

## **U.S. v. Trader**

(11th Cir 2020) 981 F.3d 961

### **Issue**

Must officers obtain a search warrant or other court authorization to obtain a suspect's email and internet protocol addresses from a provider?

### **Facts**

The parent of a nine-year old girl discovered that someone named Scott had emailed child pornography to her and had solicited nude photos. The request was made via an app called SayHi. The case was referred to the Department of Homeland Security (DHS) which determined that the sender also had an email account with an app called Kik. Pursuant to an emergency disclosure request by DHA agents, Kik sent them Scott's email and internet protocol (IP) addresses. This information led them to Scott's internet service provider, Comcast, so they sent Comcast an emergency disclosure request for subscriber records associated with that IP address. Comcast complied.

With this information, agents learned that the person who sent the photos was Scott Trader with an address in Florida. As the result, they obtained a warrant to search Trader's home, and this led to the discovery of child pornography of more than forty minors, including one of Trader's daughters.

After Trader was charged with enticing a minor to engage in sexual activity and possessing and distributing child pornography, he filed a motion to suppress the evidence obtained as the result of the disclosure requests. The motion was denied, and he pled guilty to all charges. He was sentenced to life in prison.

### **Discussion**

Although Kik and Comcast furnished the information to the agents voluntarily, he argued that they cannot obtain this information without a search warrant. In the past, it was settled that a warrant was not required to obtain information that a person had transmitted to a third party. But in 2018, the Supreme Court ruled in *Carpenter v. United States* that a warrant was required to obtain a suspect's cell site location information (CSLI).<sup>1</sup> The Court reasoned that people can reasonably expect that such information will be private because "cell phone users do not share their cell-site location information voluntarily," and that "carrying a cell phone is indispensable to participation in modern society."

The court in *Trader*, however, ruled that *Carpenter* does not restrict requests for "ordinary business records like email addresses and internet protocol addresses." Although it is true that such records could eventually lead agents to more private information, email and IP addresses, the court explained that "this kind of business record that might incidentally reveal location information falls outside *Carpenter*'s narrow exception to the third-party doctrine. Accordingly, the court ruled that a warrant was not required to obtain this information, and it affirmed Trader's conviction and sentence. POV

**Date posted:** March 18, 2021

---

<sup>1</sup> (2018) \_\_ U.S. \_\_ [138 S.Ct. 2206].