UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	
V.	)	NO. 09-CR-10017-GAO
TAREK MEHANNA	)	

MOTION IN LIMINE TO EXCLUDE ALL ELECTRONIC EVIDENCE FOR WHICH AUTHENTICITY HAS NOT BEEN ESTABLISHED

The defendant, Tarek Mehanna, requests that this court exclude all electronic evidence that has not been properly authenticated under the Federal Rules of Evidence. In order to be admissible at trial, certain electronic evidence must be authenticated in accordance with F.R.E. Rule 901(a).

The authentication of a document is necessary to establish that a document is what it purports to be and that there is a relationship between the document and an individual. See F.R.E. 901. It is critical that emails or other electronic communications used against criminal defendants be properly authenticated because it is so easy to create, alter, and manipulate electronic evidence. In determining whether the evidence is admissible, the trial court "must conclude that it was reasonably probable that the evidence had not been altered since the occurrence of the crime." United States v. Williams,

809 F.2d 75, 89 (1st Cir. 1986), *cert. denied,* 482 U.S. 906, 107 S.Ct. 2484, (1987). If the offered evidence is not readily identifiable or is susceptible to alteration, a testimonial tracing of the chain of custody is necessary. U.S. v. Abreu, 952 F.2d 1458, 1467 (1st Cir. 1992). "The purpose of testimonial tracing is to render it improbable that the original item either has been exchanged with another or has been tampered with or contaminated." See id. at 1467.

The Government's purports to admit at trial numerous electronic exhibits that have not yet been authenticated. These exhibits include every email, chat, and website posting on the trial exhibit list. The majority of these unauthenticated emails, images, chats, and web postings are grossly irrelevant. Even where it may be marginally relevant, the relevance is greatly outweighed by its potential to mislead the jury and impose unfair prejudice on the defendant.

The government's electronic evidence can be divided into two groups: 1) active communications; and 2) passive documents. The active communications consist of forum posting, instant message chats, and emails that involve one person somehow communicating with another. The second category consists of electronically stored data that was allegedly found on the defendant's computer, such as videos, photos, Word documents, and other such files that do not involve two or more people

communicating with one another. Both of these types of electronic evidence raise serious questions concerning not just authenticity, but also their relevance and their serious prejudicial effect.

The government has not provided any of the needed authentication to demonstrate chain of custody, completeness, or whether the electronic evidence was ever opened and downloaded to, or from, the defendant's computer. For example, the government raised in its proffer a photo of the Nick Berg beheading and argued that the defendant actively downloaded this image. However, after many hours of computer forensic scrutiny and analysis, the defense discovered that this photo was a "cached" file, meaning it was downloaded automatically from a website without the defendant's knowledge. The website could have been the BBC, CNN, or any other legitimate news organization that carried the image as part of a news story. It is this type of conflation by the government (and potentially a jury) of what is active versus passive communication that is extremely prejudicial to the defendant. The Court cannot allow a jury look at the evidence found on the defendant's computer and allow the government to characterize all of it as "actively" belonging to him. The government uses all of these exhibits to show the defendant's intent or state of mind. To that end, improper authentication is a gross misrepresentation of what

these materials are and what the defendant's intent was in having them on his computer.

The government further intends to use against the defendant active communications like emails and chats. However, the government must set out the identity of every person the defendant was communicating with in these correspondences. If the government intends to use the defendant's exercise of his First Amendment rights against him, it is critical they provide evidence that it indeed was the defendant's words used in the electronic communication. Additionally, it is imperative to know exactly whom the defendant was allegedly communicating with, and moreover, making sure the proffered evidence in those emails can be authenticated to guarantee they have not been altered in any discernable way.

Finally, the majority of these unauthenticated emails, images, chats, and web postings are irrelevant. The government is attempting to piece together thousands of irrelevant Islamic-related electronic evidence in an effort to frame the defendant a "homegrown terrorist." Even where there may be an argument for relevancy, the relevance is greatly outweighed by its likelihood to mislead the jury and impose unfair prejudice on the defendant.

We therefore move this court to exclude all trial exhibits that derive from computer evidence as not authentic and irrelevant.

TAREK MEHANNA
By his attorneys,

CARNEY & BASSIL

/S/ J. W. Carney, Jr.
J. W. Carney, Jr.
B.B.O. # 074760

/S/ Janice Bassil
Janice Bassil
B.B.O. # 033100

Sejal H. Patel
B.B.O. # 662259
Steven R. Morrison
B.B.O. # 669533
John E. Oh
B.B.O. # 675916
Carney & Bassil
20 Park Plaza, Suite 1405
Boston, MA 02116
617-338-5566

Dated: October 3, 2011

Certificate of Service

I hereby certify that this document filed through the ECF system will be sent electronically to the registered participants as identified on the Notice of Electronic Filing (NEF) and paper copies will be sent to those indicated as non-registered participants on or before the above date.

/S/J. W. Carney, Jr.
J. W. Carney, Jr.