UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES	)	
v.	)	No. 11-10260-NMG
AARON SWARTZ	)	

MOTION TO DISMISS COUNTS 1 AND 2 OF INDICTMENT AND INCORPORATED MEMORANDUM OF LAW

Now comes the defendant Aaron Swartz and respectfully moves that this Honorable Court dismiss Counts 1 and 2 of the indictment.

As reason therefor, defendant states:

1. Counts 1 and 2 charge him with wire fraud in violation of 18 U.S.C. §1343.

2. Section 1343 does not encompass the conduct charged in this case.

3. Section 1343 is void for vagueness in violation of the Due Process Clause as applied to the circumstances of this case.

THE DEFENDANT REQUESTS A HEARING ON THE WITHIN MOTION.

LOCAL RULE 7.1(A)(2) STATEMENT

The undersigned counsel has conferred with AUSA Stephen Heymann. The government opposes the dismissal remedy sought and will respond to defendant's request for a hearing in its response to the motion.

MEMORANDUM OF LAW

Counts 1 and 2 of the indictment charge Swartz with wire fraud in violation of 18 U.S.C. §1343. The indictment alleges that Swartz "having devised and intended to devise a scheme and

artifice to defraud and for obtaining property – journal articles digitized and distributed by JSTOR, and copies of them – by means of material false and fraudulent pretenses and representations, transmitted and caused to be transmitted by means of wire communication in interstate commerce writings, signs, and signals – that is, communications to and from JSTOR's computer servers – for the purpose of executing the scheme, and aiding and abetting it, including on or about" October 9, 2010, (Count 1) and January 4-6, 2011 (Count 2). Indictment at 10-11, ¶35. Essentially, the indictment alleges that Swartz gained access to the MIT electronic communications network through various mechanisms, and then, having obtained that access, used it to gain access to JSTOR's website, from which he then downloaded a substantial quantity of digitized journal articles.

I. SECTION 1343 DOES NOT APPLY TO THE CONDUCT CHARGED IN THIS CASE.

To convict Swartz of an offense under §1343, the government must prove beyond a reasonable doubt: "[his] knowing and willing participation in a scheme or artifice to defraud with the specific intent to defraud, and (2) the use of . . . interstate wire communications in furtherance of the scheme." *United States v. Vazquez-Botet*, 532 F.3d 37, 63 (1st Cir. 2008), *quoting United States v. Sawyer*, 85 F.3d 713, 723 (1st Cir. 1996). An essential element of the offense is that the defendant must have made a *material* misrepresentation or omission of fact. *E.g., Neder v. United States*, 527 U.S. 1, 25 (1999); *Mendez Internet Management Services, Inc. v. Banco Santander de Puerto Rico*, 621 F.3d 10, 15 (1st Cir. 2010); *United States v. Blastos*, 258 F.3d 25, 27 (1st Cir. 2001). A misrepresentation or omission is material only if it has "a natural tendency to influence, or is capable of influencing, the decision of the decisionmaking body to which it is addressed." *United States v. Moran*, 393 F.3d 1, 13 (1st Cir. 2004), *quoting Neder*, 527 U.S. 1, 16. *See, e.g., United*

States v. Philip Morris USA, Inc., 566 F.3d 1095, 1122 (D.C.Cir. 2009)(Materiality requirement is met "if the matter at issue is of importance to a reasonable person making a decision about a particular matter or transaction"); *United States v. Spirk*, 503 F.3d 619, 621 (7th Cir. 2007)(material falsehoods are those "likely to be significant to a reasonable person deciding what to do");*United States v. Heppner*, 519 F.3d 744, 749 (8th Cir. 2008); *United States v. Lawrence*, 405 F.3d 888, 901 (10th Cir. 2005)("to determine whether a statement is material the appropriate test is to examine whether it has a natural tendency to influence, or is capable of influencing a decision or action by another"). The first fatal flaw in Counts 1 and 2 is that none of the false statements alleged in the indictment were made to a "decisionmaker" or to person making a decision.[1] Instead, they were uniformly statements to a computer or information passed between computers. The indictment alleges the transmission of the following information:

- that when registering as a guest on the MIT network, Swartz used the fictitious names "Gary Host" and "Grace Host," each time obtaining a different IP address; Indictment, ¶14(a), 20, 27(a),
- that when registering as a guest on the MIT network, Swartz gave the computer's client name as "ghost laptop" and "ghost macbook," Indictment, ¶14(b), 20;
- that when registering as a guest on the MIT network, Swartz provided the email address of "ghost@mailinator.com" and "ghost42@mailinator.com," Indictment, ¶14(c), 20;
- that, when JSTOR blocked access to the IP address which Swartz's computer had been using, Swartz established a new IP address which allowed the continued downloading of articles, Indictment, ¶16(b);
- that after MIT blocked access by the computer with the Acer's MAC address, Swartz twice obtained another guest registration by "spoofing," *i.e.*, changing, the Acer's MAC address, again using the name "Gary Host" or "Grace Host" and the client name "ghost laptop," which led to the laptop's receiving a new IP address,

[1] Many of them were not in fact material false statements of fact at all. *See* Section II, *infra.*

Indictment, ¶¶19(a)-(c), 27(a)-(c);

- that during November-December, 2010, Swartz bypassed the guest registration process by connecting directly to the network and assigning himself two new IP addresses, Indictment, ¶24;

- that Swartz, through the use of MIT IP addresses, made it appear that he was affiliated with MIT, Indictment, ¶34(a);

- that Swartz used an automated collection device which made it appear that multiple people were requesting articles rather than a single person making multiple requests, Indictment, ¶34(c).

This information was all either provided by Swartz or Swartz's laptop to MIT's computer network (name, client name, email address) or was information automatically transmitted from one computer to another (IP addresses, MAC addresses, information about the program running). What is wholly missing here is any person or "decisionmaker" to whom the statements – if they were statements at all – were addressed. There was no person or decisionmaker whose "decision" the information had a tendency to influence or was capable of influencing. Nothing in the wire or mail fraud statutes or the case law construing them suggests that their reach extends to information or statements or omissions which are never reviewed or considered by a human being and do not tend to, nor are they capable of, influencing a decision by person. "Materiality" is an element incorporated directly from common law fraud, *see Neder*, 527 U.S. at 21-25, to which the concepts of machines communicating with each other in the complete absence of human agency and of machines robotically performing various functions would have been utterly foreign and incomprehensible, just as the concept that automatic responses by machines constituted "decisionmaking" would have been.

The rule of lenity precludes stretching the wire fraud statute to reach the conduct charged in this case. The rule of lenity "requires ambiguous criminal laws to be interpreted in favor of the

defendants subjected to them." *United States v. Santos*, 553 U.S. 507, 2025 (2008). *See United States v. Skilling*, 130 S.Ct. 2896, 2932 (2010)("[A]mbiguity concerning the ambit of criminal statutes should be resolved in favor of lenity"). Critically, the rule of lenity "ensures fair warning by resolving ambiguity in a criminal statute as to apply it only to conduct clearly covered." *United States v. Lanier*, 520 U.S. 259, 266 (1997).

> In various ways over the years, we have stated that when choice has to be made between two readings of what conduct Congress has made a crime, it is appropriate, before we choose the harsher alternative, to require that Congress should have spoken in language that is clear and definite. . . . This principle is founded on two policies that have long been part of our tradition. First, a fair warning should be given to the world in language that the common world will understand, of what the law intends to do if a certain line is passed. To make the warning fair, so fair as possible the line should be clear. . . . Second, because of the seriousness of criminal penalties, and because criminal punishment usually represents the moral condemnation of the community, legislatures and not courts should define criminal activity. This policy embodies the instinctive distastes against men languishing in prison unless the lawmaker has clearly said they should. . . . . Thus, where there is ambiguity in a criminal statute, doubts are resolved in favor of the defendant.

United States v. Bass, 404 U.S. 336, 347-48 (1971)(internal quotation marks and citations omitted). Nothing in the wire fraud statute clearly and definitely extends its reach to communications between computers.

In fact, Congress *has* spoken regarding use of computers to commit fraud – but in 18 U.S.C. §1030, not in the wire or mail fraud statutes. Congress' enactment of §1030(a)(2), criminalizing "intentionally access[ing] a computer without authorization or exceed[ing] authorized access, and thereby obtain[ing] . . . . [i]nformation from any protected computer" and §1030(a)(4), criminalizing "knowingly and with intent to defraud, access[ing] a protected computer without authorization, or exceed[ing] authorized access, and by means of such conduct further[ing] the intended fraud and

obtain[ing] anything of value" – essentially the conduct with which Swartz is charged[2] – provides compelling evidence that it did not believe that such conduct was already encompassed within the reach of the wire fraud statute. Counts 1 and 2 should be dismissed.

II. THE STATEMENTS AT ISSUE WERE NOT FALSE STATEMENTS OR MISREPRESENTATIONS OR OMISSIONS OF FACT.

Swartz's giving the computer's client name as "ghost laptop" and "ghost macbook" when registering as a guest on the MIT network," Indictment, ¶14(b), 20, was not false, and certainly not materially so, because, as the indictment alleges, the client name is one chosen by the user and is simply used to identify the computer on the network. Indictment, ¶14(b). The user is free to choose any name he wishes, and whatever that name is suffices to identify the computer on the network. Here, MIT was always able to identify the computers in use as either "ghost laptop" or "ghost macbook." The use of those client names was not a fraudulent misrepresentation or omission of material fact.

Similarly, Swartz's providing the email address of "ghost@mailinator.com" and "ghost42@mailinator.com that when registering as a guest on the MIT network," Indictment, ¶14(c), 20, was also not the making of a false statement. As the indictment acknowledges, the Mailinator email address was a real one through which Swartz could receive email from MIT if its personnel close to communicate with him. The use of those email addresses was not a fraudulent misrepresentation or omission of material fact.

The establishment of a new IP address, Indictment, ¶16(b), is not the making of a false statement. Indeed, it is not a statement at all. "An IP address is an identifier for a computer or device

[2] Swartz is charged with violations of these statutes in Counts 3-12.

on a TCP/IP network. Networks using the TCP/IP protocol route messages based on the IP address of the destination." http://www.webopedia.com/TERM/I/IP_address.html (last visited October 2, 2012). Thus, an IP address indicates nothing more than the address the computer is using for communications and is, in fact, always true. Swartz made no false statements or misrepresentations or omissions of material fact when he used different IP addresses to access JSTOR. For the same reasons, Swartz's use of two IP addresses which he allegedly assigned to himself after bypassing the guest registration process and connecting directly to the network, Indictment, ¶24, were not false statements or misrepresentations or omissions of material fact. By the same token, obtaining new IP addresses by "spoofing," *i.e.*, changing, the Acer's MAC address, Indictment, ¶¶19(a)-(c), 27(a)-(c), also cannot constitute false statements or misrepresentations or omissions of material fact, nor can Swartz's use of an automated collection device which made it appear that multiple people were requesting articles rather than a single person making multiple requests, Indictment, ¶34(c).

Swartz's use of MIT IP addresses did not make it appear that he was affiliated with MIT. Indictment, ¶34(a). Instead, MIT had a liberal guest user policy which permitted individuals with no affiliation with MIT whatsoever to access and use the MIT network, *see* Motion to Suppress All Fruits of Warrantless Searches Conducted from January 4, 2011, to January 6, 2011, and Incorporated Memorandum of Law at 9-10; the use of an MIT IP address did not represent to JSTOR that the person seeking access to its website was affiliated with MIT. This, too, did not constitute a material false statement or misrepresentation or omission of fact.

This leaves only Swartz's use of fictitious names when registering on MIT's network as a guest. That statement was made to MIT, not to JSTOR and only allowed Swartz to access the MIT network. It cannot support a charge of devising a scheme to defraud JSTOR of its property, specified

in the indictment as "journal articles digitized and distributed by JSTOR, and copies of them."

III. IF §1343 COULD BE APPLIED TO THE CONDUCT CHARGED HERE, IT IS VOID FOR VAGUENESS AS APPLIED TO THIS CASE.

To pass muster under the Due Process Clause, a statute must give fair warning, "in language that the common world will understand, of what the law intends to do if a certain line is crossed." *United States v. Hussein*, 351 F.3d 9, 13 (1st Cir. 2003). *See, e.g., United States v. Arcadipane*, 41 F.3d 1, 5 (1st Cir. 1994)("the Due Process Clause forbids the government from depriving an individual of his liberty unless he is given fair warning of the consequences of that conduct"). "The Due Process Clause demands that criminal statutes describe each particular offense with sufficient definiteness to 'give a person of ordinary intelligence fair notice that his contemplated conduct is forbidden.'" *Hussein*, 351 F.3d at 13, *quoting United States v. Harriss*, 347 U.S. 612, 617 (1954). *See, e.g., Kolender v. Lawson*, 461 U.S. 352, 357 (1983)("[A] penal statute [must] define the criminal offense with sufficient definiteness that ordinary people can understand what conduct is prohibited" (emphasis added)); *Connally v. General Const. Co.*, 269 U.S. 385, 391 (1926)("the terms of a penal statute creating a new offense must be sufficiently explicit to inform those who are subject to it what conduct on their part will render them liable to its penalties"(emphasis added)); *United States v. Bohai Trading Co., Inc.*, 45 F.3d 577, 581 (1st Cir. 1995)(issue is "whether the statute, as enacted by Congress, gave sufficient notice that the conduct charged was proscribed" (emphasis added)). In addition, to be valid under the Due Process Clause, penal statutes must be sufficiently specific to prevent arbitrary or discriminatory enforcement. To that end, they must provide comprehensible standards that limit prosecutorial and judicial discretion. *See, e.g., Kolender v. Lawson*, 461 U.S. 352, 357 (1983); *Grayned v. Rockford*, 408 U.S. 104, 108-09 (1972); *Smith v.*

Goguen, 415 U.S. 566, 572-73 (1974); *Papachristou v. City of Jacksonville*, 405 U.S. 156, 168 (1972).

As applied to the conduct alleged in this case to have violated §1343, the statute fails to give a person of ordinary intelligence fair notice that conduct such as that charged in this case is forbidden by the statute and could result in criminal prosecution and punishment. Neither the statute, nor any reported judicial decision, "has fairly disclosed" the conduct at issue to be "within [§1343's] scope." *Lanier*, 520 U.S. at 266.[3] It may be that the government is seeking to charge a scheme to defraud in

[3] This case is not comparable to cases which have applied the wire fraud statute to the distribution and use of devices that enabled users to obtain television or long-distance telephone or internet service without paying for it. *See, e.g.*, *Brandon v. United States,* 382 F.2d 607, 608, 610 (10th Cir.1967)(scheme to defraud telephone company of revenue for the use of long distance telephone service and facilities); *United States v. Manzer*, 69 F.3d 222, 225 (8th Cir.1995)(affirming convictions for wire fraud and mail fraud of a defendant who operated a business whose products enabled users to obtain premium television channels without paying for them); *United States v. Harriss*, 2012 WL 2402788 (D.Mass. June 26, 2012)(upholding against void for vagueness challenge conviction of defendants who sold cable modem hacking products which would permit users to obtain free or higher speed internet access without paying for it);*United States v. Norris,* 833 F.Supp. 1392, 1395-97 (N.D.Ind.1993), *aff'd*, 34 F.3d 530 (7th Cir.1994)(scheme to defraud cable television companies of revenue by selling equipment that allowed individuals to receive premium channels without paying required fee). These cases were held properly prosecuted under the wire fraud statute because the defendants' products directly enabled their users to defraud the provider of the revenue they would have obtained had the users properly contracted and paid for the services which were instead stolen. Here, in sharp contrast, nothing which Swartz did deprived either MIT or JSTOR of revenue. Guests were entitled to use the MIT network without paying a fee, and, in downloading JSTOR articles, Swartz was not depriving JSTOR of revenue. Moreover, the indictment charges that the property of which JSTOR was defrauded were articles, not revenue.

Nor is this case comparable to *United States v. Czubinski*, 106 F.3d 1069 (1st Cir. 1997), in which an IRS employee accessed and viewed confidential material which was the property of his employer. The Court held that the evidence did not suffice to support the defendant's conviction for wire fraud, but suggested in dictum that the defendant's conduct might have violated §1343 had he downloaded the confidential material. That dictum is not binding on this Court. *See, e.g.*, *Fletcher v. Haas*, 851 F.Supp.2d 287, 298 (D.Mass. 2012)(quoting Pierre N. Leval, *Judging Under the Constitution: Dicta About Dicta,* 81 N.Y.U. L.Rev. 1249, 1250 (2006)(noting that when judges accept dictum as if it were binding law, they "fail to discharge [their] responsibility to deliberate on and decide the question which needs to be decided")). Moreover, Swartz had no comparable fiduciary duty to JSTOR, the entity from which the articles were downloaded.

the complete absence of material misrepresentations and omissions. However, "the settled meaning of the term 'fraud' at common law required misrepresentation or concealment of a material fact." *United States v. Harriss*, 2012 WL 2402788 at *4 (D. Mass. June 26, 2012), *citing Neder*, 527 U.S. at 20-25. Nothing in the wire fraud statute or the cases construing it provides constitutionally adequate notice that manipulating IP addresses, spoofing MAC addresses, and gaining access to a free electronic communications network (MIT's) for the purpose of accessing another website to download journal articles which are free to those with access to the website, and for which access MIT had already paid, constitutes a federal wire fraud felony carrying a potential penalty of 30 years. Defendant's research has located no reported wire fraud case which is even remotely comparable to this one. Prosecution of Swartz under §1343 on the theory advanced by the government here would violate Swartz's rights to due process of law. The number of articles downloaded by Swartz may have exceeded JSTOR's terms of service, but the wire fraud statute does not exist to police violations of private contracts. Section 1343 is void for vagueness as applied to this case.

Respectfully submitted,
By his attorney,

/s/ Martin G. Weinberg
Martin G. Weinberg
20 Park Plaza, Suite 1000
Boston, MA 02116
(617) 227-3700 (tel.)
(617) 338-9538 (fax)
owlmgw@att.net

CERTIFICATE OF SERVICE

I, Martin G. Weinberg, hereby certify that on this 5th day of October, 2012, a copy of the foregoing document has been served via the Court's ECF system on all registered participants, including Stephen P. Heymann, AUSA.

/s/ Martin G. Weinberg

Martin G. Weinberg