NOT FOR PUBLICATION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,

based in Pennsylvania, of the "Zippo" lighter. The defendant was a California company of a very similar name which offered access to the Internet to the public. Id. at 1121. The California company argued that it did not have offices, employees or agents in Pennsylvania. It claimed that it did have a few customers in Pennsylvania at about two percent of its customer base. Id. There was, however, no specific advertising for Pennsylvania residents. Id. They grew their customer base in Pennsylvania and elsewhere by postings on their website. Id.

The court held that there was a three-prong test for determining whether a court had personal jurisdiction in these circumstances. The court stated:

> [T]he likelihood [that] personal jurisdiction can be constitutionally exercised is directly proportionate to the nature and quality of commercial activity that an entity conducts over the Internet. This sliding scale is consistent with well-developed personal jurisdiction principles. At one end of the spectrum are situations where a Defendant clearly does business over the Internet. If the Defendant enters into contracts with residents of a foreign jurisdiction that involve the knowing and repeated transmission of computer files over the Internet, personal jurisdiction is proper. At the opposite end are situations where a Defendant has simply posted information on an Internet Web site which is accessible to users in foreign jurisdictions. A passive Web site that does little more than make information available to those who are interested in it is not grounds for the exercise personal jurisdiction. The middle ground is occupied by interactive Web sites where a user can exchange information with the host computer. In these cases, the exercise of jurisdiction is determined by examining the level of interactivity and

commercial nature of the exchange of information that occurs on the Web site.

Id. at 1124 (citations omitted).

Similarly, in Toys 'R' US, Inc. v. Step Two, S.A., 318 F.3d 446 (3d. Cir. 2003), the court had before it a case venued in New Jersey involving a trademark infringement claim. The New Jersey-based Toys 'R' Us sued a Spanish company known as Step Two S.A., which was doing business with similar product lines over the Internet. The Plaintiff claimed the Spanish company used their Internet web sites to "engage in trademark infringement, unfair competition, misuse of the trademark notice symbol, and unlawful "cybersquatting." Id. at 448.

The court stated:

> The advent of the Internet has required courts to fashion guidelines for when personal jurisdiction can be based on a Defendant's operation of a web site. Courts have sought to articulate a standard that both embodies traditional rules and accounts for new factual scenarios created by the Internet. Under traditional jurisdictional analysis, the exercise of specific personal jurisdiction requires that the "Plaintiff's cause of action is related to or arises out of the Defendant's contacts with the forum." Beyond this basic nexus, for a finding of specific personal jurisdiction, the Due Process Clause of the Fifth Amendment requires (1) that the "Defendant ha[ve] constitutionally sufficient `minimum contacts' with the forum," and (2) that subjecting the Defendant to the court's jurisdiction comports with `traditional notions of fair play and substantial justice,. The first requirement, "minimum contacts," has been defined as "some act by which the Defendant purposefully avails itself of the

> privilege of conducting activities within the forum State, thus invoking the benefits and protections of its laws." Second, jurisdiction exists only if its exercise "comports with traditional notions of fair play and substantial justice," *i.e.*, the Defendant "should reasonably anticipate being haled into court" in that forum.

Id. at 451 (citations omitted).

Applying these principles to the present matter, it appears to the Court that there is personal jurisdiction over the Defendant. The New Jersey long-arm statute is expansive. It provides that this Court can exercise "in personam jurisdiction over a non-resident [party] consistent with due process of law." R. 4:4-4(b)(1). Such jurisdiction extends to the outermost limits as permitted by the U.S. Constitution. Avdel Corp. v. Mecure, 58 N.J. 264 (1971); Bayway Ref. Co. v. State Util., Inc., 333 N.J. Super. 420, 428 (App. Div. 2000).

It is difficult to evaluate the minimum contacts between Plaintiff and New Jersey given the paucity of certified material facts properly before the Court. But, based upon the record as it exists, it appears that Plaintiff does have sufficient minimum contacts with New Jersey to sustain personal jurisdiction. The Defendant, in their certified pleadings and certifications, alleges that the Tidbit Code has or is doing business with web sites located in New Jersey. The Tidbit code developed by the Plaintiff was found on several New Jersey

websites. Certification of Brian Morgenstern at ¶ 10. Further, Defendant asserts that the Tidbit code was active on the New Jersey Coded Websites in November 2013. Id. at ¶¶ 10-11. Later, contrary to the assertions of the Plaintiff, the state believes the Tidbit website was active in March, 2014. Id. at ¶ 19.

The Tidbit website urges website operators, in New Jersey and elsewhere, to download Tidbits and "[L]et your visitors help you mine [for] Bitcoins". Id. at ¶ 14. The website, apparently solicits potential customers, in New Jersey and elsewhere, to attach Tidbit code to their customer's computers and then have the website operator use their customer's computers to generate revenue through mining for Bitcoins. Id. at ¶ 15.

The Tidbit website invites an ongoing business relationship between Tidbit and other website operators. The last step listed in the posting cited above advises a web site operator to "(3)Cash out! - We'll send a transaction to your Bitcoin wallet." Id. at ¶ 15. This implies an ongoing series of transactions between Tidbits and web site operators, some of whom are based in New Jersey.

This is not a matter involving mere "postings" of material on a bulletin board or list serve. See Maritz, Inc. v. Cybergold, Inc., 947 F.Supp. 1328 (E.D.Mo.1996); Goldhaber v. Kohlenberg, 395 N.J. Super. 380 (App. Div.

2007); American Libraries Association v. Pataki, 969 F. Supp. 160 (S.D.N.Y. 1997). Rather, the Plaintiff has or would like to personally avail himself of the privilege of conducting commercial transactions with web site operators located in New Jersey. See Silverman v. Berkson, 141 N.J. 412 (1995).

This interaction with New Jersey includes both website operators utilizing Tidbit, some of whom are located in New Jersey and New Jersey consumers who have computers connected to such web sites. Both groups are directly impacted by what the Defendant characterizes as potential malware.

The Tidbit business model, as so far revealed in the pleadings and the assertions of the parties, anticipates a download of Tidbits by a website operator, an insertion of Tidbit into the Website customer's computer and the mining of Bitcoins by the website operator. At that point in this business relationship, a website operator will "cash out" by again contacting Tidbits or its designee and having the income earned through "mining" accounted for and distributed via some formula not yet revealed by the investigation.

This business model places the relationships between the parties in the first or second tier of the Zippo sliding scale. See Zippo Mfg. Co., supra, 952 F.Supp. at 1124. The

Plaintiff, under this mode, clearly is conducting business over the Internet. The Plaintiff is soliciting and entering into contracts with residents of a foreign jurisdiction, including New Jersey web site operators. These contracts and transactions seem to involve the knowing and repeated transmission of computer files over the Internet. Id.

In some instances, Plaintiff is directly entering into contracts with New Jersey based website operators for commercial gain. In other instances, Plaintiff is entering into contract with website operators whose expressed desire is to provide services to and engage in commerce with consumers in New Jersey. In either instance, the Plaintiff is entering into contracts with residents of a foreign jurisdiction for the sale of a product and services over the Internet.

It appears to the Court that Tidbits is personally availing itself of the privilege of conducting business in New Jersey. Waste Mgmt. Inc. v. Admiral Insur. Co., 138 N.J. 106 (1994). From the facts properly before the Court, there appears to be continuous, systemic, and ongoing contact between Tidbits and web site operators who offer services to New Jersey consumers.

There is a reasonable expectation that Plaintiff could be "haled into court" for potentially deceptive or fraudulent transactions between Tidbits and website operators which cater to New Jersey customers. Similarly, Plaintiff should have a reasonable expectation that they could be "haled" into court if there was deceptive and fraudulent conduct caused by Tidbits that directly impacted the end user, New Jersey consumers. Plaintiff is not being investigated by New Jersey because of: "random," "fortuitous," or "attenuated" contacts. See Burger King Corp. v. Rudzewicz, 471 U.S. 462, 475, 105 S. Ct. 2174, 2183, 85 L. Ed. 2d 528, 542 (1985) (internal quotation marks omitted).

The harm envisioned by the Defendant is substantial. If the D.C.A. investigation in fact discloses actual or the potential malware, New Jersey consumers may have their computer's "co-opted" or "hijacked" without their consent by unscrupulous website operators using the Tidbit code. If the concerns of the D.C.A. are borne out, this is exactly the type of "unconscionable commercial practice, deception, fraud, false pretense, false promise, misrepresentation, or the knowing concealment, suppression, or omission of any material fact . . . in connection with the sale or advertisement of merchandise"

that the Consumer Fraud Act was intended to encompass. N.J.S.A. 56: 8-2.

It may be that the Plaintiff is acting in good faith. The evidence presently before the Court points in that direction. But another of the Defendant's concern, with some justification, is that others may pervert the Tidbit program and cause harm. The Consumer Fraud Act was designed to protect the public even when a merchant acts in good faith. Cox, supra, 138 N.J. at 16.

The Court is mindful that the Plaintiff has never physically entered New Jersey in any substantial or relevant fashion. However, the Supreme Court in New Jersey has held that: The mere fact that neither Defendant nor the [product] was ever physically present in New Jersey does not preclude a finding that minimum contacts existed. Lebel v. Everglades, 115 N.J. at 127.

As the U.S. Supreme Court stated in Burger King Corp. v. Rudzewicz, 471 U.S. 462 (1985):

> Although territorial presence frequently will enhance a potential Defendant's affiliation with a State and reinforce the reasonable foreseeability of suit there, it is an inescapable fact of modern commercial life that a substantial amount of business is transacted solely by mail and wire communications across state lines, thus obviating the need for physical presence within a State in which business is conducted. So long as a commercial actor's efforts are "purposefully directed" toward

> residents of another State, we have consistently rejected the notion that an absence of physical contacts can defeat personal jurisdiction there.

Id. at 476.

There can be no doubt that the Plaintiff's marketing activities will, under Plaintiff's business plan as so far revealed, target commercial relationships with New Jersey website operators and New Jersey consumers. See Calder v. Jones, 465 U.S. 783; S. Ct. 1482; 79 L. Ed. 2d 804 (1984). Given the ongoing or anticipated business relationships between Tidbits with websites and residents of New Jersey, it is appears to the Court that Plaintiff's efforts are "purposely directed" toward residents of New Jersey. Plaintiff has personally availed himself of the privileges, benefits and protections of New Jersey Law. Plaintiff must also be mindful of the associated responsibilities of doing business in New Jersey.

Plaintiff asserts that the subpoena offends the traditional concepts of fair play and substantial justice. See Lebel, supra, 115 N.J. at 127. The Court must balance the burden upon the Plaintiff to come to New Jersey and answer questions versus the interest of New Jersey in protecting its citizens. The Court must consider whether effective and convenient relief is being given and the judicial efficiency of continuing this action.

This balance seems clear to the Court. The burden on Plaintiff to respond to an investigation in New Jersey is minimal. The potential harm to consumers in New Jersey, if the concerns of the D.C.A. are justified, is substantial. The subpoenas and interrogatories, on their face, do not appear overbroad or burdensome. The state had a substantial interest in furthering substantive social policies including consumer protection. Harley Davidson Motor Co., Inc. v. Anderson Die Casting, Inc., 292 N.J. Super. 62 (App. Div. 1996), aff'd, 150 N.J. 489 (1997); Lebel, supra, 115 N.J. 317 (1989). That includes requiring computer developers to answer questions about whether their code is or can be manipulated to infect the computers of New Jersey consumers with malware.

The Court finds that there is in personam jurisdiction over the Plaintiff in New Jersey. The Plaintiff has constitutionally sufficient minimum contacts with New Jersey and subjecting the Plaintiff to the jurisdiction of the Court in New Jersey does not offend traditional notions of fair play and substantial justice.

Dormant Commerce Clause

Plaintiff also argues that the subpoena is a violation of the dormant commerce clause of the U.S Constitution. Art. I Section 8, Cl. 3. The claim is that New Jersey is imposing an unfair burden on interstate commerce and is attempting to

improperly regulate the Internet. It is argued that the Defendant is issuing subpoenas concerning software stored out of state, which can be downloaded by anyone with an Internet connection. Plaintiff states it has no ability to control Tidbit once downloaded by a website operator. A citation is made to American Libraries Assn. v. Pataki, 996 F. Supp. 160 (S.D.N.Y. 1997) and American Booksellers Foundation v. Dean, 342 F.3d 96 (2d. Circuit 2003) for the proposition that the Defendant's investigation constitutes an impermissible direct regulation of interstate commerce.

American Libraries Assn v. Pataki involved a challenge to a New York statute regulating pornography on the Internet. Similarly, American Booksellers Foundation v. Dean dealt with a Vermont statute that restricted sexually explicit material that might be viewed by minors and whether the statute violated the dormant commerce clause. The Court in American Booksellers v. Dean said:

> The "dormant" Commerce Clause protects against state regulations that erect barriers against interstate trade. Dormant Commerce Clause doctrine distinguishes between state regulations that "affirmatively discriminate" against interstate commerce and evenhanded regulations that burden interstate transactions only incidentally. Regulations that clearly discriminate against interstate commerce [are] virtually invalid per se, while those that incidentally burden interstate commerce will be struck down only if the burden imposed on such commerce is clearly excessive in relation to the putative local benefits.

Id. at 102 (citations omitted).

There is no bright line distinguishing the state regulations that are per se invalid and those subject to the balancing test. Id. Courts generally examine the nature of the burden to interstate commerce and the effect on local and interstate activity caused by the State regulations. Id. Factors include the costs imposed by the regulations, the possibility of inconsistent regulations between jurisdictions and whether the regulations alter the interstate flow of goods. The Court should also weigh the impact of the in-state regulations outside the jurisdiction and whether the impact falls more heavily on out-of-state actors. Id. at 102-03.

There is a balancing that the Court must apply between the legitimate state interest to investigate and deter consumer fraud and the burden imposed on interstate commerce. See Washington State Apple Comm'n, 432 U.S. 333, 350; 97 S. Ct. 2434; 53 L. Ed. 2d 383 (1977). The dormant commerce clause protects against inconsistent legislation from different jurisdictions with different and burdensome regulatory schemes.

It is true that the Internet is a medium that, in general, requires national regulation rather than piecemeal state-by-state regulation. There is certainly the justified fear of developers of being hauled into various states with inconsistent

laws to face a myriad of different regulatory schemes. Pataki, 969 F. Supp. at 182. The Court should not permit the creative and innovative and spirit behind Tidbit and similar new applications to be threatened by heavy handed, unwarranted or ill advised investigations.

However, not every exercise of state power with an impact on interstate commerce is invalid. Edgar v. Mite Corp., 457 U.S. 624, 640; 102 S. Ct. 2629, 2639, 73 L. Ed. 2d 269, 281 (1982); Pike v. Bruce Church, Inc., 397 U.S. 137, 142; 90 S. Ct. 844, 847, 25 L. Ed. 2d 174, 178 (1970). Even-handed regulation that indirectly affects interstate commerce accompanied by a legitimate local public interest should be upheld. Edgar, supra, 457 U.S. at 640.

Although it may pose a burden on interstate commerce, regulation of consumer protection is historically a matter of legitimate local concern. SPGGC, Inc. v. Blumenthal, 408 F. Supp. 2d 87, 96 (D. Conn. 2006); Cliff v. Payco General American Credits, Inc., 262 F.3d 1113, 1125 (11th Cir 2004); Florida Lime and Avocado Growers, Inc. v. Paul, 373 U.S. 132, 135; 83 S. Ct. 1210, 1236, 10 L. Ed. 2d 248, 277 (1963).

No evidence has been presented that the investigation by the Defendant is in conflict with the actions of other jurisdictions. It does not appear that there will be layers of inconsistent regulations adopted in different forums. The

investigation by the DCA seems "even handed" and not intended to discriminate between in-state and out-of-state actors. The subpoenas and interrogatories at issue in this litigation have only an incidental effect on interstate commerce and are not clearly excessive in comparison to the local benefits being protected. Pike, supra, 397 U.S. 137 (1970).

This is not regulation of commerce that occurs wholly outside the borders of the state or discrimination against out-of-state interests in favor of in-state interest. See Granholm v. Heald, 544 U.S. 460, 1225 S. Ct. 1885; 161 L. Ed. 2d 796 (2005). State consumer protection statutes should not be held invalid merely because the Internet exists.

There exist clear, legitimate and substantial state interests in this matter. Defendant is seeking information as to whether there may be violations of the privacy rights of New Jersey citizens and whether Tidbit can be used as a vehicle to hijack consumer's computers. On its face, the investigation by the Defendant, D.C.A. does not impose an unfair burden on interstate commerce or violate the dormant commerce clause of the U.S. Constitution.

Immunity From Criminal Prosecution

Plaintiff asserts that the Consumer Fraud Act permits a person to raise a privilege against self-incrimination. The party claiming the privilege must "identify some law" as the

source of the privilege. Verniero v. Beverly Hills Ltd., Inc. 316 N.J. Super. 121 (App. Div. 1998). Plaintiff asserts that compelled testimony violates N.J. common law and the Fifth Amendment to the U.S. Constitution.

To be protected a party must establish a compulsion to testify, a potential for incrimination and a testimonial communication or act. In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335 (11th Cir. 2012); United States v. Ghidoni, 732 F.2d 814, 816 (11th Cir. 1984); United States v Authement, 607 F.2d 1129, 1131 (5th Cir. 1979). In this case Plaintiff asserts compulsion both in terms of being required to provide testimony and being required to produce documents.

There is also implicated the "foregone conclusion" theory. The act of producing documents is testimonial in nature. However, the state can defeat the privilege if the requested documents do not reveal anything that the government did not already know and the testimony is simply a "foregone conclusion." See Fisher v. United States, 425 U.S. 391, 411; 96 S. Ct. 1569, 1581, 48 L. Ed. 2d 39, 56 (1976) and United States v. Hubbell, 530 U.S. 27, 44; 120 S. Ct. 2037, 2047, 147 L. Ed. 2d 24, 41 (2000) (determining that the "existence and location" of the documents in question were a "foregone conclusion" and thus did not implicate any Fifth Amendment privileges). Some of

the implications of this theory in the Internet era are explored in In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335 (11th Cir. 2012); see also Decrypting the Fifth Amendment: The Limits of Self Incrimination in the Digital Era, University of Pennsylvania Journal of Constitutional Law, Vol. 15, Article 2 (2011).

It appears to the Court that this discussion of immunity is premature. At this juncture, Plaintiff is improperly asserting a blanket right not to produce any information. See State Farm Indem. Co. v. Warrington, 350 N.J. Super. 379, 388 (App. Div. 2002). There is a difference between a blanket refusal to answer questions and the assertion of privilege as to individual questions. Id. In the present matter, Plaintiff must answer the subpoena and interrogatories, with proper assertions of privilege when and where appropriate. It will be up to the appropriate reviewing authority, in any enforcement proceeding by the Defendant D.C.A., to judge the correctness of the privilege being asserted.

Conclusion

The subpoena and interrogatories issued by the D.C.A. are, at least on their face, a proper and valid exercise of the broad police powers conferred upon the D.C.A. by the N.J. Consumer Fraud Act. For the reasons noted above, the Court determines that there exists sufficient minimum contacts with New Jersey to

confer personal jurisdiction over the Plaintiff. Plaintiff's arguments regarding the privilege against self-incrimination are premature. Plaintiff's arguments regarding the broad scope of information being sought will be considered by this or some other Court if an appropriate enforcement action is filed. An order will be entered requiring the Plaintiff to comply with the subpoena and interrogatories subject to such defenses and privileges as may be appropriately raised by Plaintiff. The Court further grants the Defendant's motion to dismiss this action.