

The suspect on the network was arrested after the provider shared VPN access history with the FBI

VPN service providers often advertise their products as a way to surf the web anonymously, that they never record user activity. But a recent case shows that there are at least a few units that record user activity history.

VPN service providers often advertise their products as a way to surf the web anonymously, that they never record user activity. But a recent case shows that there are at least a few units that record user activity history.

That was the case of Ryan Lin, a 24-year-old man from Newton, Massachusetts, who was arrested Thursday 5 October for allegedly tracking other people online.

According to the affidavit with the FBI published by the US Department of Justice, Lin was accused of harassing and tracking an unidentified 24-year-old woman, called Jennifer Smith, from April 2016 to the time of being arrest.

It all starts with an ad on Craigslist

The two met after Lin answered an ad on Craigslist and moved to Smith and two other roommates. FBI said that shortly after moving to Smith, Smith became a victim of many hacking, harassment and online surveillance. Investigators believe that Lin obtained a password for some of Smith's accounts because she did not lock the room and the computer did not set a password.

Lin is accused of accessing Apple iCloud account of Apple, downloading personal photos and personal logs on Google Drive account.

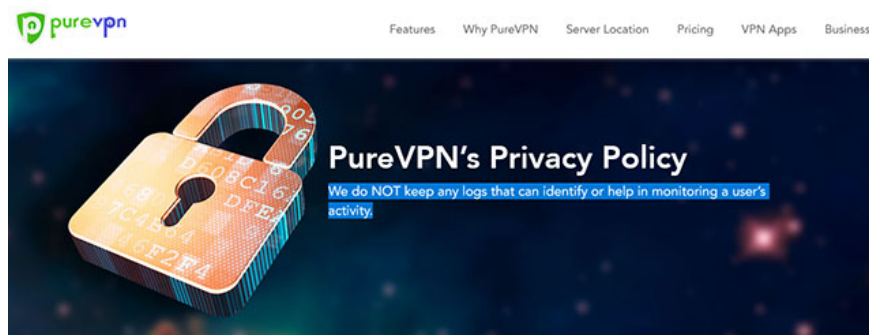
Smith is also a victim of many harassment

According to the testimony, Lin was the biggest suspect after many months of harassment. Smith told authorities that the abusive behavior began when Lin moved in and continued even after she had moved two months later, which made her very afraid.

Lin's behavior then moved to the other two roommates, and due to complaints from the police, the landlord Lin was expelled from the shared apartment in August 2016. The act of harassment and follow-up still takes place, primarily towards Smith.

Suspects behind VPN, Tor and ProtonMail

To perform their behavior, suspects use ProtonMail, VPN software and Tor to hide their identity. After investigating for nearly a year, the police asked the FBI for help.



Thanks to the history of VPN service, the FBI found Lin's criminal evidence

The first FBI evidence came from Lin's former boss when the company reinstalled the computer he used after quitting, from which the FBI found many artifacts on Chrome showing Lin read about a bomb threat at a school. Local, have an account on ProtonMail, see Smith's Spotify page and her friends .

VPN activity history binds Lin to Smith's harassment

The evidence decides when the FBI gets a history record from two VPN providers: PureVPN and WANSecutiry. Accordingly, in a few minutes, the same VPN IP address will log into Lin's real Gmail account and another Gmail account and Rover.com account that Lin created to find Smith's phone number.

PureVPN then connected the tracking action to the home and Lin's IP address. This information surprised some PureVPN customers because the company announced it would not save the user's activity history.

The funny thing is that the FBI also found a tweet from Lin warning users of VPNs about storing their history. The investigator was sure to find the right person when interviewing some of Lin's former classmates, showing off previous harassment, follow-up behavior, and calling this man 'computer genius'.

"This behavior is not a joke and is not harmless. He makes people afraid, hinders their daily life and is not aware of his obsession. No one should feel unsafe at home, school or work. The FBI and authorities hope this arrest will prevent similar acts, 'agent FBI Charge Shaw said.

You finished reading the article "**The suspect on the network was arrested after the provider shared VPN access history with the FBI**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.