NOT FOR PUBLICATION
WITHOUT THE APPROVAL OF THE COMMITTEE ON OPINIONS

JEREMY RUBIN d.b.a. TIDBIT, Plaintiff	:	SUPERIOR COURT OF NEW JERSEY ESSEX COUNTY: LAW DIVISION
v.	:	DOCKET NO.: ESX-L-567-14
	:	**OPINION**
STATE OF NEW JERSEY DIVISION OF CONSUMER AFFAIRS Defendant	:	

Counsel for Plaintiff:
Hanni Fakhoury, Esq. (Pro Hoc Vice)
Electronic Frontier Foundation
Frank Corrado, Esq.
Barry, Corrado, & Grassi, P.C.

Counsel for Defendant:
John Hoffman, Esq.
Acting Attorney General of NJ
Lorraine K. Rak, Esq.
Chief, Deputy Attorney General
Consumer Fraud Protection
Glenn T. Graham, Esq.
Deputy Attorney General
Edward J. Mullings III, Esq.
Deputy Attorney General

By: Garry Furnari, J.S.C.
Decided: November 24, 2014

Introduction

This law suit challenges the authority of the State of New Jersey to investigate potential malware written by an out-of-state software developer which soon may be marketed over the Internet in New Jersey. The Plaintiff, a student at M.I.T.,

alleges that the New Jersey Division of Community Affairs (D.C.A.) is unlawfully regulating the Internet in violation of the dormant commerce clause of the United States Constitution. Plaintiff further claims there are no substantial contacts with New Jersey and no personal jurisdiction which would permit the D.C.A. investigation. Plaintiff further argues that the D.C.A. has exceeded its authority under the N.J. Consumer Fraud Act, N.J.S.A. 56:8-1 et seq. Plaintiff seeks a preliminary and permanent injunction quashing a subpoena issued by D.C.A.

Tidbit is a computer program created by Plaintiff and others at a Node Knockout Hackathon when Plaintiff was a nineteen-year-old freshman at MIT. Tidbit was designed to allow website operators to use, with consent, the excess under-utilized computing power of their customer's personal computers. When a web site is accessed, the customer's unused computing power will be harnessed by the website operator to earn money "mining" for Bitcoins. The consumer will benefit from an advertising free website.

The Defendant, D.C.A., has concerns that Tidbit as written or modified can be used to "hijack" consumers' computers without permission. D.C.A. argues that it has the authority under the N.J. Consumer Fraud Act to investigate this and other potential "malware" whenever it may affect unwary or unknowing consumers in New Jersey.

Factual Assertions Before the Court

It is important to note that there are virtually no facts offered by Plaintiff that are properly before the Court. Plaintiff's complaint is not verified. The factual assertions contained in the certification of counsel and briefs submitted by Plaintiff are improper hearsay and not based upon personal knowledge. As correctly noted by the Defendant, the Plaintiff's factual presentation is not: ". . . of record, judicially noticeable, nor stipulated . . . and thus in violation of N.J. Court Rule 1:6-6." Defendant's Reply Brief at page 3, citing comment to N.J. Court Rule 1:6-6; Gonzalez v. Ideal Tile Importing Co., 371 N.J. Super. 349, 358 (App. Div. 2004), aff'd, 184 N.J. 415 (2005).

The only facts offered by Plaintiff that are properly before the Court are contained in the Plaintiff's certification dated January 19, 2014. It states that:

1. Plaintiff is a 19 year old student at MIT;
2. Other than once attending a family function, Plaintiff has never been to or worked in New Jersey;
3. Tidbit, the computer code at issue in this litigation, was not developed in New Jersey;
4. There are no contracts or agreements with anyone in New Jersey concerning Tidbits;
5. Tidbits was never marketed: "exclusively or primarily to individuals in New Jersey."
6. Tidbit can be downloaded by anyone with Internet access whether they are in or out of New Jersey.

Certification of Jeremy Rubin, 1/19/14, Paragraphs 1-5.

Uncertified Factual Assertions of Plaintiff

Plaintiff makes various other allegations and assertions in his unverified complaint, certifications of his attorney and legal briefs. Although not properly before the Court, these assertions are repeated here to give proper context to the Plaintiff's action.

It is asserted that in the fall of 2013 Plaintiff participated in a 'Node Knockout Hackathon'. Plaintiff's Brief at page 3. This is where computer programmers gather and develop computer code in a both collaborative and competitive process. Id. at n.6. Plaintiff and his colleagues developed a program known as "Tidbit." It was designed, when implemented, to allow web site operators to "mine for Bitcoins" and earn money leveraging the amassed under-utilized computing power of consumers visiting that website. Id. at 3-4.

Plaintiff and Defendant both state that Bitcoins are a "virtual currency" that exist only online. Id. at 1. Bitcoins allow payments and money transfers without reference to a centralized bank or clearing house. Id. at 2. Rather, Bitcoins are stored in an online "wallet." Id. A large publicly accessible ledger called a "blockchain" records and verifies every transaction. Id.

The Plaintiff's brief describes the mechanics of a "Bitcoin" ledger as follows:

> The main purpose of the ledger is to prevent anyone from spending the same Bitcoin value twice ("double-spending"). In traditional financial systems, this function is performed by central banks (which issue hard-to-counterfeit physical currency instruments) and commercial banks (which maintain accounts and account ledger). In Bitcoin, the first transaction in the ledger that purports to transfer a certain balance is presumptively valid and any subsequent contradictory attempt to transfer that balance is presumptively invalid.

Id. at 2.

The amount of currency "in circulation" is fixed. However, new Bitcoins are generated and gradually added through what is referred to as "mining." Id. at 2-3. People create and earn new Bitcoins when they solve complex mathematical problems. Id. A "minor" who solves the relevant problem is credited with a "block reward" of Bitcoins for having accomplished this feat. Id. It is advantageous to employ the under-utilized computing power of a multitude of amassed personal computers to solve these complex mathematical problems. Id.

Tidbit is the creation of Plaintiff and others. Id. at 4. Plaintiff claims that it is a "proof of concept" but not a fully functioning program. Plaintiff describes Tidbit as follows:

> Tidbit is a computer code that allows [website] developers to replace website advertising [on a consumer's computer] by instead using a client's computer to mine for Bitcoins.

Id. at 4.

Web site operators will, with the consent of their customers, block the stream of advertising directed toward a customer. Id. However, the web site operator will replace their lost advertising income by using the under-utilized capacity of their customer's computers to mine for Bitcoins. Id. Apparently Tidbit, or their agent, will keep track how much 'mining' takes place and provide the website operators with appropriate Bitcoin credit. See Certification of Brian Morgenstern at ¶ 15 and Exhibit A, thereto.

Factual Assertions of Defendant

The D.C.A., is seeking to investigate whether the Tidbit code can or is also being used by website operators to 'hijack' N.J. consumer's computers to mine for Bitcoins. Defendant's Reply Memorandum at page 2. They assert that unwary New Jersey consumers may visit websites which have installed Tidbit but which fail to adequately inform them that their underutilized computer potential is about to be "tapped" for the benefit of the website operator and Tidbit. Certification of Brian Morgenstern at ¶ 9. The Tidbit program might permit unscrupulous website operators to "hijack" the computers of unknowing consumer and "mine" for Bitcoins or perform other unwanted tasks without consent. Defendant's Reply Memorandum at page 2. As noted in oral argument, the focus of the Defendant's

investigation is the notice to and consent of consumers in New Jersey before Tidbit is loaded onto their personal computers.

Defendant also fears other improper invasions of privacy might occur. At oral argument, the Court asked whether the Tidbit code, while taking control over portions of a consumer's computer and mining for Bitcoins, could also be used to access personal or financial information. The Defendant, through counsel, responded that this did not appear to be the purpose of Tidbit. But it was certainly plausible and worrisome and that it was something the D.C.A. wished to investigate.

Contrary to the Plaintiff's assertions that Tidbit is a mere proof of concept, the D.C.A. asserts that in November 2013 they discovered active Tidbit code on at least three websites registered and located in NJ. Certification of Brian Morgenstern at ¶ 10. Further there were advertisements urging web site operators to download Tidbit on a website located at http://www.tidbit.co.in. Id. at Exhibit A. The advertisement suggests that people running websites should:

> 1. Make an account-sign up with your Bitcoin wallet.
> 2. Paste the code - We'll give you a snippet to put in your website. . .
> (3) Cash out! - We'll send a transaction to your Bitcoin wallet.

Id. at 15.

The D.C.A., in December 2013, issued the subpoena and interrogatories that are at issue in this litigation. The subpoena seeks, among other things:

1. Information regarding unauthorized access of consumer's computers by Tidbit [Paragraph 3];
2. The code, source code, control logs and installation logs concerning Tidbit [Paragraph 5];
3. Any agreements between Tidbit and any website operator concerning Tidbit [Paragraph 6];
4. All documents concerning Bitcoins that may have been mined by Tidbit [Paragraph 6, 7];
5. Documents regarding the Bitcoin wallets used or associated with Tidbit [Paragraph 7,8];
6. All information regarding the users of Tidbit, and any consumer complaints [Paragraphs 9-13].

Certification of Hanni Fakhoury at Exhibit A.

The interrogatories further ask, among other things:

1. What benefit, if any, is received by consumers using Tidbit;
2. What benefits is received by website operators that install Tidbit and use their customer's computers to 'mine' for Bitcoins;
3. Information as to all websites that have used Tidbit;
4. What disclosure consumers are given that their computer is about to install Tidbit and about to allow someone to control their computer to 'mine' for Bitcoins.

Id. at Questions 9-30.

Following the subpoena and interrogatories, there was communication back and forth between the D.C.A. and the Plaintiff's counsel. Some of the communication was about an extension of time to respond as Plaintiff was taking final exams. Some of the communication was about a production

schedule for information to be produced by Plaintiff. In January, 2014 Plaintiff, through counsel, asserted that Plaintiff would not be responding to the D.C.A. subpoena and interrogatories. Plaintiff argued that it was refusing to provide any information as to Tidbit because the code was never functional and no Bitcoins have been mined.

The D.C.A. claims that their investigation determined otherwise. They allege that Tidbit code was active in New Jersey in January, 2014. Certification of Brian Morgenstern at ¶ 17. The D.C.A. received, after issuing subpoenas to some website operators, an 'account dashboard' from 'New Jersey coded websites' which they claim shows that Tidbits was in active use in New Jersey. Certification of Edward Mullin at ¶¶ 5-6. They allege in their verified certifications, that Plaintiff has affirmatively sent the Tidbit code to several New Jersey based entities and that Tidbits was active. Certification of Brian Morgenstern at ¶¶ 10, 19. After learning of the D.C.A. subpoena, the NJ coded websites identified by the D.C.A. stopped any active use of Tidbits. Id. at ¶ 18.

The D.C.A. asserts that in February 2014, they conducted an investigation with an undercover e-mail and anonymous Bitcoin wallet. Id. at ¶ 20. The D.C.A. was able to receive the Tidbit code from the Tidbit website. Id. This investigation, according to the D.C.A., revealed that in February 2014 it was still

possible to go on the Internet and download the Tidbit program. Id. at ¶ 21.

It is unclear from the conflicting statements of the parties whether it ever was possible or might still be possible to actually mine for Bitcoins using Tidbit. Plaintiff's briefs state that Plaintiff "left out the final interaction with P2Pool while we put together Terms and Conditions. . . . [The] Tidbit code was never fully functional and could not mine for Bitcoins." Plaintiff's Brief in Support of Order to Show Cause at page 4. Defendant D.C.A. argues otherwise. See Certification of Brian Morgenstern at ¶¶ 9-11. Some of this uncertainty results from the lack of a verified complaint or other verified information submitted by the Plaintiff.

Legal Analysis

The New Jersey Consumer Fraud Act

The Attorney General of the State of New Jersey and their designees, including Defendant, are given broad investigatory powers under the N.J. Consumer Fraud Act, N.J.S.A. 56:8-1 et seq. The Act prohibits the use of any "unconscionable commercial practice, deception, fraud, false pretense, false suppression, or omission of any material fact with intent that others rely upon such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise . . . " N.J.S.A. 56:8-2. The expansive definition of merchandise

includes "any objects, wares, goods, commodities, services or anything offered directly or indirectly to the public for sale." N.J.S.A. 56:8-1(c).

The act specifically authorizes actions by the Attorney General and such others as are designated to enforce potential fraud against consumers in New Jersey. It permits the issuance of administrative subpoena and the authority to conduct hearings. N.J.S.A. 56:8-4. Enforcement of administrative subpoenas are through actions filed with the Superior Court N.J.S.A. 56:8-6.

As was stated in Cox v. Sears Roebuck & Co., 138 N.J. 2, 15-16 (1994):

> Courts have emphasized that like most remedial legislation, the Act should be construed liberally in favor of consumers. Although initially designed to combat "sharp practices and dealings" that victimized consumers by luring them into purchases through fraudulent or deceptive means, the Act is no longer aimed solely at "shifty, fast-talking and deceptive merchant[s]" but reaches "nonsoliciting artisans" as well. Thus, the Act is designed to protect the public even when a merchant acts in good faith. Moreover, we are mindful that the Act's provision authorizing consumers to bring their own private actions is integral to fulfilling the legislative purposes, and that those purposes are advanced as well by courts' affording the Attorney General "the broadest kind of power to act in the interest of the consumer public." Levin v. Lewis, 179 N.J. Super. 193 (App. Div. 1981).

Cox v. Sears Roebuck & Co., 138 N.J. at 15-16 (citations omitted).

The provisions of the act are to be interpreted and applied broadly in order to accomplish the remedial purpose of the act and "root out" consumer fraud. Lamelledo v. Beneficial Mgmt. Corp., 150 N.J. 255, 264 (1997). This authority to investigate extends to persons who are engaging or are about to engage in practices deemed unlawful. N.J.S.A. 56:8-3. The act is designed to protect against actions, even when a merchant act in good faith. Cox, supra, 138 N.J. at 16.

It is clear to the Court that the Consumer Fraud Act, with its broad enumerated powers, would authorize the subpoena and the investigation at issue in this action if the Plaintiff physically resided in the State of New Jersey. The activity being investigated falls within the confines of the enumerated powers of the statute. The statute was designed to protect New Jersey consumers from the harm envisioned by the Defendant in this matter. Protecting the public from potential "malware" programs or programs that can be readily modified to create malware clearly falls within the scope of the New Jersey Consumer Fraud Act. Plaintiff's counsel candidly admitted this at oral argument.

Plaintiff argues that the statute should not extend to out-of-state actors. The statute, however, does not limit the investigative authority to actors physically present in the State of New Jersey. Rather, the statute focuses on the

commercial activity which will result in deception or fraud to citizens in New Jersey regardless of the physical location of the actor. N.J.S.A. 56:8-2. The enforcement authority does not limit the scope of subpoenas and investigations to persons located in N.J. Rather, the Consumer Fraud Act says that the Attorney General may issue subpoenas and conduct investigations "on any person." N.J.S.A. 56:8-4.

The investigatory process is not limited by statute to the physical environs of New Jersey. The Act specifically contemplates service of out-of-state subpoenas and investigations. It state that the Attorney General may require a person to file a statement or report or answer a subpoena after personal service. N.J.S.A. 56:8-5. Personal service can be made upon an actor "without this State." N.J.S.A. 56:8-5(a) (emphasis added). Service can also be achieved against actor by registered mail "within or without this State." N.J.S.A. 56:8-5(b) (emphasis added). The statute provides that service can be perfected in such a fashion "as the Superior Court may direct in lieu of personal service within this State." N.J.S.A. 56:8-5(d).

The Court has serious concerns that the Defendant, with this investigation, may be acting to discourage creative and "cutting edge" new technology. From the evidence before the Court, it appears that the Tidbit program and other similar

creative endeavors serve a useful and legitimate purpose. There is nothing presented to the Court that evidences an inherently improper or malicious intent or design by Plaintiff. Rather, Tidbits appears to be an instrumentality or tool that has great potential for positive utility. The Court is mindful, however, of the State's concerns that this tool could also be subject to abuse and misuse.

Given the broad scope of the statute, the expansive language used by the legislature and the lack of geographic limitation, the Court finds that the subpoena issued by the Defendant is, on its face, a proper and appropriate exercise of authority under the N.J. Consumer Fraud Act. The actions under investigation clearly fall within the purview of the Act. The investigation involves potential commercial activity occurring in New Jersey and potential malware infecting the computers of New Jersey consumers, regardless of the geographic location of the actor.

In Personam Jurisdiction/Minimum State Contacts

The next issue that needs to be addressed is whether the Defendant has personal jurisdiction over the Plaintiff. The issue of personal jurisdiction in the Internet era is an evolving area of the law. The U.S. Supreme Court recently discussed personal jurisdiction due to an individual's "virtual contacts" with a forum state. It said:

> Respondents warn that if we decide petitioner lacks minimum contacts in this case, it will bring about unfairness in cases where intentional torts are committed via the Internet or other electronic means (e.g., fraudulent access of financial accounts or "phishing" schemes). . . . [T]his case does not present the very different questions [of] whether and how a Defendant's virtual "presence" and conduct translate into "contacts" with a particular State...
>
> We leave questions about virtual contacts for another day.

Walden v. Fiore, 134 S. Ct. 1115, 1125 n.9; 188 L. Ed. 2d 12 (2014).

Plaintiff argues that the issue of "virtual contacts" that the U.S. Supreme Court declined to address in Walden is central to the present action.

The New Jersey Supreme Court, in Blakley v. Continental Airlines, Inc., 164 N.J. 38 (2000) stated:

> [I]n International Shoe Co. v. Washington, the Court . . . held that a state court's assertion of personal jurisdiction does not violate the Due Process Clause if the Defendant has "certain minimum contacts with it such that the maintenance of the suit does not offend `traditional notions of fair play and substantial justice." 326 U.S. 310, 316 (1945).

Blakley v. Continental Airlines, Inc., 164 N.J. at 65.

The Court further stated:

> [T]he test for "due process requires only that in order to subject a Defendant to a judgment in personam, if he be not present within the territory of the forum, he have certain minimum contacts with it such that the maintenance of the suit does not offend `traditional notions of fair play and substantial justice.'" International Shoe Co. v. Washington, (quoting Milliken

v. Meyer). Those unchanging commands of due process govern every foray into the realm of long-arm jurisdiction over non-residents.

Id. at 66 (citations omitted.)

The recent decision of the Appellate Division in Patel v. Karnavati America, LLC, 437 N.J. Super. 415 (App. Div. 2014), provides an extensive discussion of the general law in New Jersey concerning personal jurisdiction. The court stated that the minimum contacts "analysis is fact sensitive and must be undertaken 'on a case-by-case basis.'" Id. at 424 (citations omitted). The court further stated:

> It is also well settled that the requisite quality and quantum of contacts is dependent on whether general or specific jurisdiction is asserted . . .
>
> In the context of specific jurisdiction, the minimum contacts inquiry must focus on the relationship among the Defendant, the forum, and the litigation. [W]hen the Defendant is not present in the forum state, it is essential that there be some act by which the Defendant purposefully avails [itself] of the privilege of conducting activities within the forum state, thus invoking the benefit and protection of its laws.
>
> . . . Thus, the ultimate question is whether [Defendant] submitted to the judicial power of New Jersey in connection with its activities directed at the State, justifying specific jurisdiction in a suit arising out of or related to the Defendant's contacts with the forum.

Id. (internal citations and quotations marks omitted).

Personal jurisdiction in the Internet era for 'virtual contacts' with a given forum was addressed in Zippo Manufacturing Co. v. Zippo Dot Com, Inc., 952 F.Supp. 1119 (W.D.Pa. 1997). The plaintiff was an established manufacturer,