

waiver of their right to counsel. Fazzini, 871 F.2d at 642; Moore, 706 F.2d at 539.

In this case, the record shows that Mr. Sutcliffe was actively involved in his defense. Nothing he did to have his counsels relieved constituted a waiver of his right to counsel.

B. THE TRIAL COURT LACKED JURISDICTION.

It appears that the issue of whether posting an allegedly threatening message on the Internet satisfies the interstate commerce requirement under section 875(c) has not been clearly determined by this Court. The government cites to United States v. Pirello, 255 F.3d 728 (9<sup>th</sup> Cir. 2001) to argue that the interstate commerce requirement has been satisfied.

However, in United States v. Pirello, 255 F.3d 728 (9<sup>th</sup> Cir. 2001), this Court did not hold that information posted on the Internet necessarily crosses state lines, let alone hold that internet is an instrumentality of interstate commerce. The Court simply stated as a background to the case that Internet could be used to reach a large number of people.<sup>14</sup>

---

<sup>14</sup>This Court stated that "[t]he Internet engenders a medium of communication that enables information to be quickly,

The government also cites United States v. Ellyson, 326 F.3d 522 (4<sup>th</sup> Cir. 2003) and United States v. Kilmer, 335 F.3d 1132 (10<sup>th</sup> Cir. 2003). These cases are also distinguishable.

In United States v. Ellyson, the Fourth Circuit held that in a possession of child pornography case, the prosecution met the interstate requirement because some of the pornographic images that were downloaded contained the Internet addresses for European child pornography websites or other indications that the image originated from a particular website, such as a logo. The Fourth Circuit concluded that a graphic reference to a European child pornography website, where it is superimposed over the visual depiction itself, is sufficient evidence, albeit circumstantial, to establish an interstate nexus. United

---

conveniently, and inexpensively disseminated to hundreds of millions of individuals worldwide. This quality makes the Internet a well-known and valuable tool for businesses and individuals seeking to advertise their goods to a large number of people. Unfortunately, however, the power to solicit money instantly and inexpensively from hundreds of millions of people through Internet advertising presents a double-edged sword. The same characteristics that make the Internet a valuable tool in today's commerce --i.e., the ability to effectively and efficiently reach a large audience of prospective buyers --also make it a seductive playground for unscrupulous individuals bent on defrauding innocent victims." United States v. Pirello, 255 F.3d at 729-730 (citations and quotations omitted).

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