UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

BUTERA & ANDREWS, Plaintiff, v. INTERNATIONAL BUSINESS MACHINES CORPORATION, et al., Defendants.	)	Civil Action No. 1:06-CV-647 (RBW)

MEMORANDUM OPINION

Butera & Andrews ("the plaintiff") brings this action against International Business Machines Corporation ("IBM") and an unidentified John Doe defendant, seeking monetary damages and injunctive relief for alleged interference with the plaintiff's computer records in violation of the Computer Fraud and Abuse Act ("Computer Fraud Act"), 18 U.S.C. §§ 1030(a)(2), (a)(5) (2000), the Stored Wire and Electronic Communications Act ("Stored Wire Act"), 18 U.S.C. §§ 2701(a), 2707(a) (2000), and the Federal Wiretap Act, 18 U.S.C.A. §§ 2511(1)(a)-(b) (2002). Complaint ("Compl.") ¶¶ 15-20. The plaintiff contends that the alleged violations were committed "with IBM owned or operated equipment and were directed by IBM employees or agents." Id. ¶¶ 16, 18, 20. The plaintiff asks that "all information illicitly obtained from [the] plaintiff" be returned," id. at 9-10, and that the defendants pay the plaintiff for its damages, "including damages for items illicitly taken, the costs of investigation, the cost of

additional security measures, statutory damages and attorney's fees for this action," id. at 10. Currently before the Court is IBM's motion to dismiss for failure to state a claim ("Def's Mot.").[1] For the reasons set forth below, the Court grants IBM's motion.

I. Background

The plaintiff, a law firm located in the District of Columbia, alleges the following facts in support of its claims. Compl. ¶ 1. As part of its business activities, the plaintiff "makes extensive use of electronic mail ["e-mail"] to communicate with clients and others on behalf of clients." Id. ¶ 6. Sometime in October or November of 2005, the plaintiff became aware of certain facts suggesting that its e-mail server "had been compromised by unauthorized parties." Id. ¶ 7. To look into the matter, the plaintiff retained a private investigative firm specializing in computer forensics and security. Id. ¶ 8. A security review conducted by this firm revealed that "unauthorized personnel" had penetrated the plaintiff's e-mail server and left a series of instructions "which permitted [computer hackers] to enter the system surreptitiously" and download documents from the server. Id. ¶ 9.

On November 8, 2005, the firm monitored an attempt by an unauthorized party to obtain access to the plaintiff's e-mail server.[2] Id. ¶ 11. While the attempt was unsuccessful, the firm was able to determine that it originated from a specific Internet Protocol ("IP") address. Id. An

[1] The following papers have been submitted to the Court in connection with this motion: (1) Defendant IBM's Memorandum of Law in Support of its Motion to Dismiss for Failure to State a Claim ("Def.'s Mem."); (2) Plaintiff's Opposition to Motion to Dismiss for Failure to State a Claim and Cross Motion for Limited Expedited Discovery ("Pl.'s Opp."); (3) Defendant IBM's Consolidated Reply in Support of its Motion to Dismiss for Failure to State a Claim and Opposition to Plaintiff's Cross Motion for Limited Expedited Discovery ("Def.'s Opp."); and (4) Plaintiff's Reply to Defendant IBM's Opposition to Limited Expedited Discovery ("Pl.'s Reply").

[2] The complaint states that this attempt to access the plaintiff's e-mail server occurred "[o]n November 12, 2006 [sic]." Compl. ¶ 11. However, the plaintiff's opposition to IBM's motion to dismiss corrects that date to November 8, 2005. Pl.'s Opp. at 3 n.1.

IP address is a "unique identifying number for a particular computer" that "serve[s] as locational information for the receipt and transmission of information over the [I]nternet." Id. ¶ 10. According to the plaintiff, the IP address involved in the alleged November 8th attack on its server was "registered to the [d]efendant IBM and . . . located at the IBM facility on Cornwallis Road in Durham, North Carolina." Id. ¶ 11.

The security firm allegedly found evidence of other attacks as well. From November 12, 2005, to November 25, 2005, a computer maintained by the firm's investigators was allegedly subjected to multiple "denial of service" attacks, all "originat[ing] from IP addresses which are registered to the [Durham] IBM facility." Id. ¶ 12. The plaintiff also alleges that the firm's "review of computer logs for a client of [the plaintiff] revealed over 42,000 attempts by 80 different IP addresses registered to the IBM Durham controlled machines to penetrate the [client's] internal computer server during the twelve-month period beginning on January 1, 2005."[3] Id. ¶ 13. The plaintiff does not contend that its servers, or those of its clients or the security firm, have been the subject of any attacks since January 1, 2006.

On April 7, 2006, the plaintiff initiated this action against IBM and the John Doe defendant, identified as "a person who is employed by Defendant IBM at its Durham, North Carolina facility," id. ¶ 3, alleging violations of the Computer Fraud Act, the Stored Wire Act,

[3] IBM argues that to the extent that the alleged attacks occurred against computers belonging to the plaintiff's security firm or the plaintiff's clients rather than the plaintiff itself, the plaintiff has no legal standing to assert damages on behalf of those third parties or otherwise to represent them in this matter. Def.'s Mot. at 4 n.3; see also Def.'s Opp. at 5 (stating that "the Complaint alleges only a single event that was directed at [the] Plaintiff's e-mail server through a single IBM-registered IP address"). IBM also takes issue with the plaintiff's characterization of the alleged attacks on its client's server. See Def.'s Opp. at 6 (contending that "like a Texas sharp-shooter, [the] Plaintiff apparently identified all events experienced by the client over a period of a year that involved any of the millions of IP addresses registered to IBM, drew a circle around it, and called it a 'pattern'"). Because the Court concludes that the plaintiff's complaint fails to articulate a viable claim against IBM concerning any of the alleged attacks, it need not address the merits of these arguments.

and the Federal Wiretap Act resulting from the above-mentioned attacks, id. ¶¶ 15-20. Significantly, the plaintiff does not allege that defendant IBM orchestrated, authorized, or was otherwise aware of these attacks. See id. ¶ 16 (alleging that the violations were committed by "a person or persons whose identity is unknown at this time"). Rather, the plaintiff claims "upon information and belief" that "[d]efendant John Doe, in his capacity as IBM employee or agent, initiated, directed and managed" all attacks from January 2005 onward "from the Durham, North Carolina [IBM] facility," id. ¶¶ 11, 12, 13, and contends that the attacks "were made with IBM owned or operated equipment and were directed by IBM employees or agents," id. ¶¶ 16, 18.[4] The plaintiff seeks monetary damages, including the $60,000 it has allegedly "expended . . . in the investigation, surveillance, and repair of its e-mail systems," id. at 9, as well as injunctive relief (1) "ordering . . . IBM and any of its officers, agents, servants, employees and other persons in active concert or participation with any of them to cease violations of statutory and common law"; (2) "requiring the return of all information illicitly obtained from [the] plaintiff that resides in any of the computer equipment . . . owned or maintained by . . . IBM"; and (3) "directing the disclosure of information under [IBM's] control which may reflect on who may have caused the placement of unauthorized code, unauthorized entries, denial of service attacks and theft of electronic information," id. at 9-10.

IBM now moves to dismiss the complaint, arguing that "[the] plaintiff's legal theory against [it] is fatally flawed as a matter of law." Def.'s Mot. at 2. Specifically, IBM contends,

[4] The plaintiff also asserts that IBM's policy of "maintain[ing] [computer activity] logs only for a 24 hour period" prevents the plaintiff from tracking "[i]llegal, improper or unauthorized activity of any of the computers under the control or management of the IBM Durham facility" and "encourages improper use of the [facility's] machines since it assures anonymity for any wrongdoer." Compl. ¶ 14.

inter alia, that "[the] [p]laintiff fails to allege that IBM acted 'intentionally' as that term is intended under the operable statutes, and in fact makes allegations that are entirely inconsistent with intentional conduct on the part of IBM." Id. In response, the plaintiff argues (1) that IBM's motion is properly resolved as a matter of summary judgment rather than pursuant to a motion to dismiss under Federal Rule of Civil Procedure 12(b)(6); (2) that it has alleged sufficient facts to support its statutory causes of action against IBM; and (3) that limited, expedited discovery is necessary to resolve the issues raised by IBM. Pl.'s Opp. at 1. IBM opposes the plaintiff's motion for expedited discovery, asserting that "[w]hile [the] [p]laintiff may need limited discovery from IBM to assist it in identifying the potential culprits, the appropriate way to get that discovery is not by initiating a frivolous lawsuit against IBM that is not justified by either the facts or the law." Def.'s Opp. at 2. Rather, IBM suggests that the plaintiff's proper course is to "issue[] third party subpoenas to the registered holders of the IP addresses to determine the identity of the customers who had used those addresses." Id. (citation omitted).

II. Standard of Review

When evaluating a motion for failure to state a claim upon which relief can be granted pursuant to Federal Rule of Civil Procedure 12(b)(6), the Court "must treat the complaint's factual allegations as true and must grant [the] plaintiff the benefit of all inferences that can be derived from the facts alleged." Sparrow v. United Airlines, Inc., 216 F.3d 1111, 1113 (D.C. Cir. 2000) (internal quotation marks and citations omitted). "Given the Federal Rules' simplified standard for pleading," a complaint may be dismissed under Rule 12(b)(6) "only if it is clear that no relief could be granted under any set of facts that could be proved consistent with the allegations." Swierkiewicz v. Sorema, 534 U.S. 506, 514 (2002) (internal quotation marks and

citation omitted). However, the Court need not accept "inferences drawn by [the] plaintiff if such inferences are unsupported by the facts set out in the complaint, nor legal conclusions cast in the form of factual allegations." Browning v. Clinton, 292 F.3d 235, 242 (D.C. Cir. 2002) (internal quotation marks and citation omitted).

III. Legal Analysis

The Court notes at the outset that, contrary to the plaintiff's suggestion, it need not wait until the completion of discovery to decide IBM's dispositive motion. See Pl.'s Opp. at 1 (asserting that "[the] Defendant's argument[] that the Plaintiff is unable to prove facts sufficient . . . to include them within the statutory causes of action . . . is one that can only be cured by limited discovery to resolve those issues"); id. at 11 (contending that "all of the cases upon which [IBM] relies . . . were summary judgment requests decided after discovery had been completed"); id. at 13 (claiming that it "does not presently have all the facts to support its claims" because IBM "has in the past declined to reveal the [necessary] information"); Pl.'s Reply at 3 (stating that discovery is necessary in order to adduce "the answers that will either confirm IBM's claims of complete innocence or implicate them in procedures and knowledge which they are understandably reluctant to reveal"). If IBM's motion were predicated upon the argument that the plaintiff has failed to prove IBM's involvement in the alleged attacks, then the plaintiff's contention that this is a matter appropriately resolved by way of summary judgment would have some merit. However, this is not what IBM argues in support of its motion. Rather, IBM contends that the plaintiff "has [not] even alleged the essential elements of its claim." Def.'s Opp. at 3 (emphasis added). IBM's motion is therefore appropriately brought as a motion to dismiss pursuant to Rule 12(b)(6). See Swierkiewicz, 534 U.S. at 514 (holding that Rule

12(b)(6) dismissal is proper where "it is clear that no relief could be granted under any set of facts that could be proved consistent with the allegations") (internal quotation marks and citation omitted).

A. The Plaintiff's Statutory Violation Claims

The plaintiff alleges that the attacks enumerated in its complaint are "connected to" IBM because the attempts to gain access to its computer server "were made with IBM owned or operated equipment and were directed by IBM employees or agents." Compl. ¶ 16. In moving to dismiss the claims against it, IBM argues that the plaintiff "has failed to state a claim . . . because it has not alleged any knowing, intentional or deliberate actions by IBM," Def.'s Mem. at 4, which is a necessary predicate here given that the relevant statutes "each require a showing of knowing or intentional conduct in order for a violation to occur," id. at 5 (citing the Computer Fraud Act, 18 U.S.C. §§ 1030 (a)(2), (a)(5); the Stored Wire Act, 18 U.S.C. §§ 2701(a), 2707(a); and the Federal Wiretap Act, 18 U.S.C.A. §§ 2511(1)(a)-(b)). According to IBM, "[the] [p]laintiff admits that it has no idea who attacked its computer systems," Def. Mem. at 1, and does not allege "that IBM knew about or authorized the attacks . . . or that it had any conceivable motive to do so," id. at 2. Consequently, even "assum[ing] the truth of the plaintiff's . . . allegation that an IBM employee was involved," IBM asserts that "the only inference permitted from the facts alleged in the complaint is that the attacks were conducted by a rogue employee acting outside the scope of his or her employment and without authorization." Id. In response, the plaintiff argues that "[t]he inference from the use of [IBM's] addresses in a sustained and sophisticated attack and scan of different computers belonging to or associated with the Plaintiff demonstrate[s] [IBM's] intentional participation in this activity." Pl.'s Opp. at 15. The Court

agrees with IBM that the plaintiff has not plead any intentional conduct by IBM as required by the federal statutes relied upon in the complaint.

The language of the Computer Fraud Act, the Stored Wire Act, and the Federal Wiretap Act all require "intentional" conduct before giving rise to a statutory violation. See Computer Fraud Act, 18 U.S.C. § 1030(a)(2) ("whoever . . . intentionally accesses a computer without authorization. . . ."); Stored Wire Act, 18 U.S.C. §§ 2701(a)(1) ("whoever . . . intentionally accesses without authorization. . . ."), 2707(a) (stating that "the conduct constituting the violation [must be] engaged in with a knowing or intentional state of mind . . . ."); Federal Wiretap Act, 18 U.S.C.A. §§ 2511(1)(a)-(b) ("any person who . . . intentionally intercepts . . . [or] intentionally uses. . . ."). This is not a minimal standard. As the Senate Judiciary Committee stated when recommending the passage of the Electronic Communications and Privacy Act of 1986, which amended the Federal Wiretap Act to require "intentional" rather than "willful" conduct:

> [T]he term "intentional" [in this context] is narrower than the dictionary definition of "intentional." "Intentional" means more than that one voluntarily engaged in conduct or caused a result. Such conduct or the causing of the result must have been the person's conscious objective. . . . The "intentional" state of mind is applicable only to conduct and results. Since one has no control over the existence of circumstances, one cannot "intend" them.

S. Rep. No. 99-541, at 23 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3577 (emphasis added); see also In re Pharmatrak, 329 F.3d 9, 23 (1st Cir. 2003) (quoting report); United States v. Townsend, 987 F.2d 927, 930 (2d Cir. 1993) (stating that, in order for a jury to find that a defendant acted "intentionally" under the Federal Wiretap Act, "[the] defendant's act must have been the product of [the] defendant's conscious objective"). The requirement of "intentional" conduct found in Sections 2701 and 2707 of the Stored Wire Act was also enacted as part of the

Electronic Communications and Privacy Act of 1986. S. Rep. 99-541, at 35-36, 43 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3589-90, 3597. Moreover, similar statements regarding the definition of "intentional" were made in connection with the passage of the Computer Fraud Act, as well as in other contexts. S. Rep. 99-432, at 5-7 (1986), reprinted in 1986 U.S.C.C.A.N. 2479, 2483-85 (contrasting "intentional acts of unauthorized access" with "mistaken, inadvertent, or careless ones" and stating that "[the] 'intentional' standard is designed to focus [on individuals] whose conduct evinces a clear intent to enter, without proper authorization, computer files or data belonging to another" and that "[s]uch conduct . . . must have been the person's conscious objective"); cf. S. Rep. 103-296, at 73 (1994), 1994 WL 320917 (stating that "[t]he word 'intentionally' was carefully chosen," in drafting the Counterintelligence and Security Enhancements Act of 1994, "to reflect the most strict standard for criminal culpability [such that the allegedly violative conduct must have been] engaged in with a conscious objective or desire to commit a violation") (emphasis added).

The plaintiff claims that all of the IP addresses involved in the three attacks are registered to the IBM facility, Pl's Opp. at 5, and that "the inference of IBM participation based on the presence and frequency of the IBM registered IP addresses remain strong." Pl.'s Opp. at 8 (emphasis added). As IBM observes, however, the plaintiff does not claim in its complaint "that IBM authorized any person to attack or otherwise obtain unauthorized access to [the] plaintiff's computer systems," nor does it offer any "conceivable motive for IBM to engage in such conduct, nor any benefit that could possibly be derived by IBM as a 'conscious objective' of any such attacks." Def.'s Mem. at 6; see also Def.'s Opp. at 1 (stating that "nowhere in the Complaint is there any allegation that IBM knew about or authorized the as-yet-unidentified

'hacker' to attempt to penetrate [the] Plaintiff's e-mail server, or any allegation that IBM had any conceivable benefit to be gained from such conduct"). According to the Pharmatrak Court, it is more reasonable to conclude that an act is intentional for the purpose of the relevant statues "when it serves a party's self-interest to engage in such conduct." 329 F.3d at 23. Here, the plaintiff has not even remotely suggested a motive for IBM to engage in these attacks.

Indeed, the plaintiff itself suggests that the attacks were the result of "unauthorized activity" on computers at IBM's Durham facility. Compl. ¶ 14; see also Pl.'s Opp. at 5 (noting that it is easier for an IBM employee "to circumvent IBM's external firewalls and security"). If the attacks were not authorized by IBM, there are no grounds whatsoever for bringing an action against IBM under any of the statutes relied upon by the plaintiff, as each requires "intentional" conduct on the part of the defendant. See Computer Fraud Act, 18 U.S.C. § 1030(a)(2); Stored Wire Act, 18 U.S.C. §§ 2701(a), 2707(a); Federal Wiretap Act, 18 U.S.C.A. §§ 2511(1)(a)-(b). Thus, even accepting the truth of the plaintiff's factual allegations, its complaint against IBM must be dismissed. Moreover, as the plaintiff ultimately concedes, it has pled no more than that "IBM assets initiated the attacks." Pl.'s Opp. at 6 (emphasis added). This is plainly insufficient to amount to "intentional" conduct under the relevant statutes.[5]

---

[5] In any event, the Court is not persuaded by the plaintiff's contention that "IBM assets initiated the attacks." Pl.'s Opp. at 6. The only fact advanced by the plaintiff in support of this position is that the IP addresses, which were allegedly involved in the attacks, were registered to the IBM facility in North Carolina. Compl. ¶ 11; Pl.'s Opp. at 3-4, 8. However, the mere fact that the attacks originated from the IBM registered IP addresses does not alone necessarily support the conclusion that IBM assets were involved in the attacks. As IBM notes, the plaintiff acknowledges that IBM's Durham facility "performs a variety of services, including . . . operation, supervision and maintenance of computers leased to other companies that serves as [I]nternet or private network servers." Def.'s Mem. at 3 (quoting Compl. ¶ 2) (emphasis added by IBM). IBM further contends that the IP address from which the November 8th attack was allegedly conducted "leads to a webpage for a company called Workforce Management, which is not an IBM-related entity." Id. In response, the plaintiff asserts that "a computer server to which IBM may have administrative entry rights, may not be classed by IBM as 'controlled.' Nevertheless, it provides an opportunity for IBM to insert and execute the types of programs that are the subject of this complaint." (continued...)

Far from pleading any intentional conduct on the part of IBM, the plaintiff's position appears directed, at most, at establishing the likelihood that an individual employed at the IBM facility in Durham is responsible for the alleged attacks. For example, in its opposition to IBM's motion to dismiss, the plaintiff states:

> While [the] Plaintiff may not know the name of the person or persons who pressed the "enter" button for each attack, it is reasonable to suspect that it is a person who has intimate knowledge of IBM facilities and authority from IBM to maintain, test, monitor and access the computers assigned to these [IP addresses].

Pl.'s Opp. at 5; see also id. (contending that "[t]he hacking efforts that form the basis of the Plaintiff's complaint are made much easier by a person on the inside who does not have to circumvent IBM's external firewalls and security"). The only hint in the plaintiff's complaint of an affirmative allegation that IBM itself initiated or authorized the computer attacks is the statement that the attacks "were directed by IBM employees or agents." Compl. ¶¶ 16, 18. Even this, however, is nothing more than an "inference[] unsupported by facts set out in the complaint," Rasul v. Rumsfeld, 414 F. Supp. 2d 26, 30 (D.D.C. 2006) (citations omitted), which, in any event, implicates IBM only insofar as it refers, in conclusory fashion, to "employees or agents" of the company. The plaintiff has adduced no facts to suggest that, in carrying out the complained-of attacks, John Doe was acting as IBM's agent as that term is understood in the law. See Restatement (Third) of Agency § 1.01 (2006) (defining agency as "the fiduciary relationship

---

[5](...continued)
Pl.'s Opp. at 7. However, the plaintiff fails to provide any shred of support for its claim that IBM may have inserted or executed the programs which attacked the plaintiff's computer server. Indeed, the plaintiff's argument on this point appears somewhat disingenuous (or at least based on total speculation) in light of the plaintiff's utter failure to plead intentional conduct on IBM's part in its complaint. Therefore, it is difficult for the Court to conclude that IBM assets initiated the attack based on the single fact that the IP addresses that initiated the attacks were registered to the IBM facility.

that arises when [a principal] manifests assent to [an agent] that the agent shall act on the principal's behalf and subject to the principal's control"). Moreover, as discussed below, the Court concludes on the pleadings before it that there is no basis to hold IBM liable under theories of respondeat superior or vicarious liability for the actions of the John Doe defendant, even if the attacks were actually carried out by an IBM employee or agent.

Under District of Columbia law, an employer cannot be held liable for its employees' intentional conduct solely on the basis of an employer-employee relationship. See Haddon v. United States, 68 F.3d 1420, 1424 (D.C. Cir. 1995) (holding that "[i]t is not enough that an employee's job provides an 'opportunity' to commit an intentional tort") (citation omitted); see also Keys v. Wash. Metro. Area Transit Auth., 408 F. Supp. 2d 1, 4 (D.D.C. 2005) (stating that "[t]he mere existence of [a] master and servant relationship is not enough to impose liability on the master.") (internal quotation marks and citation omitted). "[T]he employer will not be held liable for those wilful acts, intended by the agent only to further his own interest, not done for the employer at all." Jordan v. Medley, 711 F.2d 211, 214 (D.C. Cir. 1983) (internal quotation marks, citation, and bracketing omitted); see also Nelson v. United States, 838 F.2d 1280, 1283 (D.C. Cir. 1987) (noting that under District of Columbia law, courts have "focused on whether the employee was furthering [the] employer's interests" when determining an employer's liability for employee actions); Keys, 408 F. Supp. 2d at 4 (stating that the plaintiff "must plead facts, which, if true, demonstrate that alleged conduct of [an employee] was an outgrowth of their work assignments, or an integral part of their business activities, interests, or objectives, thereby establishing [the employer's] liability for its employee['s] conducts"); Fullwood v. IDS Fin. Corp., Civ. No. 88-3279-OG, 1989 U.S. Dist. LEXIS 12010, at *1 (D.D.C. Oct. 6, 1989) (stating

that "under the law of the District of Columbia, an employer is not liable for the intentional torts of an employee when the intentional torts are not motivated by an intent to further the employer's business"). The plaintiff does not allege that the complained-of attacks were committed by the John Doe defendant to "further[] his employer's interests," even assuming that the Doe defendant was employed by IBM. Nelson, 838 F.2d at 1283. Rather, all the plaintiff alleges is that "John Doe in his capacity as IBM employee or agent, initiated, directed and managed these attacks." Comp. ¶¶ 11-13 (emphasis added). The plaintiff has thus made no showing of any relationship between IBM and Doe sufficient to support its position that IBM can be held liable for Doe's misdeeds.[6]

Indeed, the Court agrees with IBM's observation that the cases cited by the plaintiff in support of its vicarious liability theory "all involve intentional conduct that was directed or

[6] Additionally, courts in other jurisdictions have held that the Computer Fraud Act "creates only a limited private right of action against the violator." Doe v. Dartmouth-Hitchcock Med. Ctr., Civ. No. 00-100-M, 2001 WL 873063, at *5 (D.N.H. July 19, 2001)(emphasis in original) (internal quotation marks and citation omitted); see also Role Models Am., Inc. v. Jones, 305 F. Supp. 2d 564, 568 (D.Md. 2004) (rejecting a Computer Fraud Act claim where the plaintiff had not alleged that the employer itself accessed the plaintiff's computers). In Dartmouth-Hitchcock, the plaintiff brought suit against a medical center, alleging that the medical center violated the Computer Fraud Act through an employee who accessed the plaintiff's medical records without authorization. 2001 WL 873063, at *3-5. The Dartmouth-Hitchcock Court granted the defendant's motion to dismiss, concluding that "imposing [liability] on the [employer] would neither be permitted by the language of the [Computer Fraud Act] itself, nor would it further the basic purpose of the Act." Id. at *5. Moreover, the Court went on to say that "to hold the [employer] vicariously liable for [the employee's] intentional violation of the defendants' own policies . . . would hardly be consistent with, or further the purpose of, the [Computer Fraud Act]." Id. Here, as already noted, the plaintiff does not allege that IBM is a "violator." Rather, the plaintiff's own statement that "it is reasonable to suspect a person on the inside who does not have to circumvent IBM's external firewalls and security," Pl.'s Opp. at 5, supports IBM's position that IBM did not authorize or direct the "wrongdoers." Moreover, the plaintiff's reliance on Charles Schwab & Co. v. Carter, Civ. No. 04-7071, 2005 WL 2369815 (N.D.Ill. Sept. 27, 2005), and Nexans Wires S.A. v. Sark-USA, Inc., 319 F. Supp. 2d 468 (S.D.N.Y. 2004), is misplaced. See Pl.'s Opp. at 12. The Charles Schwab & Co. Court distinguished its case from Dartmouth-Hitchcock, stating that the plaintiff's complaint is "sufficient" to survive the motion to dismiss because it alleged that the employer "affirmatively urged the employee to access the plaintiff's computer system beyond his authorization for their benefit." 2005 WL 2369815, at *7 (emphasis added). Similarly, the Nexans Wires Court noted that the plaintiff alleged that the employer directed its employees to access the plaintiffs' computer unlawfully. 319 F. Supp. 2d at 472. However, in the present action, the plaintiff makes no allegation that IBM "affirmatively urged" or directed any of its employees or anyone else to take the challenged actions. Id.

approved by the corporate defendant in order to gain an unfair business advantage at the expense of a competitor." Def.'s Opp. at 11; see Creative Computing v. Getloaded.com LLC, 386 F.3d 930, 932 (9th Cir. 2004) (corporate defendant hired competitor's employee, who improperly accessed and retrieved competitor's customer lists); E.F. Cultural Travel v. Explorica, Inc., 274 F.3d 577, 579 (1st Cir. 2001) (corporate defendant hired third party Internet consultant to create computer program that obtained pricing information from competitor's website); Pac. Aerospace & Elecs., Inc. v. Taylor, 295 F. Supp. 2d 1188, 1192-1193 (E.D. Wash. 2003) (corporate defendant hired competitor's employees who misappropriated trade secrets and confidential information). In the present action, the plaintiff does not allege any similar competitive relationship between itself and IBM. Moreover, the plaintiff's assertion that IBM would be vicariously liable under theories such as ratification, Pl.'s Opp. at 9, is unavailing because the plaintiff fails to "plead facts, which, if true, demonstrate that" IBM tacitly knew and approved of the conduct allegedly engaged in by its employees or agents. Keys, 408 F. Supp. 2d at 4 (granting the defendant's motion to dismiss pursuant to Rule 12(b)(6) when the plaintiff did not "plead facts, which, if true, demonstrate that the alleged conduct of [the defendant's] employees was an outgrowth of their work assignments, or an integral part of their business activities, interests, or objectives, thereby establishing the [employer's] liability for its employees' conduct") (citation omitted); see also Rwanda v. Rwanda Working Group, 227 F. Supp. 2d 45, 69 (D.D.C. 2002) (observing that "[f]or an unauthorized act to be ratified, the principal must have knowledge of the act that may ratify the act impliedly").

B. The Plaintiff's Request for Limited Expedited Discovery

Rather than granting IBM's motion to dismiss, the plaintiff asks the Court to allow it to engage in limited expedited discovery of "IBM's internal security information, personnel records, activity logs, administrative logs, security and event reports and other internal IBM material," Pl.'s Opp. at 6, in order to uncover "the answers that will either confirm IBM's claims of complete innocence or implicate them in procedures and knowledge which they are understandably reluctant to reveal," Pl.'s Reply at 3. See Pl.'s Opp. at 14 (outlining discovery requests). The plaintiff believes that this information will "include (or exclude) IBM personnel or agents from [participation in the attacks] and [demonstrate] whether these persons were acting on behalf of IBM and in furtherance of their employment." Id. at 6. The plaintiff further states that it "would concede that it could not prove participation of IBM or its employees or agents" if the documents it seeks through expedited discovery show that "IBM personnel had no administrative, maintenance, or other rights of access to the machines and their operating systems." Id. at 8.

Post-complaint discovery, however, is not the appropriate tool by which to gather facts about the extent, if any, of IBM's intentional participation in the alleged attacks.[7] As IBM observes, "[t]he issue is not whether [the] Plaintiff can prove intentional conduct at this stage, but rather whether it has even alleged the essential elements of its claim." Def.'s Opp. at 3 (emphasis in original). Here, not only does the plaintiff "acknowledge[] that it does not presently

[7] Moreover, as discussed above, even if discovery were to show that "IBM personnel . . . had rights of access" to the computers in question, this would not "prove participation of IBM" or otherwise demonstrate that IBM itself intentionally engaged in or otherwise authorized the conduct complained of by the plaintiff. Pl.'s Opp. at 8; see supra at 7-14.

have all the facts to support its claims," Pl.'s Opp. at 13, but, as the Court has already concluded, the complaint fails even to allege the requisite statutory elements to support an action against IBM. Fundamental fairness commands that "[c]ounsel should not be allowed to file a complaint first and thereafter endeavor to develop a cause of action." Weil v. Markowitz, 108 F.R.D. 113, 116 (D.D.C. 1985) (citing Fed. R. Civ. P. 11) (other citation omitted). Otherwise, totally innocent parties could be forced to defend themselves in judicial proceedings, at great expense and with the potential for public humiliation, against baseless claims predicated on nothing more than pure speculation or, even worse, mean-spirited vindictiveness. Therefore, insofar as the plaintiff's request for expedited discovery is directed at shoring up, in some post hoc manner, its reason for including IBM as a defendant in this lawsuit in light of a facially deficient complaint, the request must be denied.

Moreover, while the plaintiff speculates that factual discovery might "implicate" IBM in the alleged attacks, Pl.'s Reply at 3, it is clear that the ultimate purpose of the requested discovery is to determine "the identity of the John Doe mentioned in the complaint," Pl.'s Opp. at 6; see id. at 13 (arguing that it is "particularly true" that "a search to determine the identity of the John Doe listed in the complaint" must be undertaken at this stage of the litigation). Plaintiffs lacking necessary information about unidentified defendants must seek such information through third-party subpoenas or other third-party discovery, rather than by naming the organizations who possess the desired documents as defendants themselves in an apparent attempt to compel disclosure. See Virgin Records Am. v. John Does 1-35, Civ. No. 05-1918 (CKK), 2006 WL 1028956, at *1-*3 (D.D.C. Apr. 18, 2006) (allowing third-party subpoena directed at Internet Service Providers ("ISP") of unidentified defendants, where the plaintiff could not otherwise

"identify the true names and locations of the [alleged copyright] infringers"); Alvis Coatings, Inc. v. John Does 1-10, Civ. No. 3L94-374-H, 2004 WL 2904405, at *2 (W.D.N.C. Dec. 2, 2004) (denying motion to quash third-party subpoena directing the ISP of unidentified defendants "to provide documents sufficient to identify the name, address, and telephone number of the individuals corresponding to the specific IP addresses [named by the plaintiff]"); see also Def.'s Opp. at 2 (suggesting that third-party discovery is the "proper course" for the plaintiff to obtain information regarding the identity of the John Doe defendant). Therefore, the Court will consider the plaintiff's requests for information from IBM concerning John Doe's identity when and if such requests are brought in the form of third-party discovery now that IBM has been dismissed as a party in this action.[8]

IV. Conclusion

For the foregoing reasons, the Court grants without prejudice IBM's motion to dismiss for failure to state a claim upon which relief may be granted and denies the plaintiff's request for limited expedited discovery. A status conference in this matter shall be held on December 20, 2006, at 9:30 a.m., to assess what progress, if any, the plaintiff has made or intends to make in prosecuting this action against the John Doe defendant.

[8] In light of the plaintiff's allegation that IBM "has in the past declined to reveal" information which the plaintiff believes would assist it in providing factual support for its legal claims, Pl.'s Opp. at 13, the Court recognizes the possibility, however slim, that the plaintiff will uncover facts, whether through third-party subpoena or otherwise, which demonstrate that IBM did intentionally authorize or direct the attacks alleged in the complaint. See Pl.'s Reply at 3 (contending that factual discovery could "implicate [IBM] in procedures and knowledge which [it is] understandably reluctant to reveal"). Accordingly, the Court will dismiss the plaintiff's claims against IBM without prejudice. The plaintiff may refile its claims against IBM only if it has a concrete and particularized basis on which to do so and only if the asserted conduct meets the requisite statutory standards of intentional conduct. See Pharmatrak, 329 F.3d at 23 (holding that "[s]uch conduct or the causing of the result must have been the person's conscious objective"). The Court will look extremely skeptically upon such a claim, however.

SO ORDERED this 18th day of October, 2006.[9]

REGGIE B. WALTON
United States District Judge

[9] An Order consistent with the Court's ruling accompanies this Memorandum Opinion.