UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

UNITED STATES OF AMERICA,

Plaintiff, CRIMINAL NO. 08-20314

v. HON. NANCY G. EDMUNDS

ISSAM HAMAMA,

Defendant.
_____/

DEFENDANT'S BRIEF IN SUPPORT OF MOTION QUASH A GOVERNMENT SUBPOENA SEEKING THE CONTENTS OF THE DEFENDANT'S EMAILS

I. Introduction: The Government has issued a subpoena to Internet Service Provider Yahoo! and to Internet Service Provider MSN to compel them to produce emails maintained by the ISPs for email account addresses hamama_sam@yahoo.com and ih749@hotmail.com. The subpoenas issued pursuant to the Stored Communications Act, Title 18 U.S.C. § 2703(b)(B). 18 U.S.C. §2703 provides procedures through which a governmental entity can access both user records other subscriber information, and the content of electronic messages. Subsection (b) provides that to obtain messages that have been stored for over 180 days, the government generally must either (1) obtain a search warrant, (2) use an administrative subpoena, or (3) obtain a court order. The latter two require prior notice to the subscriber, allowing the subscriber an opportunity for judicial review before the disclosure:

> (b) Contents of wire or electronic communications in a remote computing service.
>
> (1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection--
> (A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal

> Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant; or
> (B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity--
> (i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or
> (ii) obtains a court order for such disclosure under subsection (d) of this section; except that delayed notice may be given pursuant to section 2705 of this title.

II. Argument :

Title 18 U.S.C. § 2703(a) and (b)(1)(B)(I) purport to authorize "the disclosure by a provider of electronic communications service of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days . . . with prior notice . . . if the government entity uses . . . a trial subpoena)." But it is the Court, and not Congress, that must determine the threshold Issue. *See Marbury v. Madison*, 5 U.S. 137 (1803). Because government agents intrude upon a user's privacy when they acquire private e-mails, they conduct a search under the Fourth Amendment.[1] That expectation of privacy obtains whether the e-mails acquired are stored or in transit, and whether or not their recipients have accessed them. Nothing in the private contracts between users and their web based e-mail service providers affects application of those constitutional protections. For these reasons, and for the reasons articulated below, Mr. Hamama respectfully submits that the subpoena should be quashed because the search and seizure of the contents of electronic mail during an open ended and unspecified period with a trial subpoena, violates the Fourth Amendment.

III. Issues:

[1] Such a search has First Amendment implications. *See Stanley v. Georgia*, 394 U.S. 557, 564 (1969) ("It is now well established that the Constitution protects the right to receive information and ideas.").

a. Whether a subpoena by the Government to a private Internet Service Provider seeking to obtain a defendant's email communications for an open and unspecified period violates the Fourth Amendment's prohibition against unreasonable search and seizure when the Government possesses no particular evidence or information that the sought after electronic communication contains any evidence of wrong doing and when the Government has not obtained a court order?

Yes. A subpoena of a private email account is a search within the meaning of the Fourth Amendment to the United States Constitution. On or about November 19, 2010 the Government provided notice that it intended to subpoena the email account of Mr. Hamama that is maintained by Yahoo! under the account hamama_sam@yahoo.com. On November 30, 2010, the defense was again notified of the Government's intent to subpoena the contents of email account ih749@hotmail.com. Both notices stated that the subpoenas will seek the contents of the emails pursuant to 18 U.S.C. §2703(b)(B). *Exhibits A and B.*

Warrantless searches and seizures are presumptively unreasonable under the Fourth Amendment, *Horton v. California*, 496 U.S. 128, 110 S. Ct. 2301, 2306 & n. 4, 110 L.Ed.2d 112 (1990); *Katz v. United States*, 389 U.S. 347, 357, 88 S.Ct. 507, 514, 19 L.Ed.2d 576 (1967), as are any searches and seizures of closed containers based on less than probable cause, *United States v. Ross*, 456 U.S. 798, 809-812, 102 S.Ct. 2157, 2164-2166, 72 L.Ed.2d 572 (1982). As early as 1878, the Supreme Court has acknowledged that the contents of "[l]etters and sealed packages … in the mail are as fully guarded from examination and inspection … as if they were retained by the parties forwarding them in their own domiciles." *Ex Parte Jackson*, 96 U.S. 727, 733, 24 L.Ed. 877 (1878). So long as a package is "closed against inspection," the Fourth Amendment protects its contents, "wherever they may be," and the police must obtain a warrant to search it just "as is required when papers are subjected to search in one's own household." *Id. Accord, United States v. Van Leeuwen*, 397 U.S. 249, 90 S.Ct. 1029, 25 L.Ed.2d 282 (1970). Indeed, the Supreme Court has long recognized that individuals do not surrender their

expectations of privacy in closed containers when they send them by mail or common carrier, and that "[l]etters and other sealed packages are in the general class of effects in which the public at large has a legitimate expectation of privacy; warrantless searches of such effects are presumptively unreasonable." *United States v. Jacobsen*, 466 U.S. 109, 114, 104 S.Ct. 1652, 1656-57, 80 L.Ed.2d 85 (1984), *citing United States v. Chadwich*, 433 U.S. 1, 10, 97 S.Ct. 2476, 2482, 53 L.Ed.2d 538 (1977); *United States v. Van Leeuwen*, 397 U.S. 249, 251, 90 S.Ct. 1029, 1031, 25 L.Ed.2d 282 (1970); *Ex parte Jackson*, 96 U.S. 727, 733, 24 L.Ed. 877 (1878); *United States v. Ross*, 456 U.S. 798, 809-812, 102 S.Ct. 2157, 2164-2166, 72 L.Ed.2d 572 (1982); *Robbins v. California*, 453 U.S. 420, 426, 101 S.Ct. 2841, 2845, 69 L.Ed.2d 744 (1981) (plurality opinion); *Arkansas v. Sander*, 442 U.S. 753, 762, 99 S.Ct. 2586, 2592, 61 L.Ed. 2d 235 (1979), and other cases.

"As long as a package is 'closed against inspection,' the Fourth Amendment protects its contents 'wherever they may be' and the police must obtain a search warrant." United States v. Dowler, 940 F.2d 1539, 1991 WL 155987, at *3 (10th Cir.1991) (unpublished opinion), *citing Ex parte Jackson*, 96 U.S. at 733. The bottom line is that "unless the container is such that its contents may be said to be in plain view, those contents are fully protected by the Fourth Amendment." *Robbins*, 453 U.S. at 427.

Emails stored on an ISP's server are simply another form of a closed container. The contents of an email are not visible to the naked eye; rather, there are several intrusive searches that axiomatically precede one's ability to view the contents of an email stored on an ISP's server. First, an individual seeking to view the contents of an email stored on an ISP's server must gain access to that portion of the ISP's server that houses the subscriber's email; this is a search in and of itself. Even after one gains access to a subscriber's virtual mailbox, the contents

of those emails remain shielded from public view, much like the contents of a first-class letter remain shielded from public view when you peer into a mailbox at the top of one's driveway. To view the contents of the email, an individual must take another intrusive physical act, he or she must unseal the email. To do so, one double-clicks on the email through the use of a computer mouse or perhaps uses the "open" function of the computer. Either way, the closed nature of the email conceals its contents from plain view until somebody opens or unseals the email. This is no different from the physical act of unsealing a closed first-class envelope, unsealing a closed package, unlocking a closed footlocker, opening a closed filing cabinet, or opening a closed storage facility. From a doctrinal perspective, this incontrovertible fact compels a finding that an email is a closed package and, as such, there is no constitutional difference between unsealing a first-class letter and double-clicking an email. Both closed containers are entitled to the same constitutional protection.

In creating a relationship with an ISP, the subscriber does not relinquish a reasonable expectation of privacy in any unopened or opened-and-then-closed-again email communications stored on the ISP's server. Keeping a closed email on the server of an ISP does not relinquish one's interest in the email, or his reasonable expectation of privacy therein. Indeed, in the case of email, the subscriber perhaps maintains more control over the email letter than in any other traditional third party carrier context. In the latter scenarios, the sender or receiver of a closed letter or package actually relinquishes control of the container and cannot immediately repossess the letter or package—it is in the physical possession of the postal carrier and/or common carrier outside the dominion and control of the sender or recipient. In the email context, the owner of the email can repossess a read-and-then-closed email at any moment, without any notice or permission from the ISP, can retake the email, delete the email from his mailbox, or do whatever

he or she wants to do with the email. It is, for all purposes, in that person's possession, dominion and control, at all times. The privacy interests may arguably be greater in the context of email than in the traditional carrier paradigm.

Additionally, the subscriber's relationship to the ISP adds to the reasonable expectation of privacy in the contents of closed emails contained on the ISP's server. Like an individual who rents a storage space at a local storage facility, an ISP subscriber typically secures a section of the ISP's storage facility, i.e., its server. See http://overview.mail.yahoo.com/enhancements/shareeasily, (advising subscribers have unlimited storage space on their servers).

A subscriber's "storage space" within the ISP server is locked and inaccessible to the public at large, like the individual who places a lock on his storage space. While a physical storage space or a physical filing cabinet is protected by combination or key locks the rented portion of the ISP's server is protected by a screen name and a password, precluding access to its contents by any member of the public. Additionally, like the owner of a physical storage facility, or a bailee who takes possession of another person's private documents, the ISP is not permitted to access the private mail contained on the server except for very limited circumstances—they are not permitted or expected to simply open and review private email at their whim and discretion.

It is well established that an individual manifests a subjective expectation of privacy that society views as objectively reasonable when he or she places contents into a closed container, even when he or she places that closed container in the possession of a private third party, such as within a friend's apartment, a leased house, a rented storage facility, or a third party common carrier. *See, e.g., United States v. James*, 353 F.3d 606, 614 (8th Cir.2003) (in deciding an issue

of consent, court notes that Eighth Circuit law and law of other circuits indicates that one does not cede dominion over an item to another just by putting him in possession; for example a lessee does not have authority to consent to a search of the lessor's financial records stored at the leased house merely on account of the lessor-lessee relationship); *United States v. Dowler*, 940 F.2d 1539 (10th Cir.1991) (unpublished decision) (before leaving state, appellant placed documents in boxes, file cabinet and briefcases, which were then stored by apartment manager at request of appellant's agent; held that appellant manifested an expectation that the documents would remain private and free from inspection, the apartment manager was obligated to care for her property in the regular storage area and a new relationship was created, and that appellant's expectation of privacy and protection from a wrongful search and seizure continued into the creation of the bailment by the apartment manager and her agent); *United States v. Fultz*, 146 F.3d 1102 (9th Cir. 1998) (defendant who lived "on and off" with his friend and stored many of his belongings in closed boxes in friend's garage had a reasonable expectation of privacy in his belongings, even though those belongings were kept in a place that was not exclusively controlled by him).

Finally, for all of these reasons, email communications retained on an ISP server are not analogous to the line of cases wherein individuals knowingly expose communications to a third party, which are then conveyed to law enforcement authorities pursuant to subpoenas. In *United States v. Miller*, 425 U.S. 435, 443, 96 S.Ct. 1619, 48 L.Ed.2d 71 (1976), the Court held that a customer of a bank cannot challenge on Fourth Amendment grounds the admission into evidence in a criminal prosecution of financial records obtained by the government from his bank pursuant to allegedly defective subpoena, despite the fact that he was given no notice of the subpoenas. *Miller*, 425 U.S. at 441-443. *See also Donaldson v. United States*, 400 U.S. 517, 522, 91 S.Ct.

534, 538, 27 L.Ed.2d 580 (1971) (Internal Revenue summons directed to third party does not trench upon any interests protected by the Fourth Amendment). In *Miller*, the Court ruled that no Fourth Amendment interests of the depositor were implicated because the depositor knowingly exposed those documents to the bank's employees in the ordinary course of business, and that "checks are not confidential communications but negotiable instruments to be used in commercial transactions." *Miller*, 425 U.S. at 442. As such, the Court ruled that the case was governed by the general rule that the issuance of a subpoena to a third party to obtain the records of that party does not violate the rights of a defendant. *Miller*, 425 U.S. at 443.

In the context of emails stored on an ISP server—whether they have been previously opened by the addressee are not—the emails remain closed to the public and to the ISP (except, perhaps, for limited, defined circumstances that are either inapplicable to the facts of this matter and/or that do not diminish the customer's reasonable expectation of privacy regarding the content of their email communications). Most importantly, they have not been provided to the ISP for their exposure, review or consumption. Unlike the checks at issue in *Miller*, which the Supreme Court noted are conveyed to bank and exposed to their employees in the ordinary course of business, email communications are closed containers and, even if an ISP contract provides limited circumstances in which they may be viewed by the ISP (and even if the subscriber ever reads that contract), subscribers have an objectively reasonable expectation that those emails will remain absolutely private and concealed subject to those very limited circumstances. In other words, it is not as if the subscriber understands that all employees of an ISP will be privy to his emails but expects the ISP will not share the contents with other parties; rather, it is the subscriber's expectation that the ISP will not review the contents of his emails, except, perhaps, in very limited circumstances. Moreover, while the Supreme Court specifically

noted that the documents at issue in *Miller* were "not confidential communications," *Miller*, 425 U.S. at 442, emails obviously are confidential communications. In short, an email subscriber does not knowingly expose the contents of his or her emails to any third party and the ISP does not have the right or discretion to review a subscriber's email in the ordinary course of its business.

b. The search and seizure of the contents of Mr. Hamama's emails violates the attorney client privilege and Mr. Hamama's right to counsel under the Sixth Amendment.

The Supreme Court recognized that the right to counsel in a criminal trial is fundamental and essential to a fair justice system. *Gideon v. Wainright*, 372 U.S. 335, 344-345 (U.S. 1963). In recognizing that the right to counsel is essential to a fair trial and the presentation of an effective defense, the court also found an *obvious* interest in the defendant's relationship to his or her attorney. *Morris v. Slappy*, 461 U.S. 1, 20-21 (U.S. 1983). (Emphasis added). A defendant's relationship with his or her attorney must enjoy the highest level of protection from prosecutorial intrusion to allow client and attorney to engage in open and honest discussions about the accusations so as to prepare a defense. *Id.* "[B]ut in order to do so effectively… the defendant [may be required] to disclose embarrassing and intimate information to his attorney. In view of the importance of uninhibited communication between a defendant and his attorney, attorney-client communications generally are privileged." *Id.* Accordingly, when the Government is able to invade the attorney-client privilege it undermines the right to a fair trial and threatens the entire justice system because it raises substantial doubts about the confidentiality that attorney client communication enjoys.

Mr. Hamama communicated with his attorney on numerous occasions using email. *Exhibit C*. The subpoenas to obtain the contents of Mr. Hamama's email set a precarious precedent. None of the charges in this case relate to any electronic transactions except that Mr. Hamama may have completed an SF-86 online. The genesis of Mr. Hamama's charges are alleged activities in the early 1990s. All of the evidence the government seeks to use against Mr. Hamama is from alleged activities in the mid to late 1990s. The charges alleging false statements arise from a statement to the FBI and a statement on a security clearance application form. Both were made after 2003. The heart of the Government's case rests on activities that predate the U.S. invasion of Iraq in 2003. Based on the Government's theory in pursuing Mr. Hamama, once the Saddam Hussein government was deposed, Mr. Hamama would have lost his contacts and handlers because his loyalty rested with the former regime. There is no evidence that Mr. Hamama ever engaged in email communications with his alleged handlers or whether the targeted email accounts even existed. Simply charging a continuing conspiracy is insufficient to reach the burden necessary to overcome the protections of the Fourth Amendment or the Sixth Amendment.

The defense is unaware of any additional evidence in the Government's possession that supports a reasonable inference that Mr. Hamama's emails contain any evidence related to criminal activity. In short, the Government is on a fishing expedition. If every time an indictment issues prosecutors are permitted to obtain email records, the protections of the Fourth Amendment would be rendered meaningless. Email has become one of the most frequent and commonly used methods of communication. We use it trusting that that it will remain private. We have faith that it will remain private because we rely on companies that have built their reputations on ensuring user privacy. We go to great personal lengths to protect it from prying

eyes by creating passwords that have become increasingly complex to ensure that email accounts remain protected and private. Attorneys, therefore, use email to communicate with clients trusting that their communications will remain confidential and private except in some very narrow circumstances. Physicians use it to communicate with patients expecting that their conversations are private. Even this court uses email to communicate with attorneys and internally, with the expectation that the communication is private.

Permitting the government to obtain Mr. Hamama's email records eviscerates the attorney client privilege and undermines the right to unreasonable searches under the Fourth Amendment. This court should quash the subpoena and protect the emails. If the Government is able to overcome their burden by presenting evidence amounting to probable cause, this court should review the contents of the email accounts *in camera* to ensure that the Mr. Hamama's attorney-client privilege is not violated. An offer by the government to have a "taint" team review the emails is unacceptable. The attorney-client privilege does not exist to merely shield attorney client communications from prosecutors, it exists to shield information from the entire world. Without such a shield clients cannot develop a relationship based on trust and confidence with their attorneys to properly prepare a defense.[2] *See Linton v. Perini*, 656 F.2d 207, 212 (6th Cir. 1983)(trust between counsel and defendant is the cornerstone of the adversary system and effective assistance of counsel).

WHEREFORE, Mr. Hamama, by and through undersigned counsel, respectfully requests that this court quash the subpoena. If the Government can overcome its burden to obtain the emails, Mr. Hamama respectfully requests that this court review the content of both email

[2] The American Bar Association Standards for Criminal Justice state that "[defense] counsel should seek to establish a relationship of trust and confidence with the accused." ABA Standards for Criminal Justice 4-3.1(a) (2d ed. 1980) (hereinafter ABA Standards). The Standards also suggest that "[nothing] is more fundamental to the lawyer-client relationship than the establishment of trust and confidence." *Id*., at 4.29 (commentary)

accounts *in camera* to ensure that all attorney-client privileged communications is removed before the emails are provided to the Government.

Respectfully submitted,

/S/ Haytham Faraj
Haytham Faraj (P72581)
Attorney for Defendant
22167 Morley Ave.
Dearborn, MI 48124
(313)457-1390
Haytham@puckettfaraj.com

CERTIFICATE OF SERVICE

I hereby certify that on December 1, 2010, I electronically filed the foregoing paper with the Clerk of Court using the ECF system which will send notification of such filing to the following: Mr. Michael Martin, Assistant U.S. Attorney at michael.c.martin@usdoj.gov and Ms. Cathleen Corken, Assistant U.S. Attorney at cathleen.corken@usdoj.gov.

/S/ Haytham Faraj
Haytham Faraj (P72581)
Attorney for Defendant
22167 Morley Ave.
Dearborn, MI 48124
(313)457-1390
Haytham@puckettfaraj.com