

Steven Sutcliffe

From: steven.sutcliffe [steven.sutcliffe@gmail.com]

Sent: Tuesday, November 21, 2006 2:35 PM

To: Sung B. Park

Subject: RE: IMPORTANT: jurisdiction

SHOW ME WHERE YOU BELIEVE THE GOVERNMENT PROVED I TRANSMITTED ANY PAGE ESTABLISHED THROUGH A NETWORK LOG FILE.

IN ALL THE CASES CITED THE ACCUSED ADMITTED TRANSMITTING. THE GOVERNMENT WAS NEVER PUT TO THE CRUCIBLE OF PROVING IT.

I DON'T ADMIT TRANSMITTING.

Steven Sutcliffe

From: steven.sutcliffe [steven.sutcliffe@gmail.com]
Sent: Monday, November 20, 2006 7:43 PM
To: Sung Park
Subject: 3 issues we discussed Number 2

Showing that the defendant was in fact the one who transmitted the page(s) in question.

Here was the case cited in Hew Hampshire when I was arrested there. U.S. v. WHIFFEN, 121 F.3d 18 (1st Cir. 1997)

"[t]o establish a violation of section 875(c), **the government must establish that the defendant intended to transmit the interstate communication** and that the communication contained a true threat. Whether a communication in fact contains a true threat is determined by the interpretation of a reasonable recipient familiar with the context of the communication. The government does not have to prove that the defendant subjectively intended for this recipient to understand the communication as a threat.

Darby, 37 F.3d at 1066. Our sister circuits have also considered what constitutes a "true threat" under other federal threat statutes. See United States v. Fulmer, 108 F.3d 1486, 1491 (1st Cir. 1997) (collecting cases). "

"the government must establish that the defendant intended to transmit the interstate communication "

Mr. Park, There is only one way to establish that the defendant intended to transmit the "communication." They must show the defendant did it in deed transmit it or get someone else to do it.. At least that is the standard in the first circuit. That element was never stated in the government's indictment. Nor proved at trial: EXAMPLE:

The fact that he had access to it shows his identification, shows it was *most likely* him that *posted it.*" Page 2139, Lines 11-15 Elena Duarte

Sung, anyone with a username and a password had access to it. You said that in the opening brief: Agent Harrill also testified that either the owner of the website or someone who has the user ID and password to the FTP upload section could upload the content on the website. (RT 534).

PROSECUTOR: "And all of the representatives that testified, testified that the manner in which to upload Webpages to the website that they hosted was [generally] by 'FTP' – File Transfer Protocol – which is the transfer of the electronic data from one area to another." Page 2143, Lines 21-25

Page 2147, Lines 11-16

PROSECUTOR: "Now, **you also heard the elements** of the second group of charges: Transferring social security numbers with the intent to aid and abet. And you heard the **elements of that:** That the defendant acted knowingly, ***that he transferred the number***, that it was in a manner affecting interstate commerce

"that he transferred the number" is an element, admitted by Duarte. Not someone else. They must prove that "he" transferred it. Not someone or something else transferred it.

The only way to prove who transmitted it is through the use of the server's logs.

ENTER: GOVERNMENT WITNESS: WILLIAM SIEBERT, Director of Customer Relations, Guidance Software/computer forensics consultant.

Page 1608, Lines 15-20

PROSECUTOR: "In your opinion, were they the product of visiting a site, perhaps making a download or two, and then backing up that data?"

ANSWER: "It is possible that that is the product of '**downloading**' a webpage or an – **downloading** the webpage **or** actually creating it on his machine and **uploading** it back to the Internet."

Page 1608, Lines 21-25, Page 160, Lines 1-4

PROSECUTOR: "In your examination of the seized media, were you able to form an opinion on who created – I should say, on whether the website 'evilgx.com' was created on the computer that you were examining?"

ANSWER: "Yes. I would most definitely say that the 'evilgx.com' webpages were built on the hardware seized from Mr. Sutcliffe."

PROSECUTOR: "Nothing further, Your Honor."

COURT: "Okay. Anything further?"

DEFENDANT: "Yes, Your Honor, just one question."

Page 1609, Lines 7-11 and 17-21

DEFENDANT: "Of these pages you talked about that were created – on 'evilgx' that were created on this computer, can you tell with 100 percent accuracy whether all of these pages were created by the defendant?"

ANSWER: "No, I cannot."

DEFENDANT: "And if those pages were **downloaded** to somebody else who had FTP access to that website, they could tinker with the page, too, couldn't they?"

ANSWER: "Yes. They could alter the Webpages that were up on the internet."

Page 1610, Lines 9-

DEFENDANT: "Can you tell, through your analysis, where physically the defendant or anybody was when that page, or any of those pages, was put up on the website?"

ANSWER: "No, I can't tell you where the computer was physically located when the webpages were created and **posted** to the internet."

DEFENDANT: "Nothing further, Your Honor."

ENTER: GOVERNMENT WITNESS: MONTE WHITE, Customer Support Manager, Intercosmos MediaGroup, New Orleans, Louisiana.
INVOLVES EXHIBITS: 42& 43

Page 1307, lines 11-13

PROSECUTOR: "In other words, do those logs reflect the *successful uploads* to the website?"

ANSWER: "No." [1]

ENTER: GOVERNMENT WITNESS: DAVID JOHNSON, Team Lead for Network Abuse Team, Comcast Cable Company.
INVOLVES EXHIBITS: 31 & 32

Page 1276, Lines 4-25

PROSECUTOR: "Does this [exhibit] also show any kind of identifying feature or address for the computer [of the accused[2]]?"

ANSWER: "On the bottom portion of the page, it shows the MAC address[3] of the computer[4]"

QUESTION: "The which address?"

ANSWER: "The MAC address."

QUESTION: "Without getting to technical, what is the purpose of assigning a MAC address to this account?"

ANSWER: "*The MAC address actually is the single identifier for a PC or a computer device, and that is essentially what ties a computer to an IP address at a given time.*"

QUESTION: "Does that MAC address actually correspond to hardware in the user's computer?" [5]

ANSWER: "It does." [6]

Page 1278, Lines 1-17

Q: "What time do these – what time frame do these records cover ...?"

A: "They cover the period of February 1, 2002 to March 22, 2002."

Q: "And were there any records available before that time for this computer and this IP address?"

A: "No."

Q: "So do you know whether or not -- this IP address that was originally assigned in November and that we see being used from February on, do you know whether or not for sure that was the same IP address being used in the interim?"

A: "No."

Page 1280, Lines 3-15

ACCUSED:

Q: "To your knowledge, does AT&T or Comcast have any knowledge of any logs[7] available for any dates between January and March 29th of disconnect and connect times from that cable modem?"

A: "Not to my knowledge."

Q: "To your knowledge, does Comcast or AT&T have any logs available for locations of that cable modem between January and March of 2002?"

A: "Locations of the actual cable modem device as to who – which customer may have had it at that time?"

Q: "Well, the IP address. I'm speaking specifically to the IP address?"

A: "Okay. To the IP address, not to my knowledge."

ENTER: GOVERNMENT WITNESS: MAURICE GILMORE, Owner of Hosting Solutions, Virginia, HOST from January 9 till February 18, 2002. (See page 1114)
INVOLVES EXHIBIT 36 "Subscriber Info," not FTP log transfer info!

Page 1108, Lines 8-18

PROSECUTOR: "By 'uploading their website,' is there a particular method or way to upload that your system used?"

A: "Yes. Our clients, they use a protocol FTP. And what they'll do, from they're home PC, they'll just upload their contents to our servers.

Q: And by 'upload' to your computer, does that constitute a physical *transfer* to your computer?"

A: " Yes. It does."

ENTER: GOVERNMENT WITNESS: FRANK HARRILL, Special Agent, FBI, Original Case Agent In Charge

Transcript of 11.13.2003

Page 417, Lines 7-25

PROSECUTOR: "Once a website is on the Internet, can it be changed?"

A: "It can."

Q: "How is that?"

A: ***Anyone with access to the website can upload*** – we've talked about FTP – updated content, and they could change one web page or they could change the entire website at virtually anytime."

[1] Right after this testimony the judge remembers the defense requested a copy of a pretrial status conference transcript requested TWO MONTHS ago and finally provides a copy for the accused. See page 1312, lines 15-23.

[2] The computer NIC was never entered as an exhibit, nor was the computer as a whole, either.

[3] Ethernet addresses are known as Media Access Control (MAC) addresses, hardware addresses, or sometimes just Ethernet addresses. Since many computers may share a single Ethernet segment, each must have an individual identifier.

These identifiers are hard-coded on to the NIC. A NIC is a Network Interface Card. A MAC address is a 48-bit number, also stated as a 12-digit hexadecimal number. This number is broken down into two halves, the first 24-bits identify the vendor of the Ethernet card, and the second 24-bits is a serial number assigned by the vendor. See INTRODUCING NETWORK ANALYSIS, SYNGRESS PUBLISHING, http://www.syngress.com/book_catalog/284_eps/sample.pdf

[4] MAC addresses are unique, and no two computers should have the same one. However, this is not always the case. Occasionally there could be a manufacturing error that would cause more than one network interface card to have the same

MAC address, but mostly, people will change their MAC addresses on purpose. This can be done with a program, such as ipconfig, that will allow you to fake your MAC address. Faking your MAC address is also called spoofing.

[5] There is no way he could know without examining the defendant's computer and Network Card. See fn. 4, supra.

[6] See Government's Response To Court's Order On Computer And Email Evidence, United States Of America V. Zacarias Moussaoui, Crim. No. 01-455-A Eastern District Of Virginia, Alexandria Division

(Sept. 2002). "In October 2001, further investigation revealed that that IP address was assigned to PC11, a lab computer on the campus of the University of Oklahoma, using Network Interface Card identified with MAC address 00:B0:D0:43:85:C8." Page 12, Ibid. Source:
<http://news.findlaw.com/hdocs/docs/terrorism/usmouss90402grsp.pdf>

[7] "Clearly, the FBI needs engineering personnel to develop and deploy sophisticated electronic surveillance capabilities in an increasingly complex and technical investigative environment, skilled CART personnel to conduct the computer forensics examinations to support an increasingly diverse set of cases involving computers, as well as expert NIPC personnel to examine network log files to track the path an intruder took to his victim. In cases such as Los Alamos or Columbine, both NIPC and CART personnel were called in to bring their unique areas of expertise to bear on the case." See, Statement for the Record of Louis J. Freeh, Director Federal Bureau of Investigation on Cybercrime Before the Senate Committee on Appropriations Subcommittee for the Departments of Commerce, Justice, State, the Judiciary, and Related Agencies Washington, D.C. February 16, 2000

SUNG PLEASE NOTE:

Transcript of 11.07.2003

Page 62, Lines 15-18

Judge: "The Planned Parenthood case makes it clear that there is no constitutional infirmity in 875(c). The facts of this case will warrant a prosecution.

Page 63, Lines 12-25 deals with **jurisdiction Motion filed early in 2003**

.Defendant: "I don't believe the Government can prove that and I demand the Government have to prove that **before** they try me."

Page 64, Lines 1-7

Judge: "**Your demand that the Government have to prove that is granted.** [1] The Government will have to prove that the facilities of interstate commerce were used in connection with the conduct alleged in the indictment. If it proves that, there is no jurisdictional barrier to an other wise valid conviction."

Defendant: "Thank you, Your Honor." [2]

[1] See RT 11.12.2003, Pages 4-6

[2] The judge never allowed the defendant to put the government to the test, BEFORE any trial took place. See fn. 12 above. This written challenge was later PLACED IN FILE – NOT USED. It is now missing from the file.

Steven Sutcliffe

From: steven.sutcliffe [steven.sutcliffe@gmail.com]
Sent: Tuesday, November 21, 2006 12:55 PM
To: Sung Park
Subject: network log files = jurisdiction

network log files = jurisdiction

"Clearly, the FBI needs engineering personnel to develop and deploy sophisticated electronic surveillance capabilities in an increasingly complex and technical investigative environment, skilled CART personnel to conduct the computer forensics examinations to support an increasingly diverse set of cases involving computers, as well as expert NIPC personnel to examine network log files to track the path an intruder took to his victim. In cases such as Los Alamos or Columbine, both NIPC and CART personnel were called in to bring their unique areas of expertise to bear on the case." See, Statement for the Record of Louis J. Freeh, Director Federal Bureau of Investigation on Cybercrime Before the Senate Committee on Appropriations Subcommittee for the Departments of Commerce, Justice, State, the Judiciary, and Related Agencies Washington, D.C. February 16, 2000

CALL ME IF YOU STILL DON'T AGREE WITH THIS PREMISE.