

States v. Ellyson, 326 F.3d at 533. That is not the case here.

In United States v. Kilmer, the evidence introduced at trial established that every pornographic image the defendant received or distributed using his and his family's Hotmail accounts traveled through the Hotmail servers in California and his internet service provider in Missouri before reaching his computer in Wichita, Kansas. En route, the data traveled across state lines, at least some of the way over ordinary phone or cable lines. Even email messages sent from one of defendant's accounts to another account on his computer traveled across the Kansas state line to his internet service provider located in Kansas City, Missouri, then back over the state line to the defendant's computer in Kansas. United States v. Kilmer, 335 F.3d at 1135. In light of such evidence, the Tenth Circuit found evidence of interstate transmission. Id., at 1139-1140.

In this case, there is no evidence to show that the materials that were posted on the website were actually transmitted across state lines. First of all, with respect to Counts Three, Six, Seven, and Nine, the government cannot even prove where the servers were located at the time the postings were uploaded at evilgx.com. Without proving where the servers were located and where Mr. Sutcliffe or the

person who posted the webpages was at the time the webpages were posted, the government cannot demonstrate that the messages crossed state lines.

Moreover, the government must prove that information transmitted across the Internet crossed state lines and was transmitted or edited on the server in Interstate Commerce by the defendant. Here we have a case where the government did not prove that Mr. Sutcliffe transmitted the messages because the government failed to produce any network log files that specifically identified his MAC address and a corresponding IP address showing the dates and files uploaded or edited by Mr. Sutcliffe.<sup>15</sup> Network log files are the only way to prove a specific computer uploaded any file and the dates and times of the upload or edit on a server. An IP address by itself without the corresponding MAC<sup>16</sup> does not show which computer was used to upload a

---

<sup>15</sup> "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." (RT 1276).

<sup>16</sup> "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

file. The government did not match the MAC address to Mr. Sutcliffe's computer during the trial. The government can make an inference but nothing conclusive or entirely reasonable beyond doubt can be establish without the log files containing the MAC address from the servers as well as the defendant's matching MAC from a computer identified as being used by the defendant.<sup>17</sup> Mr. Sutcliffe was not the only one with access to the files in question nor was he the only one in possession of a username and password or a computer.<sup>18</sup> (See also RT 1303-1304). Without the log files the government's jurisdiction argument fails.

---

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 (emphasis added).

<sup>17</sup> "The fact that he had access to it shows his identification, **shows it was most likely him** that posted it." (RT 2139)(emphasis added).

<sup>18</sup> "BY MR. SUTCLIFFE:

Q: 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?

A: No, I cannot.

Q: 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?

A: Yes. They could alter the webpages that were up on the internet.

Q: 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?

A: No, I can't tell you where the computer was physically located when the webpages were created and posted to the

C. SECTION 875(C) IS UNCONSTITUTIONAL ON ITS FACE FOR VAGUENESS.<sup>19</sup>

The government does not deny that only true threats and threats made with specific intent are punishable under section 875(c). However, it argues that the statute does not need to define what constitutes a threat or spell out the intent requirement in order for it to make clear what conduct is prohibited. (AB 33). The government is wrong.

Without the definition of a true threat and the requirement of a specific intent provided in the statute, an ordinary citizen would not be able to determine which conduct is prohibited. For example, threats made in jest or threats that constitute a political hyperbole (See Watts v. United States, 394 U.S. 705 (1969)) do not qualify as true threats under section 875(c); however, the statute as worded would make them punishable.

Without any guidance within the statute as to what constitute a true threat, section 875(c) fails to provide fair warning of the prohibited conduct to those it regulates. This is especially true because the statute involves a constitutionally protected right of freedom of speech. See Planned Parenthood Fed'n of Am, Inc. v. Gonzalez, 435 F.3d

---

internet." (RT 1609-1610).

<sup>19</sup>Mr. Sutcliffe filed a motion, challenging the vagueness of the statute. (ER 208).