VOLUME 6, ISSUE 2 AUTUMN 2010

NEUTRALIZING ACTUAL CONTROVERSY: HOW PATENT HOLDERS CAN REDUCE THE RISK OF DECLARATORY JUDGMENT IN PATENT DISPUTES

Homer Yang-hsien Hsu [*]

CITE AS: 6 WASH J.L. TECH. & ARTS 93 (2010)
https://digital.lib.washington.edu/dspace-law/handle/1773.1/476

ABSTRACT

Alleged patent infringers may bring declaratory judgment actions against patentees when actual controversies exist over infringement or validity. Such declaratory judgment actions are important strategic tools because they allow alleged infringers to take initiative and bring actions, thereby eliminating the risk of doing business without knowing whether continued product use would constitute infringement. Declaratory judgment actions also provide alleged infringers an opportunity to choose the forum in which to bring their suits. In order to bring such an action, however, there must be an actual controversy between the parties to establish standing. The United States Supreme Court's 2007 decision in MedImmune v. Genentech made it easier for alleged infringers to obtain declaratory judgments without actually terminating or breaching license agreements. The Court held that all circumstances should be considered when determining whether an actual controversy exists. The United States Court of Appeals for the Federal Circuit, relying on MedImmune, has since considered what communication between parties is sufficient to establish the existence of such a controversy. This Article analyzes those decisions, discusses possible implications, and describes how the Federal Circuit has finally embraced the "all circumstances" test for determining whether a sufficient controversy exists to sustain a declaratory judgment action.

---

[*] Homer Yang-hsien Hsu, University of Washington School of Law, Class of 2011. Thank you to Professor Jane K. Winn and Professor Paul T. Meiklejohn.

TABLE OF CONTENTS

INTRODUCTION

Declaratory judgment actions are important tools for alleged infringers in patent litigation because they resolve uncertainty and prevent monetary damages from continuing to accrue for infringement. In addition, declaratory judgment actions give alleged infringers strategic advantages by acting as plaintiff, including the ability to choose a favorable forum and to enjoy the benefits of primacy and memorability at trial.[1] The issue, however, is whether there is an actual controversy such that an infringer will have standing to bring an action for a declaratory judgment.

In 2007, the United States Supreme Court in *MedImmune, Inc. v. Genentech, Inc.* abandoned the two-part test traditionally applied when

[1] In trial, the plaintiff generally introduces the case ("primacy") and delivers the closing statement ("memorability" or "recency"). Primacy and memorability put plaintiffs in a better position to convince judges or juries.

determining if a party has standing to bring a declaratory judgment action—showing (1) a reasonable basis for believing the infringer will be sued and (2) meaningful preparation to infringe.[2] Instead the Court adopted a new "all circumstances" test that eliminated the first prong and made it easier to obtain declaratory relief in patent cases. However, confusion resulted when the Federal Circuit failed to consistently apply the new test and instead considered certain elements of the two-part test from time to time.

Two years after *MedImmune*, in *Hewlett-Packard Co. v. Acceleron LLC*,[3] the Federal Circuit eliminated some of that confusion when it followed the "all circumstances" test to determine whether an alleged infringer had standing to bring a declaratory judgment action. The *Hewlett-Packard* case is important not only because it confirms that the Federal Circuit follows the "all circumstances" test set out in *MedImmune*, but also because it sheds light on the trend that the Federal Circuit treats patent-holding companies differently from patentees who actually use their patents.

I. DECLARATORY JUDGMENT ACTIONS IN PATENT DISPUTES

The Declaratory Judgment Act[4] authorized federal courts to provide legal remedies to interested parties who have an "actual controversy" within the meaning of Article III of the U.S. Constitution.[5] Congress intended declaratory relief as an alternative to injunction in cases where injunctive relief is unavailable.[6] The objectives of the Declaratory Judgment Act are (1) to avoid accrual of avoidable damages to those who are not certain of their rights, (2) to afford early adjudication without waiting until the adversary decides to bring a patent infringement lawsuit, and (3) to clarify legal relationships before they have been disturbed or a party's rights have been

---

[2] MedImmune, Inc. v. Genentech, Inc., 549 U.S. 118 (2007).

[3] Hewlett-Packard Co. v. Acceleron LLC, 587 F.3d 1358, 1361 (Fed. Cir. 2009).

[4] 28 U.S.C. §§ 2201-2202 (2006).

[5] U.S. Const., art. III, § 2.

[6] Steffel v. Thompson, 415 U.S. 452 (1974).

violated.[7]

Courts do not have jurisdiction to deliver advisory opinions on questions that are abstract or hypothetical in nature, so only interested parties who have an actual controversy are eligible to bring a suit.[8] The term "actual" is one of emphasis rather than of definition, which means that the controversy should be real in the constitutional sense.[9] In other words, the Declaratory Judgment Act requires that actions for declaratory judgment meet the same test for "case or controversy" as required for conventional suits under Article III federal jurisdiction.[10] Determining whether there is an actual controversy is essential to deciding whether a party has standing to sue.[11]

Declaratory judgment actions are frequently used in patent infringement suits as both shields and swords. Employed as a shield, a defendant can bring counterclaims for a declaration of invalidity, unenforceability, and non-infringement. In contrast, when used as a sword, the declaratory judgment action allows the alleged infringer to file suit before the patentee brings an infringement action. This can prevent damages from continuing to accrue and can help businesses make risk assessments.

The advantages of declaratory judgments for alleged patent infringers are many. For example, declaratory judgment actions allow

---

[7] Travelers Ins. Co. v. Davis, 490 F.2d 536, 543 (9th Cir. 1974).

[8] Aetna Life Ins. Co. v. Haworth, 300 U.S. 227 (1937).

[9] *Id.* at 239-40.

[10] *See, e.g.*, Jennifer R. Saionz, *Declaratory Judgment Actions in Patent Cases: The Federal Circuit's Response to MedImmune v. Genentech*, 23 BERKELEY TECH. L.J. 161, 161 (2008).

[11] However, even if an actual controversy exists, courts still have discretion to hear declaratory judgment action. But the district court must have a sound basis for refusing jurisdiction over a declaratory judgment action. *See* Wilton v. Seven Falls Co., 515 U.S. 277, 289-90 (1995). *See also* Elecs. for Imaging, Inc. v. Coyle, 394 F.3d 1341, 1345-46 (Fed. Cir. 2005); Capo, Inc. v. Dioptics Med. Prod., Inc., 387 F.3d 1352, 1357 (Fed. Cir. 2004) ("There must be a sound basis for refusing to adjudicate an actual controversy, for the policy of the Act is to enable resolution of active disputes."); Genentech v. Eli Lilly & Co., 998 F.2d 931, 937 (Fed. Cir. 1993) ("When there is an actual controversy and a declaratory judgment would settle the legal relations in dispute and afford relief from uncertainty or insecurity, in the usual circumstance the declaratory action is not subject to dismissal.").

alleged infringers to eliminate uncertainty regarding potential patent infringements. In addition, bringing a declaratory judgment action gives an alleged infringer the opportunity to choose a favorable place to sue and to control aspects pertaining to litigation such as forum convenience, potential jury pools, local court rules, trial speed, and court sophistication regarding patent cases. Finally, declaratory judgment actions allow alleged infringers to better control business risks.

The declaratory judgment action is an equitable remedy. This means that the court has discretion to decline the declaratory judgment action jurisdiction if it deems appropriate, even if a justiciable controversy exists.[12]

II. FROM TWO-PART TO "ALL CIRCUMSTANCES": HISTORY OF DECLARATORY JUDGMENT ACTIONS AND SUPREME COURT'S DECISION IN *MEDIMMUNE*

The Supreme Court first established the meaning of "actual controversy" under the Declaratory Judgment Act in *Aetna Life Insurance Co. v. Haworth*.[13] In *Aetna*, the Court defined the limitation of "actual controversy" to mean controversies appropriate for judicial determination by a court described in Article III of the Constitution.[14] The Court stated that "the controversy must be definite and concrete,

---

[12] *See, e.g.*, EMC Corp. v. Norand Corp., 89 F.3d 807, 810 (Fed. Cir. 1996) ("Even if there is an actual controversy, the district court is not required to exercise declaratory judgment jurisdiction, but has discretion to decline that jurisdiction.").

[13] *Aetna Life*, 300 U.S. 227 (1937). In *Aetna Life*, the declaratory judgment defendant, Haworth, had purchased life insurance policies from Aetna Life Insurance Company. The policies provided that upon proof of total and permanent disability, the insured was no longer required to pay additional premiums, yet the insurance policies would remain in force. Haworth allegedly ceased payment of premiums and provided Aetna with documentation of disability. Haworth did not initiate suit against Aetna or make any threats to do so. Aetna sued Haworth under the Declaratory Judgment Act, seeking to have the policies declared null and void for nonpayment.

[14] *Id.* at 239-40 ("The Declaratory Judgment Act of 1934, in its limitation to 'cases of actual controversy,' manifestly has regard to the constitutional provision and is operative only in respect to controversies which are such in the constitutional sense. The word 'actual' is one of emphasis rather than of definition.").

touching the legal relations of parties having adverse legal interests."[15]

Later, in *Maryland Casualty Co. v. Pacific Coal & Oil Co.*, the Supreme Court stated that the presence of an "actual controversy" within the meaning of the statute depends on "whether the facts alleged, under all the circumstances, show that there is a substantial controversy, between parties having adverse legal interests, of sufficient immediacy and reality to warrant the issuance of a declaratory judgment."[16]

Based on this guidance, the United States Court of Appeals for the Federal Circuit tried to develop a two-part test to assess whether an actual controversy exists.[17] This dual prong test required: (1) an explicit threat or other action by the patentee that creates a reasonable apprehension on the part of the declaratory judgment plaintiff that they will face an infringement suit (the "reasonable apprehension" prong) and (2) present activity by the declaratory judgment plaintiff which could constitute infringement, or concrete steps taken with the intent to conduct such activity (the "meaningful preparation" prong).[18]

Under the first element, the defendant's (patent holder's) actions needed to create, in the alleged infringer, a reasonable apprehension of an infringement suit.[19] An express accusation of infringement was sufficient, but not necessary, to create a reasonable apprehension of suit.[20] For the second element, the plaintiff (alleged infringer) needed to engage in an activity that would be subject to an infringement

---

[15] *Id.* at 240-241.

[16] Maryland Casualty Co. v. Pacific Coal & Oil Co., 312 U.S. 270 (1941); *see also* Arrowhead Indus. Water, Inc. v. Ecolochem, Inc., 846 F.2d 731 (Fed. Cir.1988); *see also* EMC Corp. v. Norand Corp., 89 F.3d 807, 810 (Fed. Cir. 1996).

[17] *See* C.R. Bard, Inc. v. Schwartz, 716 F.2d 874, 879 (Fed. Cir. 1983) ("Courts have interpreted the controversy requirement in the patent field to generally mean that the declaratory plaintiff has sufficient interest in the controversy and that there is a reasonable threat that the patentee or licensor will bring an infringement suit against the alleged infringer.").

[18] Teva Pharm. USA, Inc. v. Novartis Pharm. Corp., 482 F.3d 1330, 1339 (Fed. Cir. 2007); *see also* Arrowhead Indus. Water, Inc. v. Ecolochem, Inc., 846 F.2d 731, 737 (Fed. Cir. 1988).

[19] *See Arrowhead* 846 F.2d at 736.

[20] *See* Goodyear Tire & Rubber Co. v. Releasomers, Inc., 824 F.2d 953, 956 (Fed. Cir. 1987).

accusation or have made "meaningful preparation" for such an activity.[21]

In *MedImmune, Inc. v. Genentech, Inc.*, the Supreme Court held that the Federal Circuit's two-part test was inconsistent with Supreme Court precedent, explicitly overruling the "reasonable apprehension" element of the test and implicitly overruling the second part as well.[22] The Supreme Court replaced the Federal Circuit's formalistic approach with a "totality of the circumstances" approach that inquires into the parties' legal interests to determine whether there is an actual controversy.[23]

The Court held that although MedImmune paid royalties to Genentech to eliminate the risk of an infringement suit, it was not prohibited from also filing a declaratory judgment action for non-infringement, invalidity, and unenforceability.[24] The Supreme Court reasoned that Article III's justiciable controversy requirement did not require an unwilling licensee to risk liability for infringement, with potential treble damages, before it could obtain a declaration of actively contested legal rights.[25] In short, the plaintiff of a declaratory judgment action does not have to choose between abandoning a claim of right and facing the threat of injury.[26]

Although the Supreme Court did not explicitly overrule both prongs of the two-part test, the Court indicated in a footnote that the Federal Circuit's two-part test conflicted with Supreme Court precedent.[27] Regardless of the Court's ultimate decision about the two-

---

[21] *See Arrowhead*, 846 F.2d at 736.

[22] MedImmune, Inc. v. Genentech, Inc., 549 U.S. 118, 132 n. 11 (2007). *See also* SanDisk Corp. v. STMicroelectronics, Inc., 480 F.3d 1372, 1380 n. 2 (Fed. Cir. 2007) ("We therefore leave to another day the effect of *MedImmun*e, if any, on the second prong.").

[23] *MedImmune*, 127 S. Ct. at 771.

[24] *Id.*

[25] *Id.* at 775 ("The rule that a plaintiff must destroy a large building, bet the farm, or (as here) risk treble damages and the loss of 80 percent of its business before seeking a declaration of its actively contested legal rights finds no support in Article III.").

[26] *Id.* at 772-73.

[27] *Id.* at 774 n. 11.

part test, it was clear from the opinion that the "all circumstances" test should apply in the future.[28] It has, however, taken the Federal Circuit a number of years to completely abandon the two-prong test and embrace the "all circumstances" analysis.

III. AFTER *MEDIMMUNE*: CONFUSION CAUSED BY CONTINUOUS USE OF ELEMENTS IN THE IMPROPER TWO-PART TEST

After *MedImmune*, the Federal Circuit initially followed aspects of the new "all circumstances" test set out by the Supreme Court. But occasionally the Federal Circuit would continue to apply the traditional two-part test, thereby leading to some confusion because the Supreme Court had held that test was improper. This confusion, however, was eventually eliminated by *Hewlett-Packard Co. v. Acceleron LLC*, a 2009 Federal Circuit case that clearly follows the "all circumstances" test of *MedImmune*. With that decision, the Federal Circuit signaled to future litigants that the "all circumstances" test will now be used going forward.

A. Initial Adherence to the "All Circumstances" Test

In *SanDisk Corp. v. STMicroelectronics, Inc.*, the Federal Circuit considered a dispute between competitors who had entered into negotiations to cross-license their patents.[29] When negotiations began to break down, SanDisk filed suit, alleging infringement of one of its patents and seeking a declaratory judgment of non-infringement and invalidity of the fourteen STMicroelectronics (ST) patents that had been discussed during the cross-licensing negotiations.[30] ST filed a motion to dismiss for lack of subject matter jurisdiction. The district court granted the motion, holding that no actual case or controversy

---

[28] *Id.* at 771 ("Basically, the question in each case is whether the facts alleged, under all the circumstances, show that there is a substantial controversy, between parties having adverse legal interests, of sufficient immediacy and reality to warrant the issuance of a declaratory judgment.").

[29] *SanDisk*, 480 F.3d 1372 (Fed. Cir. 2007).

[30] *Id.* at 1376.

existed under the declaratory judgment action because SanDisk did not "reasonably apprehend" suit.[31]

The Federal Circuit reversed. The court determined that it had jurisdiction in a declaratory judgment action where cross-licensing negotiations were ongoing.[32] Furthermore, the court held that SanDisk could bring a declaratory judgment action before it received explicit threats of litigation.[33] "[W]here a patentee asserts rights under a patent based on certain identified ongoing or planned activity of another party, and where that party contends that it has the right to engage in the accused activity without license," the court has jurisdiction over the action "and the party need not risk a suit for infringement by engaging in the identified activity before seeking a declaration of its legal rights."[34] The Federal Circuit observed that this holding was consistent with *MedImmune*.[35]

In addition, the Federal Circuit acknowledged that *MedImmune* overruled the "reasonable apprehension" element of the two-part test,[36] but the court observed that *MedImmune* did not address the "meaningful preparation" element. The Federal Circuit declined to consider the effect of *MedImmune* on the second element at that time.[37]

---

[31] *Id.*

[32] *Id.* at 1383.

[33] *Id.* at 1381 ("We hold only that where a patentee asserts rights under a patent based on certain identified ongoing or planned activity of another party, and where that party contends that it has the right to engage in the accused activity without license, an Article III case or controversy will arise and the party need not risk a suit for infringement by engaging in the identified activity before seeking a declaration of its legal rights.").

[34] *Id. See also* Cygnus Therapeutic Sys. v. ALZA Corp., 92 F.3d 1153 (Fed. Cir. 1996) (holding that declaratory judgment jurisdiction was not supported where the "patentee does nothing more than exercise its lawful commercial prerogatives and, in so doing, puts a competitor in the position of having to choose between abandoning a particular business venture or bringing matters to a head by engaging in arguably infringing activity").

[35] *SanDisk*, 480 F.3d at 1381-82.

[36] *Id.* at 1380.

[37] *Id.* at 1380 n. 2 ("We therefore leave to another day the effect of *MedImmune*, if any, on the second prong."). The second prong asks whether the plaintiff engaged in infringing activity or meaningfully prepared to engage in such activity.

In short, the Federal Circuit failed to completely embrace the Supreme Court's "all circumstances" test in *SanDisk*.

That same year, in *Teva Pharmaceuticals USA, Inc. v. Novartis Pharmaceuticals Corp.*, the Federal Circuit addressed a dispute between a generic (Teva) and a brand name (Novartis) pharmaceutical company.[38] Unlike *SanDisk Corp.*, however, *Teva Pharmaceuticals* moved closer towards the "all circumstances" test.

In *Teva Pharmaceuticals*, Novartis filed a New Drug Application (NDA) with the FDA for the drug Famvir and listed five patents covering the drug: one relating to its composition and four relating to therapeutic methods.[39] Later, Teva filed an Abbreviated New Drug Application (ANDA) for a generic version of Famvir and certified that Teva's drug did not infringe upon Novartis' patents or that the patents were invalid.[40]

Novartis sued Teva for infringement of its composition patent, but not the method patents.[41] In a separate suit, Teva brought a declaratory judgment action for invalidity and non-infringement of the unasserted method patents.[42] Because Novartis had not taken any actions or made any threats to enforce the method patents, the district court held that

---

[38] *Teva Pharm. USA, Inc. v. Novartis Pharm. Corp.*, 482 F.3d 1330 (Fed. Cir. 2007).

[39] *Teva*, 482 F.3d at 1334. The Federal Food, Drug, and Cosmetic Act provides generic pharmaceutical manufacturers with a shortened approval process for marketing generic drugs. Federal Food, Drug, and Cosmetic Act of 1938, Pub. L. No. 75-717, 52 Stat. 1040 (codified as amended at 21 U.S.C. §§ 301-399 (2000 & Supp. IV 2004)); Drug Price Competition and Patent Term Restoration Act of 1984, Pub. L. No. 98-417, 98 Stat. 1585 (1984) (codified in relevant parts at 21 U.S.C. § 355 and 35 U.S.C. § 271(e) (2000 & Supp. III 2003)).

[40] *Id.* The ANDA filed by generic manufacturers allows utilization of the safety and efficacy data submitted for the equivalent branded drug's previously filed NDA. 21 U.S.C. § 355(j) (2000 & Supp. III 2003). As an added incentive to produce generic drugs, the first company to file an ANDA for a particular drug is granted a 180-day period of market exclusivity before other generic manufacturers may enter the market. The 180-day period of market exclusivity begins to run either when the generic drug begins commercial marketing or when a court declares the patent covering the branded drug invalid.

[41] *Id.* at 1334-35.

[42] Teva Pharm. USA, Inc. v. Novartis Pharm. Corp., No. 05-2881 JLL, 2005 U.S. Dist. LEXIS 38649 (D. N.J. Dec. 12, 2005).

no justiciable controversy existed and dismissed the case for lack of subject matter jurisdiction.[43]

The Federal Circuit looked at the totality of the circumstances under which Teva had brought suit and reversed the district court, holding that Teva had a justiciable controversy under the *MedImmune* standard.[44] The court emphasized that "Novartis created a present and actual 'controversy' by choosing to sue . . . on Teva's single act of infringement, thereby placing into actual dispute the soundness of Teva's ANDA and Teva's ability to secure approval of the ANDA."[45] Though the Novartis-initiated suit was a different case from Teva's declaratory judgment action, litigation over the composition patent and the method patents necessarily involved the same technology, the same parties, and related patents. Thus, the Federal Circuit concluded that there was a justiciable controversy.[46]

B. Federal Circuit Still Considers Factors of the Improper Two-Part Test

Although the Federal Circuit began to consider "all circumstances" in *Teva Pharmaceuticals* when determining declaratory judgment jurisdiction, it seems that the traditional two-part test did not completely disappear. Just a year after the *SanDisk* and *Teva* cases, in 2008, the Federal Circuit seemed to resurrect at least part of its two-part test.

In *Cat Tech LLC v. TubeMaster, Inc.*,[47] the Federal Circuit found that the second prong of "meaningful preparation" was still intact—at least as a factor used in determining whether a dispute is immediate and real.

Cat Tech had brought suit against TubeMaster for patent infringement. TubeMaster counterclaimed, seeking a declaration that its devices did not infringe Cat Tech's patent and that the patent was invalid and unenforceable. Cat Tech subsequently amended its comp-

---

[43] *Id.* at 9.

[44] *Teva*, 482 F.3d at 1340.

[45] *Id.*

[46] *Id.*

[47] Cat Tech LLC v. TubeMaster, Inc., 528 F.3d 871 (Fed. Cir. 2008),

laint, seeking a declaratory judgment of infringement.[48] The district court concluded that TubeMaster did not infringe[49] so Cat Tech appealed.

On appeal, the Federal Circuit affirmed, but in doing so seemed to reinvigorate the "meaningful preparation element." The Federal Circuit concluded that although *MedImmune* articulated a "more lenient legal standard" for the availability of declaratory judgment relief in patent cases,[50] the issue of whether there has been "meaningful preparation" to conduct potentially infringing activity remains an important element when considering the "totality of circumstances" for purposes of the *MedImmune* test.[51] In other words, if a declaratory judgment plaintiff has not taken significant, concrete steps to conduct infringing activity, the dispute is neither "immediate" nor "real" and the requirements for justiciability have not been met.[52] In contrast, from the Federal Circuit's point of view, the immediacy requirement for a declaratory judgment could be satisfied if the alleged infringer took significant, concrete steps to use the potentially infringing design, like TubeMaster did in this case.[53]

In addition to *Cat Tech*, there are two other cases showing that the Federal Circuit appeared to be retreating from its acceptance of the "all circumstances" test in *Sandisk*. In *Janssen Pharmaceutica, N.V. v. Apotex, Inc.*,[54] the Federal Circuit required more than speculative fear of harm to establish that the dispute was "definite and concrete."[55] In *Prasco, LLC v. Medicis Pharm. Corp.*, the Federal Circuit required the plaintiff in a declaratory judgment action to show an affirmative act by the

---

[48] *Cat Tech*, 528 F.3d at 878.

[49] *Id.*

[50] *Id.* (quoting Micron Tech v. MOSAID Tech., 518 F.3d 897, 902 (Fed. Cir. 2008)).

[51] *Id.* (quoting *Teva*, 482 F.3d at 1339).

[52] *Id.* (quoting Lang v. Pac. Marine & Supply Co., 895 F.2d 761, 764 (Fed Cir. 1990) (emphasizing that the test for justiciability "looks to the accused infringer's conduct and ensures that the controversy is sufficiently real and substantial")).

[53] *Cat Tech*, 528 F.3d at 882.

[54] Janssen Pharmaceutica, N.V. v. Apotex, Inc., 540 F.3d 1353 (Fed. Cir. 2008).

[55] *Id.* at 1362-63.

patentee that demonstrated intent to sue.[56] Both of these holdings are reminiscent of the Federal Circuit's traditional two-part test.

IV. *HEWLETT-PACKARD* AND THE FEDERAL CIRCUIT'S RETURN TO *MEDIMMUNE*

In 2009, the Federal Circuit once again returned to the "all circumstances" test, but this time with more conviction. In *Hewlett-Packard Co. v. Acceleron LLC*,[57] the Federal Circuit held that when Acceleron, the patent-holder, offered a potential patent license to Hewlett-Packard without expressly accusing infringement, that contact was sufficient to give Hewlett-Packard standing to bring a declaratory judgment action.

Acceleron had contacted Hewlett-Packard on September 14, 2007 to offer a patent license with a two-week deadline for a response. Acceleron requested an opportunity to discuss the potential license of a patent recently acquired and asked Hewlett-Packard not to use any information exchanged in the discussion in any litigation. Two weeks later, Hewlett-Packard responded by agreeing not to file a declaratory judgment action for 120 days if Acceleron similarly agreed not to file an infringement action during the same period. Acceleron then responded, stating that it did not believe Hewlett-Packard had any basis for filing a declaratory judgment action. Once again, it imposed a two-week period for Hewlett-Packard to accept the patent license offer.

On October 17th, Hewlett-Packard filed a declaratory judgment suit in the District Court for the District of Delaware. Acceleron moved to dismiss for lack of subject matter jurisdiction. On March 11, 2009, the district court granted Acceleron's motion, based on the following factual filings: (1) Acceleron never proposed a confidentiality agreement, and (2) Acceleron never accepted Hewlett-Packard's 120-day -standstill proposal and never provided a counter-proposal or other assurance it would not sue Hewlett-Packard. Hewlett-Packard appealed the dismissal of its declaratory judgment action.

---

[56] Prasco, L.L.C. v. Medicis Pharm. Corp., 537 F.3d 1329, 1338 (Fed. Cir. 2008).

[57] Hewlett-Packard Co. v. Acceleron LLC, 587 F.3d 1358 (Fed. Cir. 2009).

On appeal, the Federal Circuit reversed the dismissal after holding a declaratory judgment action cannot be defeated simply by using a correspondence that "avoids the magic words such as 'litigation' or 'infringement.'"[58] The Federal Circuit further recognized that it is implausible (especially after *MedImmune* and several post-*MedImmune* decisions) to expect that a competent lawyer drafting such correspondence for a patent owner would identify specific claims, present claim charts, and explicitly allege infringement.[59]

On the other hand, the court noted that a communication from a patent owner to another party that merely identifies its patent and the other party's product line, without more communications, cannot establish adverse legal interests between the parties, let alone the existence of a "definite and concrete" dispute. More communication is required to establish declaratory judgment jurisdiction.[60]

The Federal Circuit noted that the test for declaratory judgment jurisdiction in patent cases is objective.[61] Indeed, it is the objective words and actions of the patent holder that are controlling.[62] Thus, conduct that can be reasonably inferred as demonstrating intent to enforce a patent can create declaratory judgment jurisdiction.

The Federal Circuit further observed that Acceleron was solely a licensing entity, and without enforcement it received no benefits from its patents.[63] In the Federal Circuit's view, this added significance to the fact that Acceleron refused Hewlett-Packard's request for a mutual standstill—and such a limited standstill is distinguishable from a covenant not to sue.[64]

The facts of this case, when viewed objectively and in totality, showed to the Federal Circuit's satisfaction that Acceleron took the

---

[58] *Id.*

[59] *Id.*

[60] *Id.* at 1362.

[61] *Id.* at 1363 (quoting Arrowhead Indus. Water, Inc. v. Ecolochem, Inc., 846 F.2d 731, 736 (Fed.Cir.1988)).

[62] *Id.* (quoting BP Chems. v. Union Carbide Corp., 4 F.3d 975, 979 (Fed. Cir. 1993)).

[63] *Id.* at 1364.

[64] *Id.* (such as that cited by the district court in Prasco, LLC, v. Medicis Pharmaceutical Corp., 537 F.3d 1329, 1341 (Fed. Cir. 2008)).

affirmative step of twice contacting Hewlett-Packard directly and making an implied assertion of its patent right against Hewlett-Packard. In other words, Acceleron did not directly accuse Hewlett-Packard of patent infringement, but it did (1) indicate that its patents were "relevant" to Hewlett-Packard products, (2) insist that Hewlett-Packard's response must come within two weeks, and (3) ask Hewlett-Packard not to file a declaratory judgment action. Thus, the Federal Circuit held that it is reasonable for Hewlett-Packard to interpret Acceleron's letters as implicitly asserting its patent rights under the circumstances,[65] and Hewlett-Packard was eligible to bring a declaratory judgment action.

The *Hewlett-Packard* decision is important because the Federal Circuit confirmed again—and, hopefully, once and for all—that the "all circumstances" test should be applied to determine jurisdiction over declaratory judgment actions.[66] It is also noteworthy that Federal Circuit considered that a patentee is "solely a licensing entity, and without enforcement it receives no benefits from its patents."[67] This signals that the Federal Court may treat patent holders who actually sell patented products more favorably than patent holding entities who only license patents.

V. IMPLICATION OF *HEWLETT-PACKARD*—"ALL CIRCUMSTANCES" TEST CONFIRMED & PATENT HOLDING ENTITIES BEWARE

The *Hewlett-Packard* case confirms that the Federal Circuit will apply the "all circumstances" test in determining whether an actual controversy exists to satisfy the standing requirement for declaratory judgment actions by alleged infringers during licensing negotiation. An actual controversy occurs when the patent holder and the alleged infringer have different opinions about whether accused products fall within the scope of the patents. Patent holders should therefore consider the risk of facing a declaratory judgment action if adverse

---

[65] *Id.*

[66] *Id.* ("Our decision in this case undoubtedly marks a shift from past declaratory judgment cases").

[67] *Id.*

opinions form during licensing negotiations. Patentees may want to arrange certain nondisclosure agreements (NDAs) between parties prior to the licensing negotiation. Although NDAs may not completely prevent the alleged infringer from bringing declaratory judgment actions, they may provide a contractual basis for a remedy if the accused infringer discloses materials in further declaratory judgment actions.

Another strategy would be for patentees to bring an infringement suit before initiating the licensing negotiation. The patentee can generally file a complaint first without serving the accused infringer to allow both parties to have a chance to negotiate a possible license. By doing so, the patentees can still choose favorable fora and enjoy the advantages of primacy and memorability in litigation.

Patent holding companies should expect that the courts will take into consideration that such companies generally license their patents rather than using them in other ways. The Federal Circuit reasoned that because licensing is how patent holding companies use their patents, the "actual controversy" occurs more easily when adverse positions are formed during licensing negotiation. If the patentee is a holding company, which means that patentee can only enforce the patent right by licensing, that status is also a factor to consider when determining declaratory judgment jurisdiction.

CONCLUSION

Hewlett-Packard signaled the Federal Circuit's decision to finally embrace the "all circumstances" test from *MedImmune* in determining whether there is an actual controversy to establish standing for a declaratory judgment action over patent infringement. Communication merely identifying patents and products is insufficient to establish adverse legal interests or an actual controversy. Instead, the courts will consider all circumstances under an objective standard to determine whether there is a declaratory judgment jurisdiction. If the patentee is a holding company, the courts may more easily find a sufficient controversy exists over a licensing negotiation. On the other hand, the courts still have discretion whether to hear a declaratory judgment action case even if the actual controversy element is met. To preserve

the advantage of choosing favorable fora, it is recommended that patentees bring any applicable infringement suit before initiating license negotiations.

PRACTICE POINTERS

- Patentees should avoid ultimatums or strict deadlines during license negotiation. During the license negotiation, the patentee should be aware that the accused infringer might use every correspondence and communication as evidence to show actual controversy between the parties. Demands for responses within specific timeframes could suggest a sufficient controversy has arisen.
- Patentees should avoid disclosing patents not intended. Patentees should not disclose unrelated patents during license negotiation because such disclosure may create a basis for the accused infringer to bring a declaratory judgment action against that unrelated patent.
- Patentees should consider executing nondisclosure agreements (NDAs). Before any license negotiation, both parties should consider executing a NDA to prevent disclosure of any communication during negotiation. Such an agreement may not effectively prevent the accused infringers from bringing declaratory judgment actions, but the NDA could provide a contractual basis for possible damage claims if one party breaches.
- Patentees should consider bringing suit before license negotiation. Based on the modern "all circumstances" test, it is easier for accused infringers to bring a declaratory judgment action than before. To preserve the advantages of choosing favorable fora, patentees may want to bring an infringement suit before license negotiations.
- Patentees should challenge, on equitable grounds, declaratory judgment claims brought during negotiations. Patentees should consider asking courts to decline jurisdiction if an alleged infringer files a declaratory judgment action during licensing negotiations. Since a declaratory judgment action is an equitable remedy, the

court can decline jurisdiction if it perceives the alleged infringer filed the action just to gain leverage in the licensing negotiation.

- Patentees should negotiate penalty clauses in license agreements. Patentees should include penalty clauses in license agreements that are triggered by any attack on the patent. Possible penalties could include an automatic increase in royalty rates, liquidated damages, or termination of the license.

WASHINGTON JOURNAL OF LAW, TECHNOLOGY & ARTS
VOLUME 6, ISSUE 2 AUTUMN 2010

OUTSIDER HACKING AND INSIDER TRADING: THE EXPANSION OF LIABILITY ABSENT A FIDUCIARY DUTY

James A. Jones II[*]

CITE AS: 6 WASH J.L. TECH. & ARTS 111 (2010)
https://digital.lib.washington.edu/dspace-law/handle/1773.1/477

ABSTRACT

In January 2008, the United States District Court for the Southern District of New York held that trading put options of a company's stock based on inside information allegedly obtained by hacking into a computer network did not violate antifraud provisions of federal securities law. The court ruled that the defendant's alleged "hacking and trading" did not amount to a violation of section 10(b) of the Securities Exchange Act of 1934 and Rule 10b-5, promulgated thereunder, because there was no proof the hacker breached a fiduciary duty in obtaining the information. The United States Court of Appeals for the Second Circuit overturned the District Court's decision, finding that a breach of fiduciary duty was not required for computer hacking to be "deceptive." This article evaluates the Second Circuit's decision in S.E.C. v. Dorozhko in light of the assumption that liability under the misappropriation theory requires a breach of fiduciary duty. This article also explores how the Second Circuit's decision may potentially expand section 10(b) liability to a wider range of parties who take advantage of access to material nonpublic information by trading securities based on that information.

---

[*] James A. Jones II, CPA, University of Washington School of Law, J.D. program Class of 2011; University of Washington Foster School of Business, MPAcc, 2006. Thank you to Professor Anita Ramasastry of the University of Washington School of Law and student editor Jessica Blye for their valuable feedback. Thank you also to Casey M. Nault of Graham & Dunn PC for his thoughtful review of this Article.

TABLE OF CONTENTS

INTRODUCTION

Hacking into a computer system to obtain financial information and trading securities based on that information may be illegal, but whether it constitutes insider trading under section 10(b) of the Securities Exchange Act of 1934 is a different matter. In 2008, the United States District Court for the Southern District of New York held that a Ukrainian hacker who made almost $300,000 through "hacking and trading" did not violate section 10(b) and Rule 10b-5 because there was no proof the hacker breached a fiduciary duty in obtaining the information.[1] However, the Second Circuit Court of Appeals reversed the trial court and held that a breach of fiduciary duty was not required for such "hacking and trading" to be a violation of section 10(b) and Rule 10b-5.[2]

The Second Circuit's opinion expands the definition of insider trading under section 10(b) of the Securities Exchange Act of 1934, extending liability to defendants who did not breach a fiduciary duty in obtaining the inside information.[3] This decision challenges the

---

[1] S.E.C. v. Dorozhko, 606 F. Supp. 2d 321, 324 (S.D.N.Y. 2008).

[2] S.E.C. v. Dorozhko, 574 F.3d 42, 51 (2d Cir. 2009).

[3] Martin Flumenbaum & Brad S. Karp, *Fiduciary Duty and "Deceptive" Fraudulent Conduct under Rule 10(b)*, N.Y. L.J., Aug. 31, 2009, at 3.

common assumption, gathered from a line of United States Supreme Court cases,[4] that liability under the misappropriation theory requires a breach of fiduciary duty. The decision also differs from the dicta and holdings of three other circuit court decisions.[5]

This Article examines and evaluates the Second Circuit's decision in light of Supreme Court precedent and the assumption that liability under the misappropriation theory requires a breach of fiduciary duty. This Article then compares the Second Circuit's decision to the differing circuit court rulings addressing this issue. Finally, this Article explores the implications of the Second Circuit's decision and provides practice pointers based on these implications.

I. INSIDER TRADING UNDER SECTION 10(B) OF THE SECURITIES EXCHANGE ACT OF 1934

Section 10(b) of the Securities Exchange Act of 1934 permits the U.S. Securities and Exchange Commission (SEC) to promulgate rules and regulations to protect the public and investors by prohibiting the "use or employ" of "any manipulative or deceptive device or contrivance" in connection with the purchase or sale of securities.[6] Rule 10b-5, which implements this provision, prohibits any act or omission resulting in fraud or deceit in connection with the purchase

---

[4] *See generally* Chiarella v. United States, 445 U.S. 222 (1980) (holding that the mere possession of nonpublic market information did not result in a duty to disclose under § 10(b)); United States v. O'Hagan, 521 U.S. 642 (1997) (adopting the misappropriation theory); S.E.C. v. Zandford, 535 U.S. 813 (2002) (holding that a securities broker who traded securities under his client's account and transferred the proceeds to his own account, amounted to a scheme to defraud that was "in connection with" the security transactions within the meaning of § 10(b)).

[5] *See generally* Regents of California v. Credit Suisse First Boston (USA), Inc., 482 F.3d 372, 389 (5th Cir. 2007) (stating that the Supreme Court "has established that a device, such as a scheme, is not 'deceptive' unless it involves breach of some duty of candid disclosure"); United States v. Bryan, 58 F.3d 933, 951 (4th Cir. 1995) (suggesting mere thieves do not violate § 10(b) and Rule 10b-5 by trading on stolen information); S.E.C. v. Cherif, 933 F.2d 403, 411 (7th Cir. 1991) (stating that defendant's argument of being a "mere thief" was "[t]he only possible barrier to application of the misappropriation theory").

[6] 15 U.S.C. § 78j(b) (2006).

or sale of securities.[7]

The Supreme Court has established that there are two complimentary theories of insider trading, each with a fiduciary principle at its core.[8] Under the "traditional theory" of insider trading liability, corporate insiders violate section 10(b) and Rule 10b-5 when they trade their corporation's securities while having knowledge of material, nonpublic information.[9] The Supreme Court has expanded on this theory, holding that a corporate insider violates section 10(b) by giving a "tip" to an outsider for the purpose of having the outsider trade, and the outsider does trade.[10] However, the tippee is only liable under section 10(b) for trading on material nonpublic information if the tippee is aware or should have been aware that the tipper breached his fiduciary duty to the shareholders by disclosing the information to the tippee.[11]

In *United States v. O'Hagan*, the Supreme Court adopted the "misappropriation theory" of liability under section 10(b) and Rule 10b-5. Under this theory, a person outside the corporation violates section 10(b) and Rule 10b-5 when he misappropriates material nonpublic information for the purpose of trading securities without disclosing the use of the corporation's material nonpublic information.[12] Instead of relying on a fiduciary relationship between the company insider and purchaser or seller of the company's stock, the misappropriation theory bases liability on a "fiduciary-turned-trader's deception of those who entrusted him with access to confidential information."[13]

Although fiduciary principles underlie both theories of insider trading, the SEC continues to bring complaints under section 10(b) and Rule 10b-5 regardless of whether a fiduciary-like duty has been breached. Supreme Court precedent is therefore important because it sets the boundaries for such prosecution.

---

[7] 17 C.F.R. § 240.10b-5 (2010).

[8] United States v. O'Hagan, 521 U.S. 642, 651-52 (1997).

[9] *Id.*

[10] Dirks v. S.E.C., 463 U.S. 646, 660 (1983).

[11] *Id.*

[12] *O'Hagan*, 521 U.S. at 652.

[13] *Id.*

II. THE DISTRICT COURT DETERMINES DOROZHKO DID NOT VIOLATE SECTION 10(B) OF THE SECURITIES EXCHANGE ACT OF 1934

In October 2007, Oleksandr Dorozhko, a Ukrainian national, hacked into the computer network of Thomson Financial, Inc., obtaining access to IMS Health, Inc.'s soon-to-be-released negative earnings announcement.[14] Based on this information, Dorozhko purchased all available put options in IMS Health, totaling $41,670.90.[15] When the market opened the morning following the release of IMS Health's third quarter earnings to the public, the stock plummeted and Dorozhko sold all of his 630 IMS Health put options, realizing a net profit of $286,456.59 overnight.[16]

The SEC alleged in a complaint, filed against Dorozhko on October 29, 2007, that Dorozhko violated section 10(b) and Rule 10b-5 "by either hacking into a computer network and stealing material nonpublic information, or through a more traditionally-recognized means of insider trading such as receiving a tip from a corporate insider."[17] The SEC also obtained "a temporary restraining order freezing the proceeds of Dorozhko's trades."[18]

Relying principally on three Supreme Court opinions (*Chiarella v. United States*,[19] *United States v. O'Hagan*,[20] and *S.E.C. v. Zandford*[21]), the District Court determined that the "deceptive" element of section 10(b) required a breach of a fiduciary duty.[22] The District Court held that such "'hacking and trading' [did] not amount to a violation of section 10(b) and Rule 10b-5 because Dorozhko did not breach any fiduciary or similar duty 'in connection with' the purchase or sale of a

---

[14] S.E.C. v. Dorozhko, 606 F. Supp. 2d 321, 323 (S.D.N.Y. 2008).

[15] *Id.*

[16] *Id.* at 326-27.

[17] *Id.* at 322.

[18] *Id.* at 322-23.

[19] Chiarella v. United States, 445 U.S. 222 (1980).

[20] United States v. O'Hagan, 521 U.S. 642 (1997).

[21] S.E.C. v. Zandford, 535 U.S. 813 (2002).

[22] *Dorozhko*, 606 F. Supp. 2d at 323 (citing *Chiarella*, 445 U.S. at 227-30; *O'Hagan*, 521 U.S. at 653-60; *Zandford*, 535 U.S. at 825).

security."[23] Although the District Court did note that Dorozhko "may have broken the law," the Court found Dorozhko not liable under section 10(b) "because he owed no fiduciary or similar duty either to the source of his information or those he transacted with in the market."[24] Soon after, however, the Second Circuit reversed and held that a breach of fiduciary duty is not a required element of a section 10(b) complaint.[25]

III. THE SECOND CIRCUIT'S DECISION IN LIGHT OF SUPREME COURT PRECEDENT

Prior to the Second Circuit's decision in *S.E.C. v. Dorozhko,* no federal court had ever held that the theft of material nonpublic information by a corporate outsider who subsequently trades securities based on that information violates section 10(b).[26] The Second Circuit's decision negates the assumption that liability under the misappropriation theory requires a breach of fiduciary duty. In reaching its conclusion, the Second Circuit relied primarily on the same three Supreme Court decisions relied upon by the District Court in its analysis: *Chiarella v. United States*,[27] *United States v. O'Hagan*,[28] and *S.E.C. v. Zandford*.[29]

In its analysis, the District Court reasoned that the SEC was seeking to revive Justice Blackmun's dissent in *Chiarella*.[30] The District Court suggested that Dorozhko's actions were fraudulent within the meaning of section 10(b) because he "stole" the information he traded on.[31] While the District Court relied on *Chiarella* to further support its conclusion that a breach of fiduciary duty was required to uphold a conviction under section 10(b), the Second Circuit read *Chiarella* and

---

[23] *Id.* at 324.
[24] *Id.*
[25] S.E.C. v. Dorozhko, 574 F.3d 42, 51 (2d Cir. 2009).
[26] *Dorozhko*, 606 F. Supp. 2d at 323.
[27] Chiarella v. United States, 445 U.S. 222 (1980).
[28] United States v. O'Hagan, 521 U.S. 642 (1997).
[29] S.E.C. v. Zandford, 535 U.S. 813 (2002).
[30] *Dorozhko*, 606 F. Supp. 2d at 334.
[31] *Id.*

its dissent in a different light.

In *Chiarella*, an employee of a financial printer used material nonpublic information to purchase securities offered by acquiring and target corporations.[32] The Supreme Court reversed the defendant's section 10(b) and Rule 10b-5 conviction, because the "mere possession of nonpublic market information" did not result in a duty to disclose under section 10(b).[33] Since the defendant was under no obligation to disclose his knowledge of inside information, the defendant's nondisclosure was not fraud.[34]

The Second Circuit distinguished *Chiarella* as an example of fraud based on nondisclosure while *Dorozhko* dealt with an affirmative misrepresentation.[35] *Chiarella* addressed the "legal effect of the [defendant's] silence"; whether the defendant had a duty to disclose or abstain from trading.[36] Whereas, in *Dorozhko*, the SEC argued that Dorozhko "affirmatively misrepresented himself in order to gain access to material, nonpublic information, which he then used to trade."[37]

In *O'Hagan*, the Supreme Court adopted the misappropriation theory and held that when a person misappropriates confidential information for securities trading purposes in breach of a duty to the source of the information, that person commits fraud "in connection with" a securities transaction, thereby violating section 10(b) and Rule 10b-5.[38] The District Court noted that the *O'Hagan* court's application of the misappropriation theory remained consistent with the traditional theory, in premising "a violation of section 10(b) and Rule 10b-5 on a breach of duty to disclose or abstain."[39] The District Court found significance in the Supreme Court's decision not to adopt Justice Blackmun's dissent in *Chiarella*, noting that the Supreme Court certainly could have chosen to adopt Justice Blackmun's more

---

[32] Chiarella v. United States, 445 U.S. 222, 224 (1980).
[33] *Id.* at 235.
[34] *Id.*
[35] S.E.C. v. Dorozhko, 574 F.3d 42, 47 n.4 (2d Cir. 2009).
[36] *Chiarella*, 445 U.S. at 226.
[37] *Dorozhko*, 574 F.3d at 49.
[38] United States v. O'Hagan, 521 U.S. 642, 653 (1997).
[39] S.E.C. v. Dorozhko, 606 F. Supp. 2d 321, 336 (S.D.N.Y. 2008).

expansive view of Rule 10b-5.[40] The District Court therefore concluded, based on the Supreme Court's decisions in both *Chiarella* and *O'Hagan*, that a breach of a fiduciary duty was required under both the traditional and misappropriation theory.[41]

In its analysis of *O'Hagan*, the Second Circuit noted that the Supreme Court had found that the defendant "had committed fraud through 'silence' because the defendant had a duty to disclose to the source of the information (his client) that he would trade on the information."[42] Similar to its analysis of *Chiarella*, the Second Circuit attempted to distinguish *O'Hagan* from the *Dorozhko* case on the basis of nondisclosure compared to affirmative misrepresentation. In the view of the Second Circuit, the defendant's "silence" resulted in fraud based on the defendant's fiduciary duty to disclose to the source of the nonpublic information. *O'Hagan*, on the other hand, did not concern an affirmative misrepresentation and the Court did not address whether the defendant would have violated section 10(b) had the defendant not had a fiduciary duty to disclose to the source of the nonpublic information.

In *Zandford*, the Supreme Court held that a securities broker who traded securities under his client's account and transferred the proceeds to his own account, committed a scheme to defraud that was "in connection with" the securities transactions within the meaning of section 10(b).[43] Although the District Court conceded that *Zandford* stood for "the proposition that Dorozhko's alleged scheme was 'in connection with' the purchase or sale of securities," it stopped short of

---

[40] *Id.* Justice Blackmun views section 10(b) as a "catchall" provision designed to protect investors from unknown risks. *Chiarella*, 445 U.S. at 246 (Blackmun, J., dissenting). In his view, the court's approach in *Chiarella*, "advance[d] an interpretation of § 10(b) and Rule 10b-5 that stops short of their full implications." *Id.* at 247. Justice Blackmun would have instead held "that persons having access to confidential material information that is not legally available to others generally are prohibited by Rule 10b-5 from engaging in schemes to exploit their structural informational advantage through trading in affected securities." *Id.* at 251.

[41] *Dorozhko*, 606 F. Supp. 2d at 336.

[42] S.E.C. v. Dorozhko, 574 F.3d 42, 47 (2d Cir. 2009).

[43] S.E.C. v. Zandford, 535 U.S. 813 (2002).

finding Dorozhko's alleged scheme "deceptive."[44] The District Court relied on Justice Stevens' reiterations that "Zandford's section 10(b) violation was predicated on his breach of fiduciary duty" to suggest "that there can be no 'deception,' and therefore no liability under section 10(b), absent the existence and breach of a fiduciary duty."[45] The Second Circuit did not address this part of the District Court's analysis. However, based on the Second Circuit's final conclusion, it appears that the Second Circuit did not find the *Zandford* decision to be dispositive as to whether Dorozhko's alleged scheme was "deceptive."

While the District Court relied on these three decisions to conclude the "deceptive" element of section 10(b) requires a breach of fiduciary duty, the Second Circuit concluded that "none of the Supreme Court opinions relied upon by the District Court . . . establishes a fiduciary-duty requirement as an element of every violation of section 10(b)."[46] Instead, the Second Circuit reasoned that "nondisclosure in breach of a fiduciary duty" merely satisfies section 10(b)'s requirement of a "deceptive device or contrivance," and therefore does not "*require* a fiduciary relationship as an element of an actionable securities claim under section 10(b)."[47] By concluding that a fiduciary relationship was not a required element of an actionable securities claim under section 10(b), the Second Circuit was free to adopt the SEC's theory of fraud and determine that an affirmative misrepresentation to gain access to material, nonpublic information and then trade on that information could be "deceptive."

IV. CIRCUIT SPLIT

The Second Circuit is the first federal court to hold that theft of material nonpublic information by a corporate outsider and subsequent trading on that information violates section 10(b) and Rule 10b-5. Three other Circuit Courts have addressed this issue and appear

---

[44] *Dorozhko*, 606 F. Supp. 2d at 338.

[45] *Id.*

[46] *Dorozhko*, 574 F.3d at 48.

[47] *Id.* at 49.

to side with the District Court's decision that section 10(b) and Rule 10b-5 always require a breach of a fiduciary duty.

The dicta contained in opinions by the Fourth and Seventh Circuits suggest that thieves of material nonpublic information do not violate section 10(b) or Rule 10b-5 when they trade on the basis of that information. In *S.E.C. v. Cherif*, a former employee of an investment bank secretly kept his key card and broke into the bank's offices on a number of occasions to steal information on pending corporate transactions.[48] He then traded securities on the basis of that information, making a profit.[49] Though the Seventh Circuit sustained Cherif's conviction on the grounds that an employee's duty to a former employer is not extinguished upon termination, the court did comment on Cherif's argument that he was a "mere thief" who owed no duty to anyone.[50] The Seventh Circuit remarked that Cherif's argument of being a "mere thief" was "[t]he only possible barrier to application of the misappropriation theory."[51]

In another court of appeals case, *United States v. Bryan*, the Fourth Circuit suggested even more forcefully that mere thieves do not violate section 10(b) and Rule 10b-5 by trading on stolen information.[52] The defendant, a former director of the West Virginia Lottery, used confidential information about forthcoming contracts to purchase shares in companies that did business with the West Virginia Lottery.[53] The Fourth Circuit reversed the District Court's decision, choosing not to adopt the misappropriation theory in part because the theory would lead future courts to expand and eventually abandon the concept of fiduciary duty that lay at the heart of section 10(b).[54] The Fourth Circuit predicted that courts would eventually be forced to abandon the requirement of a fiduciary duty all together and hold that mere thieves violated the misappropriation theory.[55]

---

[48] S.E.C. v. Cherif, 933 F.2d 403, 406-07 (7th Cir. 1991).

[49] *Id.*

[50] *Id.* at 411.

[51] *Id.*

[52] United States v. Bryan, 58 F.3d 933, 951 (4th Cir. 1995).

[53] *Id.* at 939.

[54] *Id.* at 951.

[55] *Id.*

Although both the Fourth and Seventh Circuits seem to suggest that "mere thieves" of material nonpublic information do not violate section 10(b) or Rule 10b-5 when they trade on the basis of that information, it should be noted that both of these cases were decided before *O'Hagan* and the adoption of the misappropriation theory by the Supreme Court. The pre-dating of *O'Hagan* combined with the fact that these comments were included in the dicta of these court of appeals cases raises doubt as to the authority of these cases.

The Fifth Circuit, however, held a breach of a fiduciary duty is a required element of a section 10(b) violation. In *Regents of the Univ. of Cal. v. Credit Suisse First Boston (USA), Inc.*, the Fifth Circuit discussed how the Supreme Court "has established that a device, such as a scheme, is not 'deceptive' unless it involves breach of some duty of candid disclosure."[56] The Fifth Circuit made this observation relying on the same precedent as that of the District Court in *Dorozhko*.

In summary, there is a circuit split as to whether a fiduciary duty is a required element of a section 10(b) violation: In the Second Circuit, the SEC need not prove a breach of a fiduciary duty; but in the Fourth, Fifth, and Seventh Circuits, the SEC must prove such a breach. In fact, the Second Circuit even comments that "[a]t least one of [its] sister circuits has made the same observation [as the District Court] relying on the same precedent."[57]

V. IMPLICATIONS OF THE SECOND CIRCUIT'S DECISION

The Second Circuit appears to have opened the door to a legal theory that computer hacking in connection with insider trading may sometimes be "deceptive" under section 10(b), while rejecting the idea that "deceptive" actions under section 10(b) can only occur through a violation of a fiduciary duty. Under the prior liability regime, a "paradoxical situation" existed where a person who obtained material nonpublic information "legally" could be held liable under criminal

---

[56] Regents of the Univ. of Cal. v. Credit Suisse First Boston (USA), Inc., 482 F.3d 372, 389 (5th Cir. 2007).

[57] S.E.C. v. Dorozhko, 574 F.3d 42, 48 (2d Cir. 2009) (referring to the Fifth Circuit's decision in *Regents of the Univ. of Cal.*, 482 F.3d 372).

and civil securities law for trading on such information, whereas a thief, acting illegally, might not be.[58] Without the Second Circuit's ruling, this situation would continue to be exploited by information thieves because there would be no associated consequence, under section 10(b) and Rule 10b-5 liability, if the thief were to trade on such information.[59] Even the District Court was aware of this situation, commenting that "[t]his case highlights a potential gap arising from reliance on fiduciary principles in the legal analysis that courts have employed to define insider trading."[60]

Under the reasoning used by the Second Circuit, the SEC will be able to bring its insider trading cases under the affirmative misrepresentation category to avoid having to show a breach of duty by the defendant.[61] This newfound ability may result in broader enforceability under section 10(b), exposing more defendants to potential civil liability under the securities law.[62] Both the District Court and Second Circuit noted that such "hacking and trading" schemes have typically been prosecuted under federal and state criminal statutes. The SEC will now be able to pursue cases of computer hacking as violations of federal securities laws in addition to violations of other federal and state criminal statutes. Thus, this decision will provide the SEC wide latitude in determining how to address securities-related misconduct, at least within the Second Circuit.

The Second Circuit's decision also has the potential to expand section 10(b) liability to a wider range of parties who take advantage of access to material nonpublic information and trade securities based on

---

[58] Carolyn Silane, *Electronic Data Theft: A Legal Loophole for Illegally-Obtained Information–A Comparative Analysis of U.S. and E.U. Insider Trading Law*, 5 SETON HALL CIRCUIT REV. 333, 363 (2009).

[59] *Id.* However, such hackers may still be liable under mail or wire fraud, 18 U.S.C. § 1341 (2006 & Supp. II 2008) or 18 U.S.C. § 1343 (2006 & Supp. II 2008), and the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2006 & Supp. II 2008).

[60] S.E.C. v. Dorozhko, 606 F. Supp. 2d 321, 323 (S.D.N.Y. 2008).

[61] Peter Henning, *On the SEC, Mark Cuban, and a Man Named Dorozhko*, WALL ST. J., Jul. 28, 2009, http://blogs.wsj.com/law/2009/07/28/on-the-sec-mark-cuban-and-a-man-named-dorozhko/.

[62] Flumenbaum & Karp, *supra* note 3.

that information. Anyone who deceptively obtains information and trades securities based on that information may be subjected to enforcement or liability, regardless of their relationship to the issuer of the information. Under this new regime, securities traders will need to be cautious as to how they come into possession of confidential information. If they do so in a manner that could be viewed as "deceptive," then trading securities based on that information could violate the securities laws, regardless of whether any duty was breached.

CONCLUSION

The Second Circuit's decision appears to have expanded the Supreme Court's definition of insider trading and extended section 10(b) liability to a wider range of parties who trade securities based on access to material nonpublic information. This decision has opened the door to a legal theory that computer hacking in connection with insider trading may sometimes be "deceptive" under section 10(b), while foreclosing the argument that "deceptive" actions under section 10(b) can only occur through a violation of a fiduciary duty. The impact of this decision, however, is minimized by the lack of a clear and consistent theory of insider trading liability as to the fiduciary duty requirement among the circuit courts. Given the split on this issue between the Second Circuit and the Fourth, Fifth, and Seventh Circuits, it is possible that the Supreme Court will review this issue in the near future. Until this issue is resolved by the Supreme Court or Congress intervenes, securities traders will have to monitor how they come into possession of confidential information. If the information is obtained in a manner that could be viewed as "deceptive," then trading securities based on that information could violate section 10(b) of the Securities Exchange Act of 1934.

PRACTICE POINTERS

- When using material, nonpublic information to purchase or sell securities, traders should be aware of whether they have a fiduciary duty to the source of the information or whether there is such a duty between the source of the information and a third party. If a

fiduciary duty does exist, a trader should not purchase or sell securities based on the information without disclosure.

- Even if no fiduciary duty exists, traders should still monitor the manner in which material, nonpublic information is obtained if such information is used to purchase or sell securities. If the information was obtained in a manner that could be viewed as "deceptive," then trading securities based on that information could violate section 10(b) and Rule 10b-5 and the trader should therefore abstain from trading on the information.
- Even if a trade based on material, nonpublic information does not violate section 10(b) and Rule 10b-5, traders should still consider the reputational damage and significant legal expenses they may incur in defending such trades. In addition, traders should consider other potential legal consequences (e.g., mail or wire fraud, traditional theft theories, or other tort actions) that may arise through use of the material, nonpublic information.

WASHINGTON JOURNAL OF LAW, TECHNOLOGY & ARTS
VOLUME 6, ISSUE 2 AUTUMN 2010

INDUCEMENT OR SOLICITATION? COMPETING INTERPRETATIONS OF THE "UNDERLYING ILLEGALITY" TEST IN THE WAKE OF *ROOMMATES.COM*

Jeffrey R. Doty[*]

CITE AS: 6 WASH J.L. TECH. & ARTS 125 (2010)
https://digital.lib.washington.edu/dspace-law/handle/1773.1/478

ABSTRACT

In Fair Housing Council of San Fernando Valley v. Roommates.com, the United States Court of Appeals for the Ninth Circuit held that a Web site operator loses the immunity granted by section 230 of the Communications Decency Act by materially contributing to the alleged illegality of its third-party content. Subsequent case law seems to reflect two different standards for determining when this "underlying illegality" test is satisfied. Most courts have adopted a narrow reading of Roommates.com, denying immunity only when a Web site has explicitly requested illegal content. In NPS LLC v. StubHub, Inc., however, a Massachusetts district court appears to adopt a broader inducement-based standard that would impose liability upon a much wider range of conduct. This Article examines the recent case law in order to identify the contours of these differing theories for negating § 230 immunity.

TABLE OF CONTENTS

---

[*] Jeffrey R. Doty, University of Washington School of Law, Class of 2011. Thank you to Professor Anita Ramasastry of the University of Washington School of Law and Stephanie Holmes, student editor, for their help, feedback, and inexhaustible patience throughout the editing process.

INTRODUCTION

Section 230 of the Communications Decency Act (CDA)[1] protects Web site operators from suits arising out of third-party content as long as the operators are not partly responsible for the development of that content.[2] In *Fair Housing Council of San Fernando Valley v. Roommates.com*,[3] the Ninth Circuit interpreted this to mean that a Web site operator loses § 230 immunity when it materially contributes to the underlying illegality of its third-party content.[4]

Subsequent case law, however, has not been entirely consistent in its application of the "underlying illegality" test. Most cases seem to indicate that the test is satisfied only when a defendant explicitly requests the illegal material, a scenario found in *FTC v. Accusearch Inc.*,[5] but the recent decision in *NPS LLC v. StubHub, Inc.*[6] suggests that a wider range of conduct generates liability. These divergent

---

[1] 47 U.S.C. § 230 (2006).

[2] *See generally* 4 RAYMOND T. NIMMER, THE LAW OF COMPUTER TECHNOLOGY § 14:11 (4th ed. 2010).

[3] Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157 (9th Cir. 2008).

[4] *Id.* at 1168.

[5] Fed. Trade Comm'n v. Accusearch Inc., 570 F.3d 1187 (10th Cir. 2009).

[6] NPS LLC v. StubHub, Inc., 2009 WL 995483 (Mass. Dist. Ct. Jan. 26, 2009).

approaches raise the possibility that two distinct standards have emerged in the wake of *Roommates.com*: "solicitation," which requires an actual request by the Web site operator, and "inducement," for which implicit suggestions may be sufficient.[7]

This Article will first provide a brief overview of § 230 and the early cases interpreting the provision. Next, the Article will describe the "underlying illegality" limitation of *Roommates.com* and analyze the recent case law that applies it. The Article will conclude by examining the relationship between the solicitation and inducement approaches and by discussing how they might affect future litigants.

I. BASIC OPERATION OF SECTION 230

The purpose behind section 230 of the Communications Decency Act (CDA)[8] was to both promote the free exchange of ideas over the Internet and to encourage voluntary monitoring for offensive or obscene material.[9] The statute accomplishes these goals by ensuring that those who merely provide an outlet or forum for third-party speech over the Internet will not be held liable for any claims that may arise out of the content of that speech.[10]

In determining whether a defendant is entitled to immunity under § 230(c)(1), courts engage in a three-part analysis.[11] First, to receive immunity, the defendant must be a "provider or user of an interactive computer service,"[12] which includes Web sites.[13] Next, the cause of

---

[7] For purposes of this Article, the words "solicitation" and "inducement" are given specific meanings. These are not terms of art however; they are used here merely as conventions. Cases applying *Roommates.com* have not explicitly defined either term, nor have they drawn any clear distinction between the two. Indeed, some courts appear to use the terms interchangeably.

[8] 47 U.S.C. § 230 (2006).

[9] Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1122 (9th Cir. 2003).

[10] Section 230(c)(1) declares that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."

[11] *See, e.g.* Universal Commc'n Sys., Inc. v. Lycos, Inc., 478 F.3d 413, 418-22 (1st Cir. 2007).

[12] 47 U.S.C. § 230(c)(1) (2006).

action must be one that treats the defendant as the "publisher" or "speaker" of the content at issue.[14] Claims that would hold the defendant liable in some other capacity are unaffected by § 230.[15] Finally, the defendant will not be entitled to immunity if "responsible, in whole or in part, for the creation or development"[16] of the content because the scope of § 230 extends only to third-party content. The bulk of § 230 litigation concerns this third prong,[17] but it appears that recent cases have adopted differing approaches for determining whether the defendant is a "content provider" under the *Roommates.com* framework.

II. THE PRE-*ROOMMATES.COM* UNDERSTANDING OF "CONTENT PROVIDER"

Before *Roommates.com*, a Web site operator could engage in a wide range of actions without being considered a "content provider." Early precedent established that immunity encompassed all "traditional editorial functions," including minor editing of spelling, grammar, and length, as well as selecting which content to publish. [18] A Web site operator would only face liability if it were to significantly alter the meaning of the content. [19] Immunity also remained intact when the

---

[13] The Internet itself qualifies as an "interactive computer service," and therefore, a defendant need only be a "user" of the Internet to satisfy the first prong of the test. Because every Web site operator is necessarily an Internet user, this requirement is rarely the subject of litigation. *See* Batzel v. Smith, 333 F.3d 1018, 1030-31 (9th Cir. 2003).

[14] 47 U.S.C. § 230(c)(1) (2006).

[15] For example, in *Barnes v. Yahoo!, Inc.*, 570 F.3d 1096 (9th Cir. 2009), the Ninth Circuit held that § 230 does not insulate a defendant against promissory estoppel claims because liability under such claims is based on the defendant's act of making a promise, rather than its role as a publisher.

[16] 47 U.S.C. § 230(f)(3) (2006) (defining "information content provider").

[17] David S. Ardia, *Free Speech Savior or Shield for Scoundrels: An Empirical Study of Intermediary Immunity Under Section 230 of the Communications Decency Act*, 43 LOY. L.A. L. REV. 373, 454-55 (2010).

[18] *See* Zeran v. Am. Online, Inc., 129 F.3d 327, 330 (4th Cir. 1997). *See also Batzel*, 333 F.3d at 1031.

[19] *See Batzel*, 333 F.3d at 1031.

Web site operator provided neutral tools for third parties to use in creating their own content.[20] Such tools included detailed questionnaires with pre-populated drop-down menus that allowed users to create online profiles.[21] These early developments reflected the notion that § 230 conferred a "broad grant of immunity" on Web site operators.[22]

III. *ROOMMATES.COM* AND THE "UNDERLYING ILLEGALITY" TEST

Fair Housing Council of San Fernando Valley v. Roommates.com is one of the first decisions to place substantive limits on § 230 immunity.[23] The defendant in *Roommates.com* provided an online community where prospective renters and those with available housing could connect with one another by searching user profiles and sending or receiving email notifications.[24] The profiles required users to disclose their race, gender, sexual orientation, and whether or not they had children, as well as their preferences for these same categories, all of which are protected characteristics under the Fair Housing Act (FHA).[25] The Web site then allowed users to conduct searches based on these illegal criteria.[26] The Ninth Circuit denied § 230 protection because the defendant had "developed" the content on users' profiles and the discriminatory results of their searches.[27]

In reaching this conclusion, the court adopted what has been

---

[20] *See, e.g.* Carafano v. Metrosplash.com, Inc., 339 F.3d 1119 (9th Cir. 2003).

[21] *See Id.* at 1124. In concluding that these questionnaires did not render the defendant a content provider of its users' profiles, the court explained that "[n]o profile has any content until a user actively creates it."

[22] *See* Curran v. Amazon.com, Inc., 2008 WL 472433, at *14 (S.D. W. Va. Feb. 19, 2008).

[23] Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157 (9th Cir. 2008).

[24] *Id.* at 1161-62.

[25] *Id.* at 1161. The Fair Housing Act generally makes it illegal to express any preferences regarding a protected characteristic in the context of the sale or rental of a dwelling. *See* 42 U.S.C. § 3604(c) (2006).

[26] *Id.* at 1167.

[27] *Id.* at 1166-67.

called the "underlying illegality"[28] test: "[A] website helps to develop unlawful content, and thus falls within the exception to section 230, if it contributes materially to the alleged illegality of the conduct."[29] The court explained that a Web site that merely provides the tools used to create content nevertheless "materially contributes" to its illegality if the tools themselves are designed to elicit or encourage its illegal nature.[30] Such tools effectively lose their "neutral" character and the Web site operator is rendered a co-developer of the third-party content resulting from their use. Rather than treating § 230 as a "broad grant of immunity," the holding in *Roommates.com* reinforces its limits by establishing the boundary between providing "neutral tools" and being actively involved in the development of a third party's illegal speech.

However, while the underlying illegality test recognizes that a Web site operator can be liable for any content it effectively causes a third party to produce, it is unclear what types of actions will exert this causal force. The uncertainty owes in large part to the vague and varying articulations of the standard found throughout the *Roommates.com* opinion.[31] Some language suggests that a Web site loses immunity by simply encouraging an illegal aspect of its user-generated

---

[28] This Article uses the term "underlying illegality" when referring to the standard set forth in *Roommates.com*. *See* Lynn C. Percival, IV, *The One-Sided Voidability of Contracts Impacted by 47 U.S.C. § 230*, 17 TEX. WESLEYAN L. REV. (forthcoming 2010), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1542423 (adopting this terminology). Other names have been suggested. *See, e.g.* Bradford J. Sayler, *Amplifying Illegality: Using the Exception to CDA Immunity Carved Out By* Fair Housing Council of San Fernando Valley v. Roommates.com *to Combat Abusive Editing Tactics*, 16 GEO. MASON L. REV. 203 (2009) (the "amplifying illegality" concept).

[29] *Roommates.com*, 521 F.3d at 1168.

[30] *Id.* at 1172.

[31] *See* Eric Goldman, *Roommates.com Denied 230 Immunity by Ninth Circuit En Banc (With My Comments)*, TECHNOLOGY AND MARKETING BLOG (April 3, 2008, 8:05 PM), http://blog.ericgoldman.org/archives/2008/04/roommatescom_de_1.htm (discussing potential consequences of the opinion's "myriad of ambiguities").

content.[32] In other parts of the opinion, however, the court stresses that the users who registered with Roommates.com were literally given no choice but to express discriminatory preferences.[33] Adding to the confusion is the spectrum of terms the court uses, variously describing content providers as those who "encourage," "solicit," "elicit," "induce," "urge," "prompt," or "promote" unlawful speech. As might be expected, decisions following *Roommates.com* have not applied the underlying illegality test consistently. Instead, the case law seems to reflect two different approaches to defining culpable behavior: one based on "solicitation" and the other on "inducement."

IV. THE SOLICITATION APPROACH

In a number of recent cases, courts appear to adopt what might be termed a "solicitation standard" for evaluating whether a defendant has materially contributed to the illegality of its third-party content.[34]

---

[32] *See, e.g.*, *Roommates.com*, 521 F.3d at 1167 ("Roommate's search function is similarly designed to steer users based on discriminatory criteria."); *Id.* at 1172 ("The salient fact in *Carafano* was that the website's classifications of user characteristics did absolutely nothing to enhance the defamatory sting of the messages, to encourage defamation or to make defamation easier.").

[33] *See, e.g.*, *Id.* at 1166, n.19 ("Roommate, of course, does much more than encourage or solicit; it forces users to answer certain questions and thereby provide information that other clients can use to discriminate unlawfully."); *Id.* at 1170, n.26 ("But, it is Roommate that *forces* users to express a preference and Roommate that forces users to disclose the information that can form the basis of discrimination by others.").

[34] The emergence of a solicitation standard is evidenced by the many cases interpreting the *Roommates.com* opinion narrowly and declining to extend its holding to other fact patterns. The most critical factor, according to these cases, is that Roommates.com *required* its users to provide discriminatory responses as a condition of using the Web site. *See, e.g.* Nemet Chevrolet, Ltd. v. Consumeraffairs.com, Inc., 591 F.3d 250, 257 (4th Cir. 2009) ("Whereas the website in *Roommates.com* required users to input illegal content as a necessary condition of use, Nemet has merely alleged that Consumeraffairs.com structured its website and its business operations to develop information related to class-action lawsuits."). Many decisions also point out that the questions themselves were discriminatory. *See, e.g.* Atl. Recording Corp. v. Project Playlist, Inc., 603 F. Supp. 2d 690, 701 (S.D.N.Y. 2009) ("The Ninth Circuit's decision was based solely on the fact that the content on the website that

This "solicitation" only occurs when the Web site operator explicitly requests the content directly from the third party. Because the standard is premised on a narrow reading the *Roommates.com* opinion, a defendant whose conduct rises to this level is likely to lose immunity regardless of which standard is used.

A. Key Considerations Under a Solicitation Standard

The solicitation approach appears to have three defining characteristics. To be considered a "developer" of the offending content, a Web site operator must make an explicit request for that content, the request must be specific enough to exclude lawful material, and there must be an illegal motive behind the request. A Web site operator that solicits content in this manner is effectively expressing its own ideas by enlisting a third party to supply the necessary material.

First, under a solicitation standard, a defendant's actions would need to rise to the level of an actual request; a Web site operator will not lose immunity over material submitted in response to an implicit suggestion. In *Best Western International, Inc. v. Furber*,[35] visitors to the defendant's Web site wrote allegedly defamatory emails which the defendant then posted online. The plaintiff sued, arguing that the Web site "impliedly suggest[ed]" that visitors should make defamatory statements, but the court flatly rejected this as a basis for denying immunity.[36] Instead, the court granted summary judgment in favor of the defendant because the Web site did not "explicitly solicit tortious material."[37]

In addition to being explicit, a request must exhibit a certain degree of specificity to constitute a material contribution under the solicitation approach. Among courts that have taken this solicitation

---

was discriminatory was supplied by Roommates.com itself."). *See also* Doe II v. MySpace, Inc., 96 Cal. Rptr. 3d 148, 158 (Cal. Ct. App. 2009) (distinguishing *Roommates.com* by pointing out that MySpace's profile questions were not discriminatory and that MySpace did not require its members to answer them as a condition of using the site).

[35] Best Western Int'l, Inc. v. Furber, 2008 WL 4182827 (D. Ariz. Sep. 5, 2008).

[36] *Id.* at *10

[37] *Id.* at *10

approach, immunity appears to be forfeited only when compliance with the request almost *necessarily* entails providing unlawful content.[38] The case law suggests two basic scenarios that would satisfy this condition. In the first scenario, a Web site operator offers a range of illegal content options and requires a third party to select from it.[39] The most frequently cited example of this scenario is the questionnaire in *Roommates.com*, which required users to select discriminatory answers from pre-populated drop-down menus. In the second scenario, a Web site operator requests a specific kind of information that is alleged to have illegal attributes. In *Woodhull v. Meinel*,[40] for example, the defendant asked a student-run newspaper for any information it had about the plaintiff that she "disliked." The plaintiff sued, claiming that the information provided was defamatory. Though the request itself would not seem to require an illegal response, the only content that fit its description had an illegal quality. In such cases, it may be difficult to determine whether the defendant solicited the content for its legal properties or for its illegal properties.

Finally, as courts often conduct an inquiry into the motivation behind the request, liability under a solicitation standard appears to require an illegal intent.[41] This intent might be inferred from the

---

[38] *See, e.g.*, Dart v. Craigslist, Inc., 665 F. Supp. 2d 961, 968 (N.D. Ill. 2009) ("The phrase 'adult,' even in conjunction with 'services,' is not unlawful it itself nor does it necessarily call for unlawful content."). *See also* Joyner v. Lazzareschi, 2009 WL 695539, at *5 (Cal. Ct. App. March 18, 2009) (finding that a defendant who created titles for discussion threads on a message board did not "develop" any defamatory postings because "[p]resumably, positive messages about plaintiff or messages defending him could be and were posted under the foregoing, general thread headings.").

[39] Examples of cases referencing this type of scenario include *Atlantic Recording Corp. v. Project Playlist, Inc.*, 603 F. Supp. 2d 690 (S.D.N.Y. 2009), *Dart v. Craigslist, Inc.*, 665 F. Supp. 2d 961 (N.D. Ill. 2009), *Goddard v. Google, Inc.*, 640 F. Supp. 2d 1193 (N.D. Cal. 2009), and *Doe II v. MySpace, Inc.*, 96 Cal. Rptr. 3d 148 (Cal. Ct. App. 2009).

[40] Woodhull v. Meinel, 202 P.3d 126 (N.M. Ct. App. 2008).

[41] For a discussion of this intentionality requirement in the *FTC v. Accusearch Inc.* trial court opinion, see Recent Cases, *Federal District Court Denies § 230 Immunity to Website that Solicits Illicit Content:* FTC v. Accusearch, Inc., 121 HARV. L. REV. 2246 (2008). The author proposes a mens rea-based exception to CDA immunity.

nature of the defendant's operations or from the manner in which the defendant uses the content.[42] In *Woodhull*, the court found it relevant that the stated purpose of the defendant's Web site was "to make fun of" the plaintiff, suggesting that the information had been solicited for its defamatory character.[43] Such inferences connect the defendant's actions to the illicit nature of the content, the key element introduced by *Roommates.com*.

B. A Possible Example from the Tenth Circuit: FTC v. Accusearch

A recent case out of the Tenth Circuit provides an example of how a defendant might lose immunity under a solicitation-based approach. In *Federal Trade Commission v. Accusearch Inc.*,[44] the defendant sold private telephone records through its Web site, Abika.com.[45] After a customer placed an order, Accusearch would hire third-party researchers to locate the information and would post the results to the customer's online account in violation of the Telecommunications Act.[46] Although Accusearch was aware that the records were obtained illegally, it claimed immunity under § 230.[47]

In an opinion that largely mirrors *Roommates.com*, the Tenth Circuit determined that Accusearch was responsible for the "development" of the records that it supplied to customers, rendering it a content provider under § 230(f)(3). The court construed the word "develop" to mean "the act of drawing something out, making it

---

[42] In *Roommates.com*, the Ninth Circuit noted that "Roommate both elicits the allegedly illegal content and makes aggressive use of it in conducting its business." Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157, 1172 (9th Cir. 2008). For further discussion of how the purposes and uses of the defendant's Web site influenced the Ninth Circuit's decision, see Varty Defterderian, Note, Fair Housing Council v. Roommates.com: *A New Path for Section 230 Immunity*, 24 BERKELEY TECH. L.J. 563 (2009).

[43] Woodhull v. Meinel, 202 P.3d 126, 129 (N.M. Ct. App. 2008).

[44] Fed. Trade Comm'n v. Accusearch Inc., 570 F.3d 1187 (10th Cir. 2009).

[45] *Id.* at 1191-92.

[46] *Id.*

[47] *Id.* at 1199.

'visible,' 'active,' or 'useable'"[48] and stated that a service provider is "responsible" for the development of offensive content "only if it in some way specifically encourages development of what is offensive about the content."[49] According to the court, Accusearch did exactly that when it exposed the confidential telephone records to public view on Abika.com.[50] Even though the content itself was provided by third-party researchers, Accusearch could not claim § 230 immunity.

Two aspects of the Tenth Circuit's analysis are particularly significant. First, the court distinguishes its earlier decision in *Ben Ezra, Weinstein, & Co. v. America Online Inc.*,[51] where a publicly traded corporation sued America Online for posting inaccurate information about its stock, information that America Online had purchased from a third-party vendor. The court points out that the offending content in *Ben Ezra* had been "erroneous stock quotations and, unsurprisingly, America Online did not solicit the errors."[52] The critical factor in *Accusearch* thus appears to be the defendant's solicitation of the confidential telephone records. Second, the court asserts that "Accusearch's responsibility is more pronounced than that of Roommates.com. Roommates.com may have encouraged users to post offending content; but the offensive postings were Accusearch's *raison d'etre* and it affirmatively solicited them."[53] Thus, the *Accusearch* court believed it was applying the underlying illegality test more narrowly than the Ninth Circuit did in *Roommates.com*. Its characterization of the *Roommates.com* scenario focused on the fact that the defendant's conduct in that case represents the minimum level of "development" that will remove § 230 immunity.

---

[48] *Id.* at 1198.

[49] *Id.* at 1199.

[50] *Id.*

[51] Ben Ezra, Weinstein, & Co. v. Am. Online Inc., 206 F.3d 980 (10th Cir. 2000).

[52] *Accusearch*, 570 F.3d at 1199.

[53] *Id.* at 1200.

V. THE INDUCEMENT APPROACH

Most of the § 230 cases decided since *Roommates.com* seem to fit within the general framework of a solicitation-based standard. At least one case, however, has taken a markedly different approach. In *NPS LLC v. StubHub, Inc.*,[54] a Massachusetts district court applied a much broader interpretation of *Roommates.com* that would deny immunity to those whose actions appear to have "induced" the creation or development of illegal content. This "inducement" does not require an actual request and can occur even when third parties retain unfettered discretion over the nature of the content. Though the exact contours of the theory are far from clear, liability under an inducement standard is based on a vague determination that the defendant's actions influenced a third party's decision to post illegal content.[55]

A. *Evidence of a Broader Interpretation: NPS v. StubHub*

In *NPS v. StubHub*, the New England Patriots brought suit against StubHub alleging tortious interference with its contractual relationships with season ticket holders.[56] StubHub operated a Web site that allowed users to buy and sell tickets to sporting, concert, theater, and other live entertainment events.[57] Although Patriots tickets were non-transferrable and the organization prohibited unauthorized exchanges, many ticket holders chose to sell their tickets through the defendant's Web site, often at prices greatly exceeding face value.[58] StubHub did not buy or sell tickets directly but it did profit from the transactions, charging a 15% commission to the seller and 10% to the buyer.[59]

---

[54] NPS LLC v. StubHub, Inc., 2009 WL 995483 (Mass. Dist. Ct. Jan. 26, 2009).

[55] *See, e.g.* Zac Locke, *Asking for It: A Grokster-Based Approach to Internet Sites That Distribute Offensive Content*, 18 SETON HALL J. SPORTS & ENT. L. 151 (2008) (discussing how the *Grokster* inducement test might be applied in § 230 cases).

[56] NPS LLC v. StubHub, Inc., 2009 WL 995483 at *4.

[57] *Id.* at *2.

[58] *Id.*

[59] *Id.*

StubHub also facilitated these ticket sales in a number of ways. For instance, it offered a limited guarantee against voided tickets.[60] It also created a special category of sellers, called "LargeSellers," for those who purchased large quantities of tickets and later resold them at a profit.[61] StubHub allowed these users to purchase tickets without the normal 10% fee and also urged them to "check the website from time to time for underpriced tickets or exclusive listings that may not be seen elsewhere."[62] StubHub even allowed these users to "mask" the ticket location by listing a seat up to five rows away, making it impossible for the Patriots to determine, based solely on the listings, which ticket holders were selling their tickets.[63]

The effect of these measures was to increase the asking price for each ticket, resulting in larger commissions.[64] By taking advantage of these features, however, LargeSellers almost invariably ran afoul of a Massachusetts anti-scalping law, which generally forbade the reselling of tickets at above face value.[65] Hence, listings with inflated ticket prices constituted illegal third-party content, which, according to the Patriots, satisfied the "improper means" element of its tortious interference claim.[66] StubHub countered with a § 230 defense.[67]

Applying the rule from *Roommates.com* without discussion, the court states that "the same evidence of knowing participation . . . sufficient . . . to establish improper means is also sufficient" to deny immunity.[68] As stated earlier in the opinion, improper means could be shown if StubHub either intentionally induced or encouraged others to violate the anti-scalping law, or profited from such violations while declining to stop or limit them,[69] a direct reference to the *Grokster*[70]

---

[60] *Id.*

[61] *Id.* at *3.

[62] *Id.*

[63] *Id.*

[64] *Id.* at *11.

[65] MASS. GEN. LAWS ANN. ch. 140, §§185A, 185D (West 2002).

[66] NPS LLC v. StubHub, Inc., 2009 WL 995483, at *10 (Mass. Dist. Ct. Jan. 26, 2009).

[67] *Id.* at *12.

[68] *Id.*

[69] *Id.* at *10.

standards for contributory infringement[71] and vicarious infringement, respectively.

According to the court, StubHub "intentionally induced or encouraged" LargeSellers to violate the anti-scalping law when it "strongly urged" them to check the Web site for underpriced tickets and offered to waive the 10% fee.[72] By virtue of its commission system, StubHub also profited when tickets were sold for more than face value, and it declined to stop or limit this activity because it did not require sellers to list the face value of the ticket, making it impossible to know whether the law was being violated.[73]

These actions were enough to take StubHub outside the scope of § 230. Because the opinion itself only purports to decide the immunity issue based on the "same evidence," and not necessarily the same standard, as the improper means issue, one cannot conclusively say that *Grokster* is responsible for the result. Based on the facts alone, however, the court's interpretation of the underlying illegality test is a clear departure from the prior narrow interpretations of *Roommates.com*.

While the *StubHub* decision itself may not carry much precedential weight, it could be a preview of how the underlying illegality test will be applied by courts eager to establish limits on § 230 immunity.[74] The

---

[70] Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 545 U.S. 913 (2005).

[71] "[O]ne who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties." *Id.* at 936-937. For a discussion on the impact such a standard would have on § 230 jurisprudence, see Varty Defterderian, Note, Fair Housing Council v. Roommates.com: *A New Path for Section 230 Immunity*, 24 BERKELEY TECH. L.J. 563 (2009).

[72] NPS LLC v. StubHub, Inc., 2009 WL 995483, at *11 (Mass. Dist. Ct. Jan. 26, 2009).

[73] *Id.* at *11. It is worth noting that StubHub displayed the text of the Massachusetts anti-scalping law on its "Q & A" page. *See Id.* at *2.

[74] An inducement-based approach appears in another case as well, though not as an interpretation of the *Roommates.com* exception. In *People v. Gourlay*, 2009 WL 529216 (Mich. Ct. App. March 3, 2009), a criminal defendant was convicted for his role in providing Web hosting services as well as "artistic assistance" to a minor who had created a Web site to broadcast pornographic images of himself over the

Seventh Circuit in particular has shown some hostility toward expansive readings of the statute and its decision in *Chicago Lawyers' Committee v. Craigslist*[75] even indicates that *Grokster* would apply in the context of § 230 as well.[76] The inducement standard would represent a natural extension of this theory. Furthermore, the Ninth Circuit itself is gaining a reputation for its willingness to deny § 230 protection. If called upon to clarify its holding in *Roommates.com*, the court may be inclined to follow an inducement-based approach.

B. Distinguishing Inducement from Solicitation

As is readily apparent from the *StubHub* case, inducement differs from solicitation in at least two important respects: it requires no explicit request and can occur even when users have been given the option of posting legal content.

First, a Web site operator can be liable under an inducement standard without making any explicit statements or requests. StubHub never requested that its users increase the price of the tickets they sold; indeed, the Web site's user agreement expressly required sellers to comply with all applicable laws when setting their prices.[77] The second key difference is that, under inducement, a Web site operator can still be considered a "developer" of user-generated content even if users have the option of posting legal content. In *StubHub*, the Web site had

---

Internet. The defendant appealed, arguing that 47 U.S.C. § 230 preempted his conviction because he had not created or developed the pornographic content. In dismissing this claim, the court noted that the offense required proof that he had "persuade[d], induce[d], entice[d], coerce[d], cause[d], or knowingly allowe[d]" a child to engage in a sexually abusive activity. *Id.* at *4. Because of this, the court concluded, a defendant who has committed the offense has necessarily placed himself outside the scope of § 230 immunity. *Id.* at *5. Though based on a Michigan criminal statute, MICH. COMP. LAWS ANN. § 750.145c(2) (West 2004), the analysis in *Gourlay* would seem to permit a loss of immunity even in cases of "persuasion," a far cry from the rigorous requirements of the solicitation theory.

[75] Chicago Lawyer's Comm. For Civil Rights Under Law, Inc., v. Craigslist, Inc., 519 F.3d 666 (7th Cir. 2008).

[76] *Id.* at 670.

[77] NPS LLC v. StubHub, Inc., 2009 WL 995483, at *11 (Mass. Dist. Ct. Jan. 26, 2009).

"developed" the illegal ticket prices even though its users remained entirely free to engage in legitimate ticket sales.

These two features demonstrate the relatively tenuous causal relationship capable of triggering liability under an inducement standard. Because of these differences, the inducement standard carves out a much larger exception to the protections available under § 230.

C. Key Considerations Under an Inducement Standard

When evaluating claims under an inducement standard, a court might focus on the specific actions of a defendant, the intent behind those actions, and the influence they exert on a third-party's decision to produce illegal content. There must some cognizable act by the defendant to support a denial of immunity, but this act need not be an actual request for unlawful content. [78] A plaintiff would also need to demonstrate that the act was driven by an illegal intent.[79] This intent can be inferred from context, particularly when a Web site's revenue depends on the particular choices that its users make. [80]

Perhaps most importantly, the defendant's actions must in some way influence a third party's decision to develop content that is unlawful. Although the discussion in *StubHub* offers little guidance on this point, the facts of the case help to identify three categories of behavior that may be problematic. The first involves creating financial incentives for others to produce illegal material,[81] such as the special

---

[78] *See, e.g.*, Universal Commc'n Sys., Inc. v. Lycos, Inc., 478 F.3d 413, 421 (1st Cir. 2007) ("Even assuming arguendo that active inducement could negate Section 230 immunity, it is clear that UCS has not alleged any acts by Lycos that come even close to constituting the 'clear expression or other affirmative steps taken to foster' unlawful activity that would be necessary to find active inducement.") (citing Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 545 U.S. 913, 914 (2005)).

[79] People v. Gourlay, 2009 WL 529216, at *4 (Mich. Ct. App. March 3, 2009) ("[W]hen a person persuades, induces, entices, or coerces another, the person is actively and intentionally attempting to bring about a particular action or result.").

[80] Hattie Harman, *Drop-Down Lists and the Communication Decency Act: A Creation Conundrum*, 43 IND. L. REV. 143, 172-173 (2009).

[81] *See, e.g.,* Dart v. Craigslist, Inc., 665 F. Supp. 2d 961, 966 (N.D. Ill. 2009) ("Nothing in the service craigslist offers induces anyone to post any particular listing or express a preference for discrimination; for example, craigslist does not offer a

discount given to LargeSellers in *StubHub*. Another category involves reducing the risk of detection for users who commit illegal acts. Although not specifically mentioned in the court's analysis, the ability of StubHub users to "mask" the location of their seats would fall under this category. Other examples may include guarantees of anonymity offered by "repu-taint" Web sites.[82] A third category covers instances where a Web site operator provides suggestions or examples of illegal content for its users to emulate,[83] although it is unclear whether this alone could sufficiently influence a user's behavior. *StubHub* may offer an example from this category as well, as the court found it significant that the defendant had "strongly urged" LargeSellers to check the listings for underpriced tickets. Beyond these general observations, however, the contours of an inducement standard remain unclear.

CONCLUSION

Cases decided in the wake of *Roomates.com* seem to reflect two different standards for determining when the "underlying illegality" test is satisfied. Most courts apply a "solicitation" standard, requiring the Web site operator to explicitly request the offending material. This request must be specific enough that compliance with its terms would almost necessarily entail providing illegal content. An "inducement" standard, on the other hand, could deprive a Web site operator of immunity even when its users retain a significant degree of control over the illicit nature of the posted content. Inducement describes conduct that influences a third party's decision to develop illegal material, either by creating financial incentives, reducing the risk of detection, or perhaps offering examples for third parties to emulate. Liability will not attach under either standard however, unless the

---

lower price to people who include discriminatory statements in their postings.") (citing Chicago Lawyer's Comm. For Civil Rights Under Law, Inc., v. Craigslist, Inc., 519 F.3d 666, 671-72 (7th Cir. 2008)).

[82] *See* Patricia Sánchez Abril , *Repu-Taint Sites and the Limits of § 230 Immunity*, J. INTERNET L., Jan. 2009, at 3 (explaining that a "repu-taint" Web site is one that encourages users to post sensitive information about others without regard for the disclosure's veracity or consequences.).

[83] *Id.*

defendant harbored an illegal intent, which often must be inferred from context. Despite indications that some courts might be willing to adopt a broader interpretation of *Roommates.com*, the weight of authority continues to support strong protections for Web site operators.

PRACTICE POINTERS

- Regardless of how broadly a court may interpret the *Roommates.com* exception, a plaintiff will still need to establish that the Web site operator intended for its users to produce unlawful content and that it took specific action to bring about that result.
- Under a narrower "solicitation" standard, defendants will generally be entitled to § 230 immunity unless their actions amount to an explicit request that is specifically limited to illegal material.
- Under a broader "inducement"-type standard, a plaintiff may be able to overcome a § 230 defense by merely showing that the defendant's actions in some way influenced a third party's decision to produce illegal content.
- To reduce exposure, Web site operators should examine their fee structures or pricing policies to ensure that they do not create financial incentives for unlawful behavior. Any sample content or recommendations to users should be removed if they might tend to suggest an illegal course of action.

WASHINGTON JOURNAL OF LAW, TECHNOLOGY & ARTS
VOLUME 6, ISSUE 2 AUTUMN 2010

LOCATION SURVEILLANCE BY GPS: BALANCING AN EMPLOYER'S BUSINESS INTEREST WITH EMPLOYEE PRIVACY

Kendra Rosenberg[*]

CITE AS: 6 WASH J.L. TECH. & ARTS 143 (2010)
https://digital.lib.washington.edu/dspace-law/handle/1773.1/479

ABSTRACT

Employers are increasingly using GPS tracking devices as business tools to monitor employee movements. Recent judicial decisions have found an employer's interest in using location surveillance on employer-owned property generally trumps an employee's privacy interests. However, employers deciding to use GPS should be aware of the potential limitations on tracking an employee based on state constitutional, statutory, and common law rights to privacy. This Article focuses on the permissible scope of an employer's use of GPS to track employees in the workplace.

TABLE OF CONTENTS

---

[*] Kendra Rosenberg, University of Washington School of Law, Class of 2011. Thank you to Professor Jane Winn of the University of Washington School of Law; Peter Winn, Assistant U.S. Attorney, US Department of Justice; and student article editor Jennifer Heidt White.

INTRODUCTION

Employers are beginning to use Global Positioning System ("GPS") navigation devices more frequently as a practical tool to monitor employees' locations. This increased use of GPS has, however, also increased tensions between employers and their employees, as employers' property rights clash with employees' rights to privacy.[1] This tension has come to a head in the form of lawsuits, such as the New York Taxi Workers Alliance's suit in 2007 to enjoin the city from requiring GPS installation in all licensed city cabs.[2]

Since no federal or state law currently restricts the use of GPS in employer-owned vehicles, many employees have sought legal recourse in constitutional and statutory privacy rights and common law protections. Although no lawsuit challenging an employer's use of GPS has been successful, this Article provides useful guidance about how employers may avoid such litigation. First, this Article discusses the current use of GPS technology in an effort to explore how this type of litigation arises. Next, this Article explores the different causes of action pursued by employees to date, including alleged violations of state constitutional, statutory and common law rights to privacy, and claims of federal discrimination. Finally, this Article offers practice pointers to employers seeking to use GPS technology in the workplace.

I. LOCATION SURVEILLANCE IN THE WORKPLACE

GPS devices use a satellite-based electronic system that reveals the

---

[1] *See generally* National Workrights Institute, On Your Tracks: GPS Tracking in the Workplace 5-7 (2004), http://epic.org/privacy/workplace/gps-traking.pdf.

[2] Alexandre v. N.Y.C. Taxi & Limousine Comm'n, No. 07 CV 8175(RMB), 2007 WL 2826952, at *1 (S.D.N.Y. Sept. 28, 2007) (denying plaintiff's request for a preliminary injunction).

location of objects or individuals in real-time.[3] On a vehicle, GPS technology can be used to remotely monitor vehicle movements, speed, and precise location.[4] Location information is sent live through a receiver for real-time tracking updates or is stored in the GPS unit for later use and delivery to a server for monitoring.[5]

Many public entities have started using GPS in public employer-owned vehicles after citing the need to monitor the quality of performance and to increase employee efficiency.[6] For example, the city of Oakland, California installed GPS trackers on vehicles in response to complaints about unsatisfactory street sweeping.[7] Similarly, King County, Washington installed GPS equipment on solid waste trailers to maximize the efficient use of the equipment.[8] Public schools are also using GPS to track the location of school buses, citing the need to monitor bus drivers and bus routes, speeds, and idling times.[9]

Private employers also use GPS on employer-owned delivery vehicles to increase productivity, improve customer service, reduce labor costs, and promote responsible behavior among employees.[10] By using GPS, employers can receive real-time information about vehicle locations to help deal with customers' complaints and potentially lower costs by efficiently coordinating delivery fleets. Employees can use GPS to get directions and coordinate delivery routes according to the

---

[3] William A. Herbert, *The Impact of Emerging Technologies in the Workplace: Who's Watching the Man (Who's Watching Me?)*, 25 HOFSTRA LAB. & EMP. L.J. 355, 370 (2008).

[4] Sarah Rahter, Note, *Privacy Implications of GPS Tracking Technology*, 4 I/S: J.L. & POL'Y FOR INFO. SOC'Y 755, 756-58 (2008).

[5] John E. Woodard, *Oops, My GPS Made Me Do It! GPS Manufacturer Liability Under a Strict Liability Paradigm When GPS Fails to Give Accurate Directions to GPS End-Users*, 34 U. DAYTON L. REV. 429, 440 (2009).

[6] *See, e.g.*, National Workrights Institute, *supra* note 1, at 12.

[7] *See id.* at 11.

[8] *See, e.g.*, Teamsters Local 174 v. King County., No. 9204-PECB, 2006 WL 272493 (Wash. Pub. Emp. Rel. Comm'n Jan. 12, 2006) (regarding union opposition to GPS installation in Solid Waste Division vehicles).

[9] Clare Jensen, *Tacoma School Buses Modernize With GPS Units*, TACOMA WEEKLY, Sept. 30, 2009, *available at* http://www.tacomaweekly.com/article/3590/.

[10] *Bosses Keep Sharp Eye on Mobile Workers*, MSNBC, (Dec. 30, 2004, 12:56 PM), http://www.msnbc.msn.com/id/6769377/.

availability of vehicles and traffic patterns.

Employees bringing lawsuits against employers for using GPS in the workplace have sought recourse through both state and federal causes of action.[11] Recent judicial decisions suggest that claims by employees asserting state constitutional, statutory, and common law privacy violations are increasing. Because the use of GPS in the workplace has yet to be addressed in many jurisdictions, it is important for employers to consider potentially applicable federal and state laws that may regulate the location surveillance of individuals generally.

II. VIOLATION OF PRIVACY CLAIMS

The privacy implications of GPS use frequently arise in litigation related to law enforcement using location tracking devices to monitor suspects. Courts considering an employer's use of GPS have repeatedly referred to the scope of an individuals' expectation of privacy as defined through the criminal case precedent in jurisdictions that do not regulate the tracking of an individual's movements. Thus, employers could determine what constitutes a "reasonable expectation of privacy" by looking to Fourth Amendment precedent and state law regarding constitutional and statutory employee privacy protections.

A. *The History of GPS Litigation in the Criminal Context: State and Federal Constitutional Protections*

Although the United States Supreme Court has not yet decided whether the use of GPS to track an individual implicates constitutional rights or privacy interests, the Court has addressed the issue with other tracking technologies. For example, the Supreme Court held in *United States v. Knotts*,[12] that police did not violate a suspect's Fourth Amendment rights when they monitored the signal from a tracking device installed in a chemical container being transported by the

---

[11] *See, e.g.*, Gerardi v. City of Bridgeport, 985 A.2d 328, 335 (Conn. 2010); Elgin v. St. Louis Coca-Cola Bottling Co., No. 4:05CV970-DJS, 2005 WL 3050633 (E.D. Mo. Nov. 14, 2005); State v. Jackson, 76 P.3d 217 (Wash. 2003).

[12] United States v. Knotts, 460 U.S. 276 (1983).

defendant. The Court held that monitoring the beeper signal, while the automobile transported the can, did not invade the individual's legitimate expectation of privacy because it revealed information that could have been obtained through visual surveillance. Therefore, it did not constitute a search or a seizure.[13] This holding suggests GPS surveillance during criminal investigations could be lawful if the information obtained could also be gathered from visual surveillance.

In *United States v. Karo,* the Supreme Court affirmed *Knotts*, but narrowly held the monitoring of a beeper in a private residence, a location not open to visual surveillance, violates the Fourth Amendment rights to a justifiable interest in the privacy of one's residence.[14] In *Karo,* Drug Enforcement Administration agents installed a beeper to monitor the location of a can of ether after an informant told agents the ether would be used to extract cocaine from clothing. The agents monitored the beeper signal as the suspects moved the can between residences and commercial storage facilities. The Court held that a private residence is a place in which the individual normally expects privacy and monitoring the electronic device revealed information that could not have been visually verified.[15]

State courts, relying on *Knotts* and *Karo*, have applied state constitutional privacy protections in GPS tracking cases. In *State v. Jackson*, for example, the Washington Supreme Court held that installation of the GPS on a vehicle for surveillance purposes violated the state constitutional right to be free from unreasonable search and seizure.[16] The Court noted in dicta that GPS had a capacity to gather large amounts of long-term personal data:

> [T]he intrusion into private affairs made possible with a GPS device is quite extensive as the information obtained can disclose a great deal about an individual's life. . . . In this age, vehicles are used to take people to a vast number of places that can reveal preferences,

---

[13] *Knotts*, 460 U.S. at 284-85.

[14] United States v. Karo, 468 U.S. 705, 714 (1984).

[15] *Karo*, 468 U.S. at 715.

[16] 76 P.3d 217, 264 (Wash. 2003).

alignments, associations, personal ails and foibles.[17]

The Supreme Judicial Court of Massachusetts also held that the installation of GPS on the defendant's vehicle by police constituted a seizure because operation of the GPS required power from the vehicle's electrical system; therefore, it was an ongoing physical intrusion.[18] In New York state court, a trial judge found a search unlawful because the GPS was placed on the defendant's vehicle by police and used to track the defendant's movements over a 65-day period, noting that a ride in a motor vehicle "does not so completely deprive its occupants of any reasonable expectation of privacy."[19] Despite these examples, whether or not the use of GPS technology reveals private information that invades a protected privacy interest as a matter of law is not settled in most jurisdictions.

Courts have looked to the Supreme Court precedent in *Knotts* and *Karo* when deciding the scope of an individual's expectation of privacy.[20] Because the criminal law precedent principally examines whether the location being monitored is open to visual surveillance when determining a justifiable privacy interest, employees operating a vehicle in the public view may not have a privacy interest in an automobile. States that provide for an employee's right to privacy may grant greater protections to employees, in addition to common law recognition of torts of unreasonable intrusion upon seclusion and invasion of privacy.

B. Claimed Violations of State-Provided Rights to Privacy

In addition to the Fourth Amendment protection against unreasonable searches and seizures, many states also provide employees with state statutory protections against violations of privacy by their

---

[17] *Id.* at 262.

[18] Commonwealth v. Connolly, 913 N.E. 2d 356, 369 (Mass. 2009).

[19] People v. Weaver, 909 N.E.2d 1195, 1200 (N.Y. 2009).

[20] CLIFFORD S. FISHMAN & ANNE T. MCKENNA, WIRETAPPING AND EAVESDROPPING: SURVEILLANCE IN THE INTERNET AGE § 29:37 (3d. ed. 2008) ("the federal circuits courts to have addressed (*sic.*) the issue have applied the *Knotts/Karo* line of reasoning and rationale to GPS cases").

employers.[21] Two states lead in the regulation of tracking devices: California and Connecticut. These two states exemplify the challenge faced by state courts and state legislatures in dealing with emerging tracking technology. In California it is a misdemeanor to use an electronic tracking device to determine the location or movement of a person without his or her consent.[22] In Connecticut, the state legislature statutorily prohibits any employer from electronically monitoring an employee's activities without prior notice to all employees who may be affected.[23]

The Supreme Court of Connecticut in *Girardi v. City of Bridgeport* interpreted the Connecticut statute prohibiting an employer from electronically monitoring an employee's activities without prior notice, holding the statute did not create a private right of action.[24] The employer, the City of Bridgeport, had installed the GPS in a city-owned vehicle. The plaintiff operated the vehicle as part of his job as a fire inspector for the city.[25] The plaintiff claimed the City violated the Connecticut electronic monitoring statute when information gained through the GPS device, without the plaintiff's knowledge, was used to discipline the plaintiff for poor job performance.[26] The Supreme Court of Connecticut held the statute does not entitle an employee to any specific relief or remedy.[27] Therefore, the only enforcement mechanism for claimed violations of the Connecticut electronic monitoring statute

---

[21] *See, e.g.*, CAL. PENAL CODE § 637.7 (West. 2009) (electronic tracking of a person's location violates a person's reasonable expectation of privacy); CONN. GEN. STAT. § 31-48d (2003) (requiring every employer engaging in any type of electronic monitoring to give notice to all employees who may be affected by the monitoring); *see also* H.B. 16, 150th Gen. Assemb., Reg. Sess. (Ga. 2009) (amending GA. CODE ANN. § 16-11-62.1, to read that "no person shall use a electronic tracking device to determine the location or movement of another person without such other person's consent"). *Cf.* DEL. CODE ANN. tit. 11. §1335(a) (2007) (crime to knowingly install location tracking device in motor vehicle without consent of owner, lessor or lessee of vehicle).

[22] *See, e.g.,* CAL. PENAL CODE § 637.7 (West. 2009).

[23] CONN. GEN. STAT. § 31-48d (2003).

[24] Gerardi v. City of Bridgeport, 985 A.2d 328, 335 (Conn. 2010).

[25] *Gerardi*, 985 A.2d at 335.

[26] *Id.*

[27] *Id.*

is limited to proceedings before the state labor commissioner; employees do not have the right to bring a civil action under the statute.

The Superior Court of Connecticut in *Girardi* reached both the issue of administrative exhaustion and the plaintiff's substantive claim that the City violated the state electronic monitoring statute.[28] The court looked to the criminal law precedent set out in *Karo* and found the City did not violate the employee's expectation of privacy. The monitoring of the GPS device did not reveal information that could not be obtained through visual surveillance of the public roads. As the lower court in *Girardi* demonstrates, courts are likely to draw on Fourth Amendment standards for privacy protections in the employment context. An employee may have a judicially cognizable claim if the information gained by the GPS device reveals personal information not in the public view.

C. *Common Law Torts of Unreasonable Intrusion and Invasion of Privacy*

Due to the lack of statutory regulation of GPS by the federal government and most states, plaintiffs may seek remedy for an invasion of an employee's privacy under the common law tort of unreasonable intrusion upon the seclusion of another.[29] Tort claims for an invasion of privacy require the plaintiff meet an objective standard by showing the intrusion would be highly offensive to a reasonable person.[30] Precedent illustrates that employees will struggle to meet this burden of showing objective offensiveness caused by an employer installing a GPS device in an employer-owned vehicle.

In *Elgin v. St. Louis Coca-Cola Bottling Co.*,[31] for example, the plaintiff sued his employer for the tort of intrusion upon seclusion for placing a GPS tracking device in one of the employer's company

---

[28] Gerardi v. City of Bridgeport, No. CV080423011S, 2007 WL 4755007 (Conn. Super. Ct. 2007), *aff'd on other grounds*, 985 A.2d 328 (Conn. 2010).

[29] RESTATEMENT (SECOND) OF TORTS § 652B (1977).

[30] *Id.*

[31] Elgin v. St. Louis Coca-Cola Bottling Co., No. 4:05CV970-DJS, 2005 WL 3050633 (E.D. Mo. Nov. 14, 2005).

vehicles.[32] The federal district court concluded an individual's privacy claim as to an automobile's path of travel was limited.[33] Here, the plaintiff did not consent to the placement of the GPS tracking device, nor did he know about its attachment to the vehicle until after it had been used during a workplace investigation of cash shortages from vending machines.[34] The employer tracked the employer-owned vehicle assigned to the plaintiff during both working and non-working hours.[35] The court found "use of the tracking device on defendant's company car, even though it was assigned to plaintiff, does not constitute a substantial intrusion upon plaintiff's seclusion, as it revealed no more than highly public information as to the van's location."[36] Because the common law tort of intrusion upon seclusion is limited to actions that intrude unreasonably into the individual's expectation of privacy and does not extend to activities that are public, the plaintiff failed to demonstrate the substantial intrusion necessary to be successful on the action.[37] The court granted summary judgment in the defendant's favor.

On similar facts, in *Tubbs v. Wynne Transportation Services* a federal district court found no unreasonable intrusion by the employer.[38] Tubbs sued his former employer, Wynne Transport Service Inc. ("Wynne") for defamation, invasion of privacy, false arrest, false imprisonment, malicious prosecution and race discrimination.[39] The federal judge granted Wynne's motion for summary judgment on the tort claim of invasion of privacy finding that Tubbs, who drove employer-owned trucks that were each outfitted with a GPS device that

---

[32] The plaintiff also sued the defendant for discrimination in violation of the Missouri Human Rights Act. The court granted the defendant's motion for summary judgment as to that claim. *Elgin,* 2005 WL 3050633, at *3.

[33] *Elgin*, 2005 WL 3050633, at *4 (quoting United States v. Knotts, 460 U.S. 276, 281 (1983)).

[34] *Id.* at *1.

[35] *Id.*

[36] *Id.* at *4.

[37] *Id.*

[38] Tubbs v. Wynee Transp. Servs. Inc., No. H-06-0360, 2007 WL 1189640, at *10 (S.D. Tex. Apr. 19, 2007).

[39] *Id.* at *1.

transmitted the truck's location to the company, failed to meet the objective standard of showing an unreasonable intrusion under these facts.[40]

Thus, courts that have considered the issue have concluded that an employer may install a GPS device in an employer-owned vehicle.

III. USING GPS IN THE WORKPLACE

Although no challenge to an employer's use of GPS has been successful in court, it remains good business practice for employers to implement written policies defining the use of GPS.[41] Both public and private employers who want to employ a GPS device in the workplace may consider several possible responses such as developing a policy for electronic monitoring or giving employees prior notice of the GPS use.

Employers that choose to use GPS should determine whether the jurisdiction has statutory protections against the use of electronic tracking devices. Even without statutory prohibitions against tracking, employers should be cautious of state constitutional protections of an employee's privacy if the information obtained reveals personal information unrelated to employment.

An employer intercepting electronic communications may want to provide actual notice to employees that the tracking device is monitoring the employer-owned vehicle to encourage better compliance with company policy. Further, an employee's knowledge of the GPS monitoring may establish notice of the privacy invasion in the event of litigation. In *Brantley v. Muscogee County School District*, the court highlighted the employer's written policy for all employer-owned vans to have GPS installed, and the plaintiff's knowledge of this plan, in finding that there was no objectively reasonable belief that the GPS was installed discriminatorily.[42] A clear written employment policy

---

[40] *Id.*

[41] *Cf.* TBG Ins. Services Corp v. Superior Court, 117 Cal. Rptr. 2d 155, 161 (Cal. Ct. App. 2002) (holding an employer's written electronic and computer use policy gave advance notice to the employee and the employee's written consent to the policy defeated the employee's claim to a reasonable expectation of privacy).

[42] Brantley v. Muscogee Cnty. Sch. Dist., No. 4:06-CV-89, 2008 WL 794778, at *10 (M.D. Ga. March 20, 2008) (court found GPS was not installed in a discrimatory

regarding location surveillance may encourage employee compliance with employer rules and procedures.

In addition, employers that provide actual notice to employees prior to the installation of tracking devices may be able to prevent employee claims of a subjective privacy interest. Even though private employers are not subject to the same Fourth Amendment limitations as public employers, the case law has referred to Fourth Amendment protections when deciding the scope of an individual's expectation of privacy.[43] Employers who provide notice to employees of the GPS monitoring can seek employee compliance with policies while also putting the employees on notice that there is no expectation of privacy in the location of the employer-owned vehicle.

CONCLUSION

Recent judicial decisions have found an employer's interest in employer-owned property generally trumps employee privacy interests regarding location surveillance. Employees seeking to limit employers' use of GPS have brought various causes of action including alleged violations of state constitutional, statutory, and common law rights to privacy, and claims of federal discrimination. Although no employee challenging an employer's use of GPS has been successful in litigation, the increased use of GPS in the employment setting is likely to lead to disagreements about the privacy of employees. Additional states may begin regulating the use of GPS as these devices become more popular as a business tool to gather information about employees' movement. Because there is currently no direct federal regulation of GPS surveillance, employers should carefully plan implementation of GPS, should they choose to use it, according to the legal requirements in the states where they operate.

---

manner and the employer did not violate Title VII of the Civil Rights Act of 1965).

[43] *See, e.g.*, Jenn Heidt White, *Text Message Monitoring After* Quon v. Arch Wireless*: What Private Employers Need to Know About the Stored Communications Act and an Employee's Right to Privacy*, 5 SHIDLER J.L. COM. & TECH. 19 (2009).

PRACTICE POINTERS

- Employers should establish the use of GPS as tied to the ordinary course of business by developing a written policy for location surveillance that explains: the (1) purpose of the location surveillance corresponding to the specific needs of the company, (2) type of location data processed (active or passive tracking), (3) duration that location data will be stored, and (4) the individuals or third parties with access to data.
- Employers should consider providing actual notice to employees prior to the installation of the tracking device to encourage employee compliance with employment policies and to put the employee on notice that there is no expectation of privacy in the location of the employer-owned vehicle.
- Employers should be cautious when targeting the installation of GPS tracking devices to a vehicle assigned to an employee who will take the vehicle to his or her private residence.

WASHINGTON JOURNAL OF LAW, TECHNOLOGY & ARTS
VOLUME 6, ISSUE 2 AUTUMN 2010

DEATH OF THE SPAM WRANGLER: CAN-SPAM PRIVATE PLAINTIFFS REQUIRED TO SHOW ACTUAL HARM

Susuk Lim [*]

CITE AS: 6 WASH J.L. TECH. & ARTS 155 (2010)
https://digital.lib.washington.edu/dspace-law/handle/1773.1/480

ABSTRACT

In Gordon v. Virtumundo, the United States Court of Appeals for the Ninth Circuit published its first opinion on private plaintiff standing requirements for actions under the federal CAN-SPAM Act. The court strictly interpreted CAN-SPAM's enforcement language, rejecting attempts by professional litigants to insert themselves into CAN-SPAM's limited private right of action. This Article analyzes Gordon's treatment of CAN-SPAM's private right of action and federal preemption provisions. It concludes by assessing the decision's expected effect on future spam-related litigation.

TABLE OF CONTENTS

---

[*] Susuk Lim, University of Washington School of Law, Class of 2011. Thank you to Professor Anita Ramasastry and student editor Jessica Lee Blye.

INTRODUCTION

The public furor over unsolicited commercial e-mail, known as spam, has fed a cottage industry dedicated to profiting from statutory damages codified in the CAN-SPAM Act of 2003.[1] Uncertainty about the scope of CAN-SPAM's private right of action and limited precedent left courts largely powerless to dismiss such claims without expending significant resources on evaluating their individual merits. In its landmark *Gordon v. Virtumundo* decision, the Ninth Circuit erased many, but not all, of these ambiguities. It derived eligibility from legislative intent and held that CAN-SPAM's private standing requirements should be narrowly construed.[2] The court also held that eligible private plaintiffs must demonstrate actual harm of a specific type and causation.[3] Finally, the court determined that CAN-SPAM's preemption clause was broad, only allowing spam-related litigation under state law if the violation materially and intentionally references the state law at issue and the law itself specifically relates to falsity or deception.[4] *Gordon* largely shuts out professional plaintiffs from CAN-SPAM eligibility. It also modifies the requirements for legitimate claimants, necessitating a change in litigation approach.

I. THE CAN-SPAM ACT OF 2003

Unsolicited bulk and commercial e-mail messages, known as spam, are sent in large quantities to indiscriminate sets of recipients. During the first half of 2009, spam constituted 85.5% of all e-mail traffic.[5]

---

[1] Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act of 2003, 15 U.S.C. §§ 7701-7713 (2006); *See, e.g.*, Mike Masnick, *Serial Anti-Spam Lawsuit Filer Loses Appeal . . . And His Possessions*, TECHDIRT (Aug. 24, 2009, 10:25 AM), http://www.techdirt.com/articles /20090821/0334155954.shtml.

[2] *See* Gordon v. Virtumundo, 575 F.3d 1040, 1051 (9th Cir. 2009).

[3] *See id.* at 1053-54.

[4] *See id.* at 1063.

[5] *Kaspersky - Spam Volume Remained High in H1 2009 Despite Economic Crisis*,

This ever-rising tide of spam has caused public consternation and high business spending toward network and business asset protection.[6] Legislators balanced this public sentiment with the economic and marketing utility of legitimate commercial e-mail when they drafted and subsequently enacted CAN-SPAM in 2003.[7]

CAN-SPAM governs the content, representation, and delivery of commercial e-mail.[8] It does not outlaw unsolicited e-mail outright. Commercial e-mail is only unlawful if it does not allow for verifiable and timely user-initiated unsubscription,[9] contains inaccurate or misleading sender information,[10] or is sent under or through falsified means.[11] CAN-SPAM also limits standing to governmental and regulatory bodies, but provides a limited private right of action to a class of plaintiffs it terms Internet access services ("IASs").[12] The term "Internet access service" is statutorily defined as "a service that enables users to access content, information, electronic mail, or other services offered over the Internet, and may also include access to proprietary content, information, and other services as part of a package of services offered to consumers."[13] In the absence of precedent, this language was sufficiently ambiguous to cause most courts to construe the definition very

---

SPAM FIGHTER (Nov. 9, 2009), http://www.spamfighter.com/News-13076-Kaspersky-%E2%80%93-Spam-Volume-Remained-High-in-H1-2009-Despite-Economic-Crisis.htm

[6] *See* Rebecca Lieb, *Make Spammers Pay Before You Do*, ISP-PLANET (Jul. 31, 2002), http://www.ispplanet.com/business/2002/spam_cost.html.

[7] *See* 15 U.S.C. § 7701 (2006).

[8] *See* 15 U.S.C. § 7702(2) (2006).

[9] 15 U.S.C. § 7704(a)(3)(A)(i) (2006).

[10] 15 U.S.C. § 7704(a)(2) (2006).

[11] *See* 15 U.S.C § 7704(b) (2006).

[12] *See* 15 U.S.C. § 7706(g)(1) (2006).

[13] 47 U.S.C. § 231(e)(4) (2006).

broadly.[14]

IASs are only granted CAN-SPAM standing if they suffer adverse effects as a result of a substantive CAN-SPAM violation.[15] The courts generally construed CAN-SPAM's "adverse effects" language to require a showing of both sufficient extent of harm as well as type of harm generally suffered by IASs.[16] However, the courts broadly refused to require a showing of any connection between specific violations and alleged harm.[17]

The Act provides for statutory damages of up to $100 per violating message[18] and $1,000,000 in aggregate.[19] It allows treble damages for aggregated or willful violations.[20] The Act also preempts related state law that "expressly regulates the use of electronic mail to send commercial messages, except to the extent that [it] prohibits falsity or deception."[21] State laws not specific to electronic mail are saved from preemption, as are laws addressing fraud or computer crime.[22]

Between CAN-SPAM's steep statutory damages, the ease of meeting its standing requirements, and widespread public hatred for spam, it is easy to see how an unscrupulous private plaintiff could make a significant amount of money by manipulating the previous regime.

---

[14] *See, e.g.*, Ferguson v. Quinstreet, No. C07-5378RJB, 2008 WL 3166307, at *5 (W.D. Wash. Aug. 5, 2008) (in the absence of guidance, the term must be given its broadest definition under CAN-SPAM); MySpace v. The Globe.com, No. CV06-3391-RGK(JCx), 2007 WL 1686966, at *3 (C.D. Cal. Feb. 27, 2007) (IAS providers can include any traditional ISP, any e-mail provider, and most Web site owners); Hypertouch v. Kennedy-Western Univ., No. C04-05203SI, 2006 WL 648688, at *3 (N.D. Cal. Mar. 8, 2006) (holding that providing e-mail service alone, without any other services, was sufficient to qualify as an IAS under CAN-SPAM).

[15] *See, e.g.*, *Ferguson*, 2008 WL 3166307; *MySpace*, 2007 WL 1686966, at *3; *Hypertouch*, 2006 WL 648688, at *3.

[16] *See, e.g.*, ASIS Internet Servs. v. Optin Global, No. C-05-05124JCS, 2008 WL 1902217, at *17 (N.D. Cal. Apr. 29, 2008); Brosnan v. Alki Mortgage, No. C074339JL, 2008 WL 413732, at *2 (N.D. Cal. Feb. 13, 2008); *Hypertouch*, 2006 WL 648688, at *4.

[17] *See, e.g., Optin Global*, 2008 WL 1902217, at *5-6.

[18] 15 U.S.C. § 7706(g)(3)(A)(i) (2006).

[19] 15 U.S.C. § 7706(g)(3)(B) (2006).

[20] 15 U.S.C. § 7706(g)(3)(C) (2006).

[21] 15 U.S.C. § 7707(b)(1) (2006).

[22] 15 U.S.C. § 7707(b)(2) (2006).

One CAN-SPAM defendant complained somewhat prophetically that such "a broad interpretation [would] create a flood of suits by 'spam litigation mills.'"[23]

II. THE *GORDON* DECISION

The Ninth Circuit chilled the potential anti-spam litigation industry with its decision in *Gordon*.[24] Appellant James S. Gordon was variously described as an "anti-spam enthusiast" and "professional plaintiff," whose sole source of income was monetary settlements from his litigation campaign.[25] His technique was to configure several Internet domains and e-mail inboxes under his control to not only passively accept spam but also to actively seek it. Once spam messages began arriving, Gordon would sue the senders or relaying providers. One such provider was Virtumundo, Inc., an e-mail marketing firm.

The district court determined that Gordon lacked CAN-SPAM standing and granted Virtumundo's motion for summary judgment.[26] It held that while Gordon qualified as an IAS under the prevailing definition of the term,[27] he failed to show adverse harm because any harm he suffered was the same as that suffered by ordinary e-mail users.[28] The court further held that since Virtumundo did nothing to hide its e-mail domains from end-users, it did not materially falsify or deceive, thus negating any claim Gordon might have had under state law via CAN-SPAM's preemption exception.[29]

Gordon appealed and the U.S. Court of Appeals for the Ninth Circuit affirmed the district court's decision in a strongly worded and decisive ruling. First, it explicitly rejected a broad interpretation of the

---

[23] ASIS Internet Servs. v. Active Response, No. C076211TEH, 2008 WL 2952809, at *6 (N.D. Cal. Jul. 30, 2008) (quoting defendant).

[24] *See* Gordon v. Virtumundo, 575 F.3d 1040 (9th Cir. 2009).

[25] *Id.* at 1056.

[26] *See* Gordon v. Virtumundo, No. 06-0204-JCC, 2007 WL 1459395, at *15 (W.D. Wash. May 15, 2007).

[27] *See id.* at 8.

[28] *See id.*

[29] *See id.* at 12.

definition of IAS.[30] Although the court noted that the actual definition of IAS may have a technical or hardware prerequisite, it refused to set forth any general test or definitional boundaries.[31] Nevertheless, the court considered CAN-SPAM's legislative intent and determined that a plaintiff was not an IAS because it had no control over the serving hardware and did not provide any service the service provider could not offer. As Gordon provided no actual services beyond what was already freely available to his "customers," the court determined that he did not qualify as an IAS.

Second, the Ninth Circuit added a two-part *extent* of harm requirement to the existing "adversely affected" test, which only necessitated showing adequate *type* of harm. The resulting test has three elements: (1) that there be, "at bare minimum, a demonstrated relationship between purported harms and the type of e-mail practices regulated by the Act,"[32] (2) the type of harm suffered must be "both real and of the type experienced by ISPs,"[33] and (3) any ISP-type harm suffered must be above and beyond the ordinary difficulties suffered by the normal operation of the ISP, even after normal reasonable precautions to avoid them.[34] Gordon failed on all counts. He could not proffer evidence of a connection between spam and his purported harms; he only suffered harm of the type ordinarily incurred by ordinary consumers. Even if he could meet the first two criteria, his efforts in actually attracting spam could not be construed as reasonable precautions to avoid it. The court noted that, for fear of creating an impossibly high standard, it was not requiring direct evidence of harm from *specific* e-mails. It merely required evidence of general harm of the correct type and extent.[35]

Finally, citing *Omega Travel v. Mummagraphics*, the *Gordon* court

---

[30] *See Gordon*, 575 F.3d at 1051.

[31] *See id.* at 1052.

[32] *Id.* at 1054.

[33] *Id.* at 1053.

[34] *Id.* at 1054.

[35] *See id.* at 1054 n.12. While the court noted the impracticability of tracing harm to a specific set of offending e-mails, it did not offer concrete examples of what it considered to be sufficiently harmful. Instead, the court reserved the future possibility of requiring evidence of specific e-mails causing alleged harm.

held that not only did Gordon's state claims fail to qualify for CAN-SPAM's preemption exception, but the state law itself was preempted.[36] The court seized on CAN-SPAM's stated legislative intent that the act regulate commercial e-mail "on a nationwide basis"[37] and only excepted state laws that "*target* fraud or deception."[38] The *Omega* court did not find that state laws prohibiting "mere error" or "insignificant inaccuracies" qualified as exceptions to preemption.[39] The *Gordon* court found that the state law in question, Washington's Commercial Electronic Mail Act (CEMA),[40] was substantially aimed at the same goals as CAN-SPAM and was thus preempted, regardless of CEMA's incidental language treating falsity or deception.[41] Such language, the court opined, left open the possibility of violation by inaccuracy, rather than intent, and thus ran afoul of *Omega's* preemption of statutes punishing "mere error" or technicalities.[42] In Gordon's case, because Virtumundo did nothing to hide the identity of its e-mails from discovery easily accessible by the public, Gordon's assertion of falsity and deception were without merit, and his state CEMA claims were preempted by his failed federal CAN-SPAM claims.

III. *GORDON'S* EFFECTS ON FUTURE SPAM LITIGATION

The *Gordon* decision drew mixed reactions. Some lauded the Ninth Circuit for sweeping away frivolous litigation and sharpening CAN-SPAM's focus,[43] while others criticized what they perceived as a

---

[36] *See Gordon*, 575 F.3d at 1060-62 (citing Omega World Travel v. Mummagraphics, 469 F.3d 348 (4th Cir. 2006)).

[37] *Id.* (citing 15 U.S.C. § 7701(b)(1) (2006)).

[38] *Id.*

[39] *Omega*, 469 F.3d at 354-55.

[40] WASH. REV. CODE § 19.190.030 (2010).

[41] *See* Gordon v. Virtumundo, 575 F.3d 1040, 1064 (9th Cir. 2009).

[42] *Id.*

[43] *See, e.g.*, Bruce Nye, *CAN-SPAM Act–Common Sense From the Ninth Circuit*, CAL BIZ LIT (Aug. 10, 2009, 9:19 AM), http://www.calbizlit.com/cal_biz_lit/2009/08/canspam-act-common-sense-from-the-ninth-circuit.html; David Johnson, *CAN-SPAM Update: Ninth Circuit Ruling Shuts Down Anti-SPAM Cottage Industry*, DIGITAL MEDIA LAWYER BLOG (Aug. 20, 2009), http://www.digitalmedialawyerblog.com/

weakening of anti-spam measures."[44] The debate centers on a widely disparate portrayal of Gordon himself; those in favor of the ruling viewed Gordon as an opportunistic litigant, while those against praised him as a scrupulous and canny anti-spam crusader.

Whatever Gordon's true motivations, the Ninth Circuit used a less-than-favorable view to assess his claims and formulate its holding.[45] Generally, the court sought to separate the actual law as codified in CAN-SPAM from sentiment as to what it *should* have been.[46] The Ninth Circuit singularly emphasized the congressional intent behind CAN-SPAM in every part of its analysis, which has wide-ranging implications on private standing for future related litigation.[47]

A. Higher Threshold for Internet Access Service (IAS) Status

As noted above, prior to *Gordon*, courts construed CAN-SPAM's IAS definition broadly but inconsistently. While CAN-SPAM uses the definition of "Internet" from the Internet Tax Freedom Act (ITFA),[48] it does not use the ITFA's definition of either IAS or the more restricted "Internet access provider," which specifically invoked hardware-based Internet service providers (ISPs).[49] Instead, it uses a much broader IAS definition[50] from the Child Online Protection Act,[51]

2009/08/digital_media_law_ninth_circui.html.

[44] *See, e.g.*, J. Craig Williams, *Prying Back The Lid On The CAN-Spam Act: No Private Right To Challenge Spammers*, MAY IT PLEASE THE COURT (Aug. 9, 2009, 7:54 AM), http://www.mayitpleasethecourt.com/journal.asp?blogid=2025.

[45] *See Gordon*, 575 F.3d at 1055 ("It is readily apparent that Gordon, an individual who seeks out spam for the very purpose of filing lawsuits, is not the type of private plaintiff that Congress had in mind.").

[46] *Gordon*, 575 F.3d at 1056 n.15 ("As should be apparent here, 'the law' that Gordon purportedly enforces relates more to his subjective view of what the law ought to be, and differs substantially from the law itself.").

[47] *See id.* at 1057 ("The CAN-SPAM Act was enacted to protect individuals and legitimate businesses—not to support a litigation mill for entrepreneurs like Gordon.").

[48] 47 U.S.C. § 151 (2006).

[49] *Id.*

[50] *See* 15 U.S.C. § 7702(11) (2006).

[51] 47 U.S.C. § 231(e)(4) (2006).

which not only includes ISPs such as Comcast, and Verizon DSL, but also *meta*-level service providers.[52]

Gordon carved out an exception to this broad definition by excluding professional litigants and other small-time private plaintiffs like blog owners or personal Web site operators. The court "reject[ed] any overly broad interpretation of 'Internet access service' that ignore[d] congressional intent," which generally viewed CAN-SPAM as only applicable to those in the best position to regulate spam and not those who merely received it.[53] Though the court refused to lay down any specific test, it advised that subsequent courts should "inquire into the plaintiff's purported Internet-related service operations" in questionable cases and determine what purpose those operations served.[54] Even if the operations were legitimate, their scale and complexity must be weighed; those providing a "nominal role in providing Internet-related services" cannot qualify.[55]

The court used Gordon's enterprise as an example of a non-IAS, even though it met CAN-SPAM's literal IAS definition. On its face, this appears to violate the Ninth Circuit's general precedent that "the legislative purpose of a statute is expressed by the ordinary meaning of the words used."[56] Gordon's service appears to enable users to access e-mail, fitting squarely within the literal CAN-SPAM IAS definition. However, the *Gordon* court distinguished Gordon's enterprise from IAS classification by noting its lack of value.[57] It observed that Gordon failed to operate as a bona-fide e-mail provider; he "avoided taking even minimal efforts to avoid or block spam" and instead actively

---

[52] *See* Ethan Ackerman, *Just Who Is an Internet Access Service Provider Under CAN-SPAM?*, TECHNOLOGY AND MARKETING LAW BLOG (Nov. 14, 2008, 1:29 AM), http://blog.ericgoldman.org/archives/2008/11/just_who_is_an.htm (asserting that Web sites like Facebook, Google, etc. also fall under the CAN-SPAM definition of IAS).

[53] Gordon v. Virtumundo, 575 F.3d 1040, 1050-51 (9th Cir. 2009).

[54] *Id.* at 1055.

[55] *See id.* at 1052.

[56] Leisnoi, Inc. v. Stratman, 154 F.3d 1062, 1066 (9th Cir. 1998); *accord* Seldovia Native Ass'n v. Lujan, 904 F.2d 1335, 1341 (9th Cir. 1990).

[57] *See Gordon*, 575 F.3d at 1051-52.

accumulated it for the purposes of initiating litigation.[58] The court also cited Gordon's lack of involvement in the creation of his e-mail service, which was limited to using a home computer to access a much larger e-mail provider's services.[59] The court determined that Gordon's service was not a service at all, as it did not provide users access to Internet resources beyond what was already available to them.[60]

The Ninth Circuit's decision sets the IAS threshold considerably higher, especially for professional plaintiffs. The decision's effect on more legitimate enterprises is still unclear, however. There is little to distinguish the methods used to set up legitimate e-mail domains, blogs, etc.—some of which may attract thousands or millions of users—from those employed by Gordon. The Ninth Circuit's expressly incomplete guidance on the matter suggests that it may have targeted Gordon's dubious aims rather than the lack of complexity or utility of his methods.[61]

The Ninth Circuit's precedent creates a definitional continuum for IAS status, requiring fact-based inquiry to determine eligibility. On the one hand, services created specifically to enable litigation are categorically ineligible. On the other hand, entities allowing primary access to the Internet itself or other legitimate Internet-based services—social networking and e-mail, for instance—are covered under IAS' generally broad definition. The threshold is less clear for plaintiffs between the extremes, especially for those providing secondary services such as personal blogs or family e-mail domains.

The Ninth Circuit's rule of statutory construction seemingly cabins the *Gordon* IAS limitations to explicitly illegitimate or useless services. Had Gordon actually maintained legitimate e-mail services for his clients, the court's analysis would have been a significantly closer proposition. Professional plaintiffs may begin "spam farming" more passively to avoid the elevated threshold.

---

[58] *Gordon*, 575 F.3d. at 1052.

[59] *Id.*

[60] *See id.*

[61] *See* Eric Goldman, *An End to Spam Litigation Factories?*, TECHNOLOGY AND MARKETING LAW BLOG (Aug. 7, 2009, 12:40 PM), http://blog.ericgoldman.org/archives/2009/08/an_end_to_spam.htm.

B. *The "Adversely Affected" Test and Required Showing of Actual Harm*

Even if a private plaintiff can show bona-fide IAS status, under *Gordon* they must now show that they were both adversely affected by IAS-type harm and that the harm was real, with an extent beyond that of "mere annoyance . . . and greater than the negligible burdens typically borne by an IAS provider in the ordinary course of business."[62]

As before, the CAN-SPAM Act redresses only harms that parallel its limited private right of action, including harms unique to IAS providers such as "investing in new equipment to increase capacity[,] customer service personnel to deal with increased subscriber complaints, [and] maintaining e-mail filtering systems and other anti-spam technology."[63] *Gordon* made it clear that consumer-related harms are irrelevant to CAN-SPAM analysis, not only neutralizing claims by private consumers, but also claims by IASs based partially or entirely on, for example, loss of personal data.[64] Such claims must now seek redress for the derivative effects of consumer-related harms, such as additional customer service costs.[65]

However, the calculation of adverse effect under CAN-SPAM now includes a baseline element. The *Gordon* court differentiates between the fixed and variable costs of spam prevention, and notes that subsequent courts must "be careful to distinguish the ordinary costs and burdens associated with operating an Internet access service from actual harm."[66] The court "expect[s] a legitimate service provider to secure adequate bandwidth and storage capacity and take reasonable precautions, such as implementing spam filters, as part of its normal operations."[67] The court seems to view spam as an expected part of the Internet industry, and any showing of actual harm for the purposes of CAN-SPAM standing must be above and beyond the normal expenses

---

[62] *Gordon*, 575 F.3d at 1054.

[63] *Id.* at 1053.

[64] Goldman, *supra* note 61.

[65] *See Gordon*, 575 F.3d at 1054.

[66] *Id.*

[67] *Id.*

required to counteract it.[68] "Network slowdowns, server crashes, increased bandwidth usage, and hardware and software upgrades bear no inherent relationship to spam or spamming practices," and evidence of them alone is insufficient to show that the IAS was adversely affected by misconduct.[69] Such events must be accompanied with evidence that "the e-mails at issue . . . contribute to a larger, collective spam problem that cause ISP-type harms."[70]

This seems to imply that an influx of spam of an unusual amount or insidiousness, mapped to a specific and abnormal IAS-type harm, is required for private standing under CAN-SPAM. However, due to what the Ninth Circuit perceived as "the impracticability of tracing harm to a specific e-mail or batch of e-mails," it refused to impose "a direct causation requirement," though it reserved the right to do so in future litigation.[71]

Gordon's stricter private standing requirements are effectively waived for "well-recognized ISPs or plainly legitimate Internet access service providers."[72] It reasoned that "adequate harm might be presumed because any reasonable person would agree that such entities dedicate considerable resources to and incur significant financial costs in dealing with spam."[73] For these plaintiffs, standing under CAN-SPAM is automatically granted. Conversely, harms alleged by plaintiffs with questionable IAS status should be "closely examine[d]."[74] This language has the effect of bifurcating the "adverse effect" requirements for large commercial providers and smaller enterprises.[75] It should be noted that *Gordon* left open the question of what characterizes a "recognized" ISP or a "plainly legitimate" IAS.

As with its restriction of the IAS definition, the *Gordon* court's holding on the CAN-SPAM harm elements invalidates most profes-

---

[68] Goldman, *supra* note 61.
[69] *Gordon*, 575 F.3d at 1054.
[70] *Id.*
[71] *Gordon*, 575 F.3d at 1054 n.12.
[72] *Id.* at 1055.
[73] *Id.*
[74] *Id.*
[75] Goldman, *supra* note 61.

sional litigants' standing arguments. It also requires a higher standing threshold for private plaintiffs of all but the largest and most well recognized IASs.

C. CAN-SPAM Preempts Overlapping State Law

Gordon's application of *Omega World Travel v. Mummagraphics* is a definite statement of CAN-SPAM's preemption of applicable state law. One of CAN-SPAM's stated aims is to address the states' disparate standards for commercial e-mail, which it found to be incompatible with the geographically independent nature of e-mail.[76] However, in some states, CAN-SPAM's enactment resulted in the creation of new anti-spam laws to work around the preemption statute, making enterprises like Gordon's more successful because of the additional state law action at their disposal.[77] These new laws were often more lax about standing and causation, sometimes focusing on the perpetrator's knowledgeable intent of their actions rather than any actual harm suffered by recipients, and provided any private recipient or Web site owner with a right of action.[78]

Just as the *Omega* decision invalidated these quickly-revised state laws in the Fourth Circuit, *Gordon's* affirmation of *Omega*'s principles may negate similarly situated state laws in the Ninth Circuit, following its disqualification of Washington's CEMA in *Gordon.* It is important to note that *Gordon* and *Omega* only interpret CAN-SPAM as preempting state laws specific to electronic mail; other laws, including statutes targeting fraud or computer crime, are still viable for litigation.[79] However, as *Gordon* demonstrated, such state claims must not be based on other, explicitly preempted grounds.[80]

---

[76] 15 U.S.C. §7701(a)(11) (2006).

[77] *See* Goldman, *supra* note 61.

[78] *See, e.g.*, State v. Heckel, 93 P.3d 189, 192-94 (Wash. App. 2004) (assessing defendant's liability for violating Wash. Rev. Code 19.190.020 in terms of *constructive knowledge of receipt*).

[79] Gordon v. Virtumundo, 575 F.3d 1040, 1065 n.24 (9th Cir. 2009).

[80] *See id.* at 1064-65 n. 23.

D. Prevailing Defendants May Be Awarded Attorney's Fees

Virtumundo was able to recover attorney's fees from Gordon at the district court level. This may have been the first time a defendant had prevailed in collecting attorney's fees in a CAN-SPAM action.[81] The district court found that since CAN-SPAM was intended to have a limited private right of action, a dual-standard approach to attorney's fees where plaintiffs' requests are always viewed favorably was not appropriate.[82] Congress' intent, it reasoned, was not for "private parties with no harm to invoke CAN-SPAM [and] collect millions of dollars."[83] The district court concluded that CAN-SPAM was best suited for an even-handed approach under *Fogerty*, wherein a prevailing defendant's request for remuneration would be "'evaluated no differently than the question to whether to award fees to a prevailing plaintiff.'"[84] Upon evaluating Gordon's serial litigation tendencies, the district court found ample reason to award Virtumundo attorney's fees with the "goal of deterrence."[85]

This novel reasoning was not addressed and thus not explicitly overruled by the Ninth Circuit. The district court turned professional litigation under CAN-SPAM into a much riskier financial proposition in the Western District of Washington; the Ninth Circuit's silence on the matter may move other courts in its jurisdiction to rule similarly.

CONCLUSION

Gordon effectively neutralizes most professional plaintiffs' standing arguments in the Ninth Circuit under CAN-SPAM's private right of action. First, the threshold question of whether a plaintiff is an IAS

---

[81] Eric Goldman, *CAN-SPAM Defendant Awarded $111k in Fees/Costs: Gordon v. Virtumundo*, CIRCLEID (Aug. 6, 2007, 4:44 PM), http://www.circleid.com/posts/070806_can_spam_act_gordon_virtumundo.

[82] Gordon v. Virtumundo, No. 06-0204-JCC, at *5-6 (W.D. Wash. Aug. 1, 2007) (order granting attorney's fees), *available at* http://www.spamnotes.com/files/31236-29497/Virtumundo_Order.pdf.

[83] *Id.* at *7.

[84] *Id.* at *5 (citing Fogerty v. Fantasy, 510 U.S. 517, 534 (1994)).

[85] *Id.* at *10.

involves close judicial scrutiny regarding its underlying purpose. Second, if the plaintiff is an IAS, it must show that it suffered significant IAS-type harm above and beyond ordinary inconvenience from a normal spam volume. Third, should the plaintiff's CAN-SPAM claim fail, the viability of a parallel state claim is now highly questionable. Finally, if the court determines that the claim is frivolous, the plaintiff runs the risk of being responsible for the defendant's legal fees and costs.

A side effect of the Ninth Circuit's methodical dissolution of CAN-SPAM litigation factories is that legitimate Web site operators and e-mail providers have a higher standard of harm, and possibly threshold IAS standing, to meet. Large and well-known providers and operators, however, may automatically be presumed to have standing with little inquiry into the merits of their claims.

PRACTICE POINTERS

- Examine the legitimacy and motives of private plaintiffs. New Ninth Circuit CAN-SPAM standing requirements make it difficult for litigation factories to succeed in court.
- Provide evidence of complexity, utility, and specialty. The more useful, involved, or unique the service provided by the plaintiff, the more likely they are to attain IAS status.
- Emphasize omnipresence or legitimacy of the service. A showing of obvious legitimacy of the plaintiff's service, or widespread recognition as an ISP, effectively bypasses the stringent "adversely affected by" requirements of the Ninth Circuit.
- Concentrate on materially deceptive practices. Mere errors and technical glitches are not likely to meet the standard under either federal or state law.
- Be prepared to defend against claims for attorney's fees. If the defendant prevails, it is possible that the court will use the *Fogerty* even-handed standard for determining costs.