UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

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

MOTION TO SUPPRESS ALL FRUITS OF INTERCEPTIONS AND DISCLOSURES OF ELECTRONIC COMMUNICATIONS AND OTHER INFORMATION BY MIT PERSONNEL IN VIOLATION OF THE FOURTH AMENDMENT AND THE STORED COMMUNICATIONS ACT AND INCORPORATED MEMORANDUM OF LAW (MOTION TO SUPPRESS NO. 1)

Now comes the defendant Aaron Swartz and respectfully moves that this Honorable Court suppress as evidence at the trial of this case (1) the network flow data and DHCP logs collected by MIT personnel and disclosed to the government without a warrant or court order or subpoena, as well as all evidence derived therefrom, and (2) all evidence from the packet capture instituted by MIT personnel on the morning of January 4, 2011, and continuing, at the request of the government that MIT personnel continue to intercept electronic communications, through January 6, 2011, and subsequently turned over to the Secret Service, as well as all evidence derived therefrom.[1]

As reason therefor, defendant states:

[1] In a separate motion to suppress, Swartz contends that after law enforcement agents arrived on the scene on January 4, 2011, and recommended that MIT personnel continue the packet capture they had begun earlier that morning and began to direct the investigation, MIT personnel were acting as government agents, and their actions were therefore subject to the requirements of the Fourth Amendment. *See* Motion to Suppress All Fruits of Warrantless Searches Conducted from January 4, 2011, to January 6, 2011, And Incorporated Memorandum of Law. This motion is directed in part at the interceptions conducted by MIT personnel before they began acting as government agents, as well as MIT's turning over to the government material in which Swartz had a reasonable expectation of privacy, in the complete absence of judicial process compelling MIT to produce such evidence to the government at a time when law enforcement agents were directing MIT employees regarding how to further their criminal investigation of the defendant.

1. He had a reasonable expectation of privacy in the electronic communications flowing to and from his ACER netbook.[2]

2. The interception of network flow data to the netbook and the packet capture constituted interceptions of electronic communications within the meaning of Title III.

3. The interceptions conducted by MIT and its disclosure of the information gathered to the Secret Service violated 18 U.S.C. §2511(1), as no exceptions to the requirements of Title III apply to MIT's conduct. The evidence, along with all derivative fruits thereof, must, therefore, be suppressed as violative of the Fourth Amendment.

4. The disclosure of DHCP logs by MIT personnel in the absence of a warrant issued upon a showing of probable cause or a court order pursuant to 18 U.S.C. §2703(d) violated the Fourth Amendment and/or the Stored Communications Act.

5. MIT's disclosure to the Secret Service of DHCP logs, network flow data, and packet capture information in the absence of a subpoena or search warrant violated 18 U.S.C. §§2702, 2703, as well as Swartz's rights under the Fourth Amendment such that suppression of the evidence, as well as all derivative fruits, in required.

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 suppression remedies sought and will respond to defendant's request for a hearing in its response to the motion.

---

[2] All averments herein regarding Swartz's ownership and possession of the ACER netbook and the attached hard drive, and the communications flowing to and from them, are made pursuant to the protections provided by *Simmons v. United States*, 390 U.S. 377, 392-94 (1968).

MEMORANDUM OF LAW

I. FACTUAL BACKGROUND.

On September 26, 2010, MIT received an email from Brian Larsen at JSTOR, an online archive of scholarly journal articles, informing it that there had been, that morning, an excessive downloading of journals. By the next day, the IP addresses from which the journals were being downloaded had been located (largely, if not exclusively, by JSTOR) and the user information for the guest registration of the computer being used had been identified; JSTOR then blocked access to these IP addresses. Timeline of events related to JSTOR downloading incident: 9/26/10 - 1/6/11, Exhibit 1 ("Timeline") at 1. On October 9, 2010, JSTOR again notified MIT that its access was being blocked because of excessive downloading. Timeline at 2. JSTOR quickly identified the IP address being used for the downloads, and MIT personnel thereafter discovered that access was being accomplished in Building 16 by a computer registered through its visitor guest registration process by the same guest whose computer was linked to the September incident.[3] Timeline at 2-3.

MIT and JSTOR conferred regarding methods to prevent excessive downloading. Timeline at 3-4. On December 26, 2010, there was another episode of excessive downloading, which MIT personnel did not learn of until on or about January 3, 2011. On the morning of January 4, 2011, at approximately 8:00 am, MIT personnel located the netbook being used for the downloads and decided to leave it in place and institute a packet capture of the network traffic to and from the netbook.[4] Timeline at 6. This was accomplished using the laptop of Dave Newman, MIT Senior

---

[3] MIT personnel first received notice of the October 9, 2010, incident when they returned following the Columbus Day holiday on October 12, 2010. Timeline at 2.

[4] A packet capture captures the entire communication, including subject matter and content, and to the extent it was diverting and copying communications in transit to and from the netbook, this constituted a classic interception of electronic communications in violation of *United States v. Councilman*, 418 F.3d 67 (1st Cir. 2005)(*en banc*). *See* page 9, *infra.*

Network Engineer, which was connected to the netbook and intercepted the communications coming to and from it. *Id.* Later that day, beginning at 11:00 am, the Secret Service assumed control of the investigation.[5] Later on January 4, 2011, Mike Halsall, MIT Senior Network & Information Security Analyst, turned over to Secret Service S/A Michael Pickett "historical network flow data concerning 18.55.6.240 & 7.240 [the IP addresses associated with the earlier JSTOR downloads][6] dating from 12/14 until present and relevant DHCP log information[7] from prior occurrences of ghost-macbook and ghost-laptop [the two guest registrations at issue] JSTOR downloading incidents (from Sept. and Oct.)." Timeline at 7. The disclosure took place only after the MIT General Counsel's Office approved the disclosure of the information to law enforcement authorities even in the absence of a warrant or court order or subpoena – and at a time when MIT personnel were acting as government agents – and in contravention of MIT policy that such information, which exceeded that found in bank records or telephone toll records, would be disclosed only upon the receipt of lawful court orders or subpoenas, *i.e.*, process complying with the Stored Communications Act, 18 U.S.C. §2701 *et seq. See* Section IV, *infra.* In a separate email from Halsall to S/A Picket on January 8, 2011, Halsall told Pickett that he "hop[ed] to have the pcap/flows/videos/logs all in by to me Monday,

---

[5] *See* Motion to Suppress All Fruits of Warrantless Searches Conducted from January 4, 2011, to January 6, 2011, And Incorporated Memorandum of Law.

[6] Network flow data shows connections made between computers and the amount of information transmitted. It shows the start and stop time of a connection, the source IP address, the IP address of the website contacted, source and destination port numbers, and the number of bytes of information transmitted.

[7] "DHCP" stands for Dynamic Host Configuration Protocol. DHCP assists with the assignment of IP addresses to computers on networks. When a computer joins a network, the computer issues a DHCP request on the network, which asks a DHCP server on the network to provide an IP address to the requesting computer. Part of the information contained in this request is the MAC (Media Access Control) address which is a unique identifier of the network card contained in the computer requesting an IP address. It also includes the commands made by the computer in question. *See* page 7, *infra.*

possibly sooner – if you don't already have a copy of the video or pcap [packet capture], I'll make sure you get one." Exhibit 2. No warrant or court order has been provided to counsel which would evidence the government's having, even post-interception, acquired the contents of the warrantless interceptions by seeking judicial authorization as required.

II. MIT'S ACTIONS VIOLATED TITLE III.

A. Swartz Had a Reasonable Expectation of Privacy in his Electronic Communications to and from his Netbook.[8]

Swartz had a subjective expectation of privacy in electronic communications to and from his netbook, and that expectation is one which society should recognize as objectively reasonable. The netbook was connected to the MIT network, but "the mere act of accessing a network does not in itself extinguish privacy expectations." *United States v. Heckenkamp*, 482 F.3d 1142, 1146 (9th Cir. 2007). MIT has a liberal guest access policy, which was described by Tim McGovern, MIT Manager of Network Security & Support Services, as follows:

> No authentication of visitors. Visitor network access is provided as an on-demand self-service process for anyone who walks onto campus, plugs in, or elects to use our wireless network, and declares themselves a visitor, and they get 14 days of network privileges.
>
> No identity verification. Visitors are asked to provide an email address. The email address is not used to verify that a bona fide identity exists . . . .
>
> No authentication of users accessing JSTOR.org. By agreement, JSTOR.org allows any computer with a net 18 IP address [an MIT IP address] to access their resources without further identification or authentication.

Exhibit 3. In fact, in internal emails, JSTOR described MIT as "unique" in having an open campus. Exhibit 4. Unlike other institutions which require passwords to access their servers and require additional layers of authentication to access digital libraries such as JSTOR, MIT required neither

[8] Swartz incorporates by reference the discussion in Section II of his Motion to Suppress All Fruits of Warrantless Searches Conducted from January 4, 2011, to January 6, 2011, And Incorporated Memorandum of Law.

a password, a formal affiliation with the school, or any form of identification for any visitor to become an authorized guest enjoying access to the MIT electronic communication service which was the equal of that afforded to MIT students and professors.

Swartz was validly signed on to the MIT network as a guest, as the MIT guest policy permitted him to be, as verified by an October 14, 2010, email from Ellen Duranceau, MIT Program Manager of Scholarly Publishing and Licensing, to Brian Larsen at JSTOR, informing him that "[o]ur investigations here point to the same *guest* that was involved in the 9/27 incident. We don't have enough information to follow the trail completely, but the signs suggest that the same *guest user* was responsible for this latest activity. . . . all of this excessive use was caused by a *guest visitor* at MIT," Exhibit 5 (emphasis added), and then by an October 18, 2010, email from Ms. Duranceau to Tim McGovern, MIT Manager of Network Security & Support Services:

> Tim and Mike:
> Would it be accurate for me to answer [JSTOR's] query this way:
>
> "*We offer guests access to the MIT network, and this practice will continue*. However, once we [in the future] institute our additional authorization layer for JSTOR, *this route will be closed to guests*. So we will have closed the pathway used."
> * * * *
> Mike, I will be asking JSTOR about your mod_rewrite idea once I check in with Rich Wenger in the Libraries and once JSTOR has shifted more clearly into implementing the new method rather than still working on resolving the excessive use issue.

Exhibit 6 (emphasis added). Thus, MIT had an open-access network that permitted anyone to access it by signing in as a visitor/guest, and anyone signed in to the MIT network was permitted to access JSTOR without further identification or authorization. The name and email address used to sign in as a visitor were fundamentally irrelevant to MIT, as it did not use it in any way to identify the visitor or even to ascertain whether it was a "bona fide identity," nor did guests to the MIT network receive notice that they were prohibited from using static IP addresses, changing IP addresses, or changing MAC addresses when accessing the MIT network on successive occasions. Neither MIT nor JSTOR

initiated the additional authorization protocol prior to the seizure of the netbook and Swartz's arrest on January 6, 2011.

That MIT regarded Swartz as a guest user is also confirmed by several other MIT communications during the fall of 2010. On September 29, 2010, Ellen Duranceau informed Brian Larsen at JSTOR that "the origin of the activity was *a guest visiting MIT*." Exhibit 7 (emphasis added). JSTOR is available to "[u]sers [who] come to MIT to establish a guest account on the network, and "do not have to have MIT affiliation to use the content." Summary of Key Points by Ellen Duranceau, Exhibit 8. *See* Email from Ellen Duranceau to Ann Wolpert, October 15, 2010, Exhibit 9 ("we cannot identify the *guest* involved in these incidents" (emphasis added)); Email from Ellen Duranceau to Brian Larsen, October 15, 2010, Exhibit 10 ("[o]ur records and logs . . . do not allow us to definitively identify the *guest*" (emphasis added); Email from Ellen Duranceau to Rich Wenger, October 18, 2010, Exhibit 11 ("it appears that the individual used MIT's wireless network guest account process").

In addition, MIT's written policy on DHCP logs created a reasonable expectation of privacy in *that* information, providing that they would be deleted after 30 days, IS&T Policies:DHCP Usage Logs Policy, available at http://ist.mit.edu/about/policies/dhcp-usage-logs (last visited September 24, 2012), and that they would be disclosed *only* in response to a court order or subpoena:

> When any network device, e.g., a computer, connects to MITnet and is assigned a dynamic IP address, MIT's DHCP server adds a record to its log containing the following information:
>
> - The date and time of the request
> - The MAC address of the requesting device or computer
> - The IP address provided
> - The specific DHCP command that was issued
> - Other technical information related to the request
>
> In the event of a request relating to a potential legal proceeding, IS&T staff may create a case in Request Tracker and store subsets of a log pertinent to the case at hand in the case record.

> The DHCP server is in a secure location and complies with secure data storage best practices. IS&T's Network Services Infrastructure team acts as the data custodian for DHCP logs, and ensures that the logs are stored securely and are deleted when they expire.
>
> * * * *
>
> *MIT is required to comply with a court order or valid subpoena that requests the disclosure of information contained in DHCP logs. Failure to comply could have serious consequences for the individuals, IS&T, and the Institute. MIT's Office of the General Counsel is qualified and authorized to confirm that a request for information contained in logs is legitimate and not an improper attempt to gain access to confidential information.*

Id. (emphasis added).

Moreover, on many occasions, the MIT RADIUS log server provided further evidence documenting MIT's authorization of Swartz's access to the MIT network:

> **Remote Authentication Dial In User Service** (**RADIUS**) is a networking protocol that provides centralized Authentication, *Authorization*, and Accounting (AAA) management for computers to connect and use a network service. . . . Because of the broad support and the ubiquitous nature of the RADIUS protocol, it is often used by ISPs and enterprises to manage access to the Internet or internal networks, wireless networks, and integrated e-mail services. . . . The RADIUS server is usually a background process running on a UNIX or Microsoft Windows server. RADIUS serves three functions:
>
> - to authenticate users or devices before granting them access to a network,
> - *to authorize those users or devices for certain network services* and
> - to account for usage of those services.

http://en.wikipedia.org/wiki/RADIUS (last visited September 23, 2012)(emphasis added). Swartz, accordingly, maintained a reasonable expectation of privacy in the communications to and from his netbook and that expectation was objectively reasonable.

B. MIT's Actions in Intercepting Communications to and from Swartz's Netbook and Disclosure of the Intercepted Communications Violated Title III.

18 U.S.C. §2511(1) prohibits:

> **(a)** intentionally intercept[ing], endeavor[ing] to intercept, or procur[ing] any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;
>
> * * * *
>
> **(c)** intentionally disclos[ing], or endeavor[ing] to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the

> information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;
>
> **(d)** intentionally us[ing], or endeavor[ing] to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection . . . .

18 U.S.C. §2510(12) defines "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate or foreign commerce . . . ." Section 2510(4) defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." "Contents" is in turn defined as "*any* information concerning the substance, purport or meaning" of the communication. §2510(8)(emphasis added).

The packet capture, which targeted the content of data being sent to or from the netbook that was discovered in Building 16's data room, revealed the contents of electronic communications of all electronic communications intercepted. *See* Email from Dave Newman, MIT Senior Network Engineer, to S/A Pickett, January 5, 2011, Exhibit 12 ("I have collected about 70G of network traffic so far with about 98% of which is the JSTOR journal downloads"). Use of the packet capture constituted the interception of electronic communications of the defendant and others, including, but not limited to, those with whom he was communicating within the meaning of Title III, *see, e.g., United States v. Councilman*, 418 F.3d 67 (1st Cir. 2005)(*en banc*)(diverting incoming communications constitutes interception within the meaning of Title III), which was unlawful in the absence of a valid Title III order authorizing the interceptions of the electronic communications, of which none were sought or issued here.

The DHCP logs also captured content as they captured the message sent from the sending computer requesting an IP address, which is the "substance, purport, or meaning" of the communication.[9] The network flow data showed that a communication took place between one computer and another and the amount of information transmitted. These, too, constitute "contents."[10] In *In re Application of United States*, 396 F.Supp.2d 45, 48-49 (D.Mass. 2005), the Court recognized that "dialing, routing, addressing and signaling information" may disclose "content" and mandated that the order include instructions to the provider that "[t]he disclosure of the 'contents' of communications is prohibited pursuant to this Order even if what is disclosed is also dialing, routing, addressing and signaling information'" and that "the term 'contents' of communications includes subject lines, application commands, search queries, requested file names, and file paths." *See, e.g., United States v. Forrester*, 512 F.3d 500, 510 n.6 (9th Cir. 2008)(suggesting that a technique which reveals the URL visited would be "constitutionally problematic").

Therefore, the interceptions were unlawful unless they fell within an exception to the prohibitions of §2511. The "provider exception" to Title III, §2511(2)(a)(i) provides:

> It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose or use that communication in the normal course of his employment while engaged in any activity which is a *necessary incident to the rendition of his service or to the protection of the rights and property of the provider of that service* . . . .

---

[9] Another issue specific to the DHCP logs is addressed in Section III, *infra.*

[10] Such information is not analogous to a pen register, which has been held not to reveal content, because a pen register does not even show whether a communication even took place, *see United States v. New York Tel. Co.*, 434 U.S. 159, 167 (1977). Even a pen register requires a court order based upon a "certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency." 18 U.S.C. §3122(b)(2).

(emphasis added).[11] "The statute's use of the word necessary, its proviso restricting random monitoring and Congress' intent to maximize the protection of privacy . . . suggests that this authorization should be limited in scope." *United States v. Freeman*, 524 F.2d 337, 341 (7th Cir. 1975). *See, e.g., United States v. Cornfeld*, 563 F.2d 967, 970 (9th Cir. 1977)("the authority to intercept and disclose . . . communications is not unlimited"); *United States v. Harvey*, 540 F.2d 1345, 1350 (8th Cir. 1976)(authority granted by §2511(2)(a)(i) "may be exercised only to the extent necessary for 'the protection of the rights and property of the carrier'"); *United States v. McLaren*, 957 F.Supp. 215, 218 (M.D.Fla. 1997)("the court must consider whether the provider of electronic communication service had reasonable cause to suspect that *its* property rights were being abused by a particular subscriber"(emphasis added)).

Here, the circumstances demonstrate that MIT personnel did not intercept the communications at issue to protect *MIT*'s rights or property *as a provider of electronic communication service.* Instead, its concern was initially with the protection of the rights and property of JSTOR and thereafter with assisting law enforcement with discovering the motive and intent of the owner of the netbook and in acquiring evidence that would further the criminal investigation of the individual responsible for the JSTOR downloading. Once the netbook was physically discovered, MIT personnel, aware that its owner would return to retrieve the external hard drive that was attached to the netbook and receiving the downloaded data, installed video surveillance to identify the owner and help in his apprehension. The investigation commenced with a notification from JSTOR regarding excessive downloads of journal articles, and thereafter MIT

[11] 18 U.S.C. §2510(15) defines "electronic communication service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications."

personnel worked with JSTOR to develop and institute a plan which would prevent MIT guest users from accessing JSTOR without an additional level of authorization and permission. There was no need for further investigation on MIT's part, as its electronic communication system was never in the slightest danger of injury or other detrimental impact. Once the netbook was located, MIT advised JSTOR of the discovery and asked it to block the particular IP address it was using. *See* Exhibit 13. MIT also had the option, which it did not choose to exercise, to simply take the netbook offline. Instead, it kept the connection alive only to assist law enforcement and to further a criminal investigation, objectives well outside the narrow parameters of the provider exception to the general prohibition of warrantless interceptions of wireless communications in transit..

Even at the outset of the investigation which began again on January 3, 2011, the objective was to placate JSTOR, which had deemed MIT's prior efforts to identify the person responsible for the downloads "tepid," Exhibit 14, and ensure continued MIT access to JSTOR, as witness the central role played in the investigation by Ellen Duranceau, MIT Program Manager of Scholarly Publishing and Licensing, and not a "necessary incident" to the "protection of the rights and property" of MIT as electronic communications service provider. As of the next morning, January 4, 2011, MIT personnel were acting as agents of law enforcement, and their purpose was not to protect MIT's electronic communications system but instead to further the criminal investigation.[12] Section 2511(2)(a)(i) does not extend to the protection of institutional interests in general but instead only to the protection of the electronic communication system itself.[13] Once the ACER was located

---

[12] *See* Motion to Suppress All Fruits of Warrantless Searches Conducted from January 4, 2011, to January 6, 2011, And Incorporated Memorandum of Law.

[13] The interceptions also did not fall within the "trespasser exception," §2511(2)(i), because Swartz was not a trespasser, *see* Motion to Suppress All Fruits of Warrantless Searches Conducted from January 4, 2011, to January 6, 2011, And Incorporated Memorandum of Law at 16-19, and, most importantly for present purposes, MIT personnel were not, until law enforcement agents

on the morning of January 4, 2011, MIT's problem with JSTOR could have been ended by disconnecting that computer from the MIT network. Instead, it elected to intercept communications, not to protect the MIT system, but to gather information for law enforcement purposes, such as the motive and intent of the person responsible for the downloads, and to determine whether any of the downloaded information had been transmitted to others by the netbook, a purpose which was protective of JSTOR and in furtherance of law enforcement's acquisition of proof of the possible commission of various federal offenses, but not protective of MIT's electronic communication services, as required by the statutory exception.

Moreover, even if the Court were to conclude that MIT, as electronic communications service provider, was acting to protect its own interest *qua* service provider as it searched for the "offending" computer, "the federal courts . . . have construed [§2511(2)(a)(i)] to impose a standard of reasonableness upon the investigating communication carrier." *United States v. Harvey*, 540 F.2d 1345, 1351 (8th Cir. 1976). *See, e.g., United States v. Hudson*, 2011 WL 4727811 at *7 -*8 (E.D.La. Oct. 5, 2011)("The Fifth Circuit has held that this provision imposes a reasonableness requirement on carriers," *citing United States v. Clegg*, 509 F.2d 605, 613-14 (5th Cir. 1975)); *United States v. McLaren*, 957 F.Supp. 215, 218 (M.D.Fla. 1997)(court "must consider whether the interception activities were reasonable"). The interceptions at issue here went far beyond anything that was necessary to the protection of MIT's rights and property; prior to the January 4, 2011, interceptions and the warrantless disclosures of protected information, the ACER laptop had been discovered, its connection to the MIT network had been identified, video surveillance had been instituted to identify the owner, and a narrow shutdown of service to that computer would have accomplished any legitimate goal of protecting MIT's electronic communication service.

---

encouraged and adopted the ongoing packet capture, acting "under color of law."

Similarly, an electronic communications system provider may disclose to law enforcement *only* those intercepted communications which are a "necessary incident" to the protection of the provider's property rights. *See, e.g., Clegg*, 509 F.2d at 612-13. *See, e.g., United States v. Auler*, 539 F.2d 642, 646 n.10 (7th Cir. 1976)("Evidence which is obtained through an unreasonably broad surveillance cannot be legally disclosed to the government, regardless of whether it is offered at trial"). Only those communications of which §2511(2)(a)(i) reasonably permits the interception may be disclosed and admitted as evidence at the trial of a criminal case; "evidence obtained through surveillance beyond the authorization of §2511(2)(a)(i) . . . must be suppressed." *Id.* at 646. None of the disclosures on January 4, 2011, was justified by this narrow exception to an MIT guest's entitlement to the protections of the Fourth Amendment and Title III. As such, consistent with *Councilman*, the network data capture constituted unlawful interceptions of electronic communications in violation of the Fourth Amendment, requiring suppression of the captured information and all evidence derived therefrom.

III. THE GOVERNMENT COULD NOT OBTAIN DCHP LOG INFORMATION IN THE ABSENCE OF A WARRANT OR, AT MINIMUM, A §2703(D) ORDER.

The DHCP log records and stores a variety of data. *See* page 7, *supra.* For present purposes, the critical fact about DCHP addressees is that their recording and storage allows the tracking of an individual through the location of his computer. Where laptops and other portable devices are concerned, that data is comparable to cell site data in that it permits the government to determine an individual's location and to track his movements as he moves his laptop from place to place. Two types of DHCP data are at issue here: the historical data which the government sought from MIT, and with which MIT provided the government, and the ongoing real-time DHCP data which law enforcement obtained on an ongoing basis after they assumed control of the investigation on January

4, 2011, all of which was sought, and obtained, by the government without a warrant or a court order issued pursuant to §2703(d).

Individuals have a reasonable expectation of privacy in their movements. *See, e.g., In re Application of United States*, 849 F.Supp.2d 526, 538-43 (D.Md. 2011). Moreover, an individual retains a reasonable expectation of privacy in DHCP log information because, as the Third Circuit held in the cell site location context, "a . . . customer has not 'voluntarily' shared his information with [a third party] in any meaningful way." *In re Application of United States*, 620 F.3d 304, 317 (3d Cir. 2010). As Justice Sotomayor explained in her concurring opinion in *United States v. Jones*, 132 S.Ct. 945 (2012):

> More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. *E.g., Smith* [*v. Maryland*], 442 U.S. [735,] 742 [(1979)] . . .; *United States v. Miller,* 425 U.S. 435, 443 . . . (1976). This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers. Perhaps, as Justice ALITO notes, some people may find the "tradeoff" of privacy for convenience "worthwhile," or come to accept this "diminution of privacy" as "inevitable," . . . and perhaps not. I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year. But whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy. I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection. See *Smith,* 442 U.S., at 749 (Marshall, J., dissenting) ("Privacy is not a discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes"); see also *Katz* [*v. United States*], 389 U.S. [347,] 351-352 [(1967)]("[W]hat [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected").

Id. at 957.

As to both historical and "real time" cell site data, courts have been divided regarding whether the government must demonstrate probable cause as required by the Fourth Amendment or whether the lesser showing required under §2703(d) will suffice. *Compare In re Application of the United States*, 2012 WL 3260215 at *1-*2 (S.D.Tex. July 30, 2012); *In re Application of the United States*, 809 F.Supp.2d 113, 118-20 (E.D.N.Y.2011); *In re United States*, 747 F.Supp.2d. 827, 837-40 (S.D.Tex.2010); *In re Application of United States*, 736 F.Supp.2d 578, 579 (E.D.N.Y.2010)(requiring showing of probable cause), *with In re Application of United States*, 620 F.3d at 313; *In re Application of United States*, 849 F.Supp.2d 177, 179 (D.Mass. 2012); *United States v. Graham,* 846 F.Supp.2d 384, 396 (D.Md. 2012); *United States v. Benford*, 2010 WL 1266507, at *2-*3 (N.D.Ind. March 26, 2010); *In re Applications of United States*, 509 F.Supp.2d 76, 80-81 (D.Mass. 2007); *In re Application of United States*, 396 F.Supp.2d 294, 327 (E.D.N.Y. 2005)(§2703(d) order suffices).

Courts are likewise split with respect to the government's burden to obtain real time cell site data. *Compare In re Application of the United States*, 849 F.Supp.2d 526 (D.Md. 2011); *In re Application of the United States*, 2009 WL 159187 (S.D.N.Y. Jan.13, 2009); *In re Application of the United States*, 497 F.Supp.2d 301 (D.P.R.2007); *In re Application of the United States*, 2006 WL 2871743 (E.D.Wis. Oct. 6, 2006); *In re Application*, 439 F.Supp.2d 456 (D.Md.2006); *In re United States*, 441 F.Supp.2d 816 (S.D.Tex.2006); *In re United States*, 2006 WL 1876847 (N.D.Ind. July 5, 2006); *In re Application of the United States*, 2006 WL 468300 (S.D.N.Y. Feb. 28, 2006); *In re United States*, 416 F.Supp.2d 390 (D.Md.2006); *In re United States*, 415 F.Supp.2d 211 (W.D.N.Y.2006); *In re United States*, 412 F.Supp.2d 947 (E.D.Wis.2006), *aff'd* 2006 WL 2871743 (E.D.Wis. Oct. 6, 2006); *In re United States*, 407 F.Supp.2d 134 (D.D.C.2006)(requiring a showing of probable cause), *with In re Application of the United States*, 2008 WL 5255815 (E.D.N.Y.

Dec.16, 2008); *In re United States*, 2008 WL 5082506 (E.D.N.Y. Nov. 26, 2008); *In re Application of the United States*, 460 F.Supp.2d 448 (S.D.N.Y.2006); *In re United States*, 433 F.Supp.2d 804 (S.D.Tex.2006); *In re Application of the United States*, 415 F.Supp.2d 663 (S.D.W.Va.2006); *In re Application of the United States*, 411 F.Supp.2d 678 (W.D.La.2006)(probable cause not required).

The cases requiring a showing of probable cause for both historical cell site data and real time cell site data are the better reasoned and more consonant with the requirements of the Fourth Amendment and its historical role in protecting citizens from serious invasions of personal privacy. The same analysis is applicable to both historical DHCP data and real time DHCP data, and the government's acquisition of this information in the absence of a warrant based on probable cause violated the Fourth Amendment. The invasion of this information also has serious First Amendment implications in that it traces an individual's communicational associations. *See In re Application of United States*, 849 F.Supp.2d at 538 n.5. At a minimum, a §2703(d) order was required. Accordingly, the DHCP log information, and all information derived therefrom, including the laptop and hard drive seized from the MIT Student Center which were discovered as an unattenuated result of the "real time" inspection of DHCP logs on January 6, 2011, must be suppressed.

IV. MIT'S ACTIONS VIOLATED THE STORED COMMUNICATIONS ACT ("SCA").

18 U.S.C. §2702(a)(1) prohibits any person or entity "providing an electronic communication service to the public" from "knowingly divul[ging] to any person or entity the contents of a communication while in electronic storage by that service."[14] Section 2702(a)(3) prohibits "a provider of . . . electronic communication service to the public" from "divulg[ing] a record or other

[14] "Electronic storage" includes "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof" and "any storage of such communication by an electronic service communication provider for purposes of backup protection of such communication." 18 U.S.C. §2510(17).

information pertaining to a subscriber or a customer of such service . . . ." MIT was a provider of electronic communication service to the public because it freely allowed guests with no affiliation to MIT to access the MIT network and because it provided wireless service which was readily accessible to anyone within reach of its signal, which extended to areas outside the bounds of the MIT campus.[15] As a guest, Swartz was a customer or subscriber of MIT's electronic communication service. The SCA contains a provider exception similar to that of Title III: the provider of electronic communication service may disclose the content of communications or information pertaining to a subscriber or customer "as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service." §§2702(b)(5), (c)(3). This exception does not apply for the same reasons previously addressed in conjunction with the provider exception of Title III.

Moreover, here, MIT did not voluntarily disclose the information on its own initiative. Indeed, disclosure of the information was contrary to MIT policy, which provided its users, including guests, with a reasonable expectation of privacy in the DHCP logs and other information collected by MIT. *See* pages 7-8, *supra.* MIT disclosed the information only after its General Counsel's office authorized the disclosure, *which had been requested by the government after it had assumed control of the investigation and after MIT had deferred to the government's control over the investigation*. Thus, at the time of the disclosures, MIT personnel were acting as government agents. In short, MIT personnel, by the late morning of January 4, 2011, were acting as agents of federal and state law enforcement.

> Congress passed the Stored Communications Act in 1986 as part of the Electronic Communications Privacy Act. "The SCA was enacted because the advent of the Internet

[15] MIT's wireless network signal is available outside of the campus, for example, at the Kendall Hotel and on the streets and sidewalks that border the campus.

> presented a host of potential privacy breaches that the Fourth Amendment does not address." *Quon v. Arch Wireless Operating Co., Inc.,* 529 F.3d 892, 900 (9th Cir.2008)[, *rev'd on other grounds sub nom. City of Ontario v. Quon*, 130 S.Ct 1531 (2010)] (citing Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It,* 72 Geo. Wash. L. Rev. 1208, 1209–13 (2004)). The SCA prevents "providers" of communication services from divulging private communications to certain entities and individuals. Kerr, *supra,* at 1213. It "creates a set of Fourth Amendment-like privacy protections by statute, regulating the relationship between government investigators and service providers in possession of users' private information." *Id.* at 1212. First, the statute limits the government's right to compel providers to disclose information in their possession about their customers and subscribers. 18 U.S.C. § 2703. . . . Second, the statute limits the right of an Internet Service Provider ("ISP") to disclose information about customers and subscribers to the government voluntarily. 18 U.S.C. § 2702.

Crispin v. Christian Audigier, Inc., 717 F.Supp.2d 965, 971-72 (C.D. Cal. 2010).

As addressed in the previous section, MIT could not voluntarily disclose the information without violating the SCA. Under §2703, the government could not lawfully request or obtain access to the content of electronic communications in the absence of a warrant issued in accordance with the Rules of Criminal Procedure. 18 U.S.C. §2703(a).

> In passing the Electronic Communications Privacy Act in 1986, Congress expressed the need to expand the protections of the Fourth Amendment to new forms of communication and data storage. 132 Cong. Rec. H4039-01 (1986); S.Rep. No. 99-541, at 1-2 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3555-56. The legislative history indicates that Congress wished to encourage the development and use of these new methods of communication by ensuring that they were protected and private. S.Rep. No. 99-541, at 5. Congress recognized that courts had struggled with the application of the Fourth Amendment to the seizure of intangibles, like telephone conversations. *Id.* at 2. They therefore sought to strike a balance between the competing interests addressed by the Fourth Amendment in the world of electronic communications by "protect[ing] privacy interests in personal and proprietary information, while protecting the Government's legitimate law enforcement needs." *Id.* at 3.
>
> It is clear that Congress wished to apply the protections associated with search warrants to searches authorized under § 2703(a).

In re United States, 665 F.Supp.2d 1210, 1220 (D.Or. 2009). The government could not lawfully obtain "record[s] or other information pertaining to a subscriber or customer" of MIT's electronic communications system in the absence of a warrant or a court order issued pursuant to §2703(d). 18 U.S.C. §2703(c)(1). Under §2703(c)(2), the government may obtain the name and address of a

customer or subscriber, records of session times and duration, length of services and types of service used, and "other subscriber number or identity, including any temporarily assigned network address" only through an administrative, grand jury, or trial subpoena. The information at issue here went beyond this narrow description, but, in any event, the government did not seek the information pursuant to subpoena. The DHCP logs, the network flow data, and the packet capture all either contained "content" of the electronic communications to and from the netbook, in which Swartz had a reasonable expectation of privacy or "record[s] or other information" pertaining to Swartz's use of MIT's electronic communications system, in which he also had a reasonable expectation of privacy. Indeed, MIT's DHCP log policy created an objectively reasonable expectation that those logs would remain confidential unless they were required to be disclosed pursuant to a lawful order or subpoena, of which there was none here. The government's conduct, in seeking the production of this material without a warrant and without a §2703(d) order violated the Fourth Amendment. *See, e.g., United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010). The material at issue must, accordingly, be suppressed, along with all derivative fruits thereof.

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. One copy of the exhibits to the motion was served on the government by hand this same date.

/s/ Martin G. Weinberg

Martin G. Weinberg