
Privacy software, criminal use

By Jenifer B. McKim

Globe Staff / March 8, 2012

A Walpole nonprofit company, largely funded by the federal government, is inadvertently providing child pornographers, drug dealers, and other criminals around the world with software that allows them to remain anonymous on the Internet.

The little-known organization, Tor Project Inc., says its free program is designed to help people protect themselves from Internet surveillance. Users include those speaking out against oppressive political regimes in other countries, corporate whistle-blowers, law enforcement officials, and domestic abuse victims.

But the software, which can easily be downloaded from the Tor Project website, also is attracting a growing number of people who trade illegal pornographic material and buy and sell drugs on a part of the Web known as the "darknet," according to federal authorities, advocates for children, and Internet specialists.

Its use for illicit purposes creates new challenges for law enforcement officials hunting increasingly technologically savvy criminals, and highlights the sometimes unwanted consequences of protecting free speech online.

The darknet is "a secret Internet," said Chester Wisniewski, senior adviser at Burlington computer security company Sophos Inc. "It's free speech to the extreme. It's really tragic there are some sickos using this same technology for their purposes."

The Tor Project is widely considered the largest service in the world that allows users to navigate the Internet anonymously. Andrew Lewman, the organization's executive director, said he is approached regularly by law enforcement officials whose investigations have been frustrated by Tor technology, which hampers authorities' ability to identify suspected online criminals and masks the origin of child pornography and drug-dealing websites.

But Lewman said Tor Project and its software can't be blamed for aiding crimes in the same way cellphone and computer makers should not be held accountable for the misuse of those devices. He has rejected informal requests by law enforcement agencies to create a way for them to identify Tor users, saying it would defeat the purpose of the software. But Lewman said he is willing to help investigators better understand the technology, and provides a link on the Tor website for anybody to report evidence of child pornography.

"I'm not going to compromise Tor," said Lewman, who works out of a small storefront office on Main Street in Walpole. "'Good' is so relative around the world. I bet the Egyptian government didn't think their activists were good."

Tor stands for "the onion routing" project, initiated by the US Naval Research Laboratory in the 1990s to camouflage government communications by sending messages through a system of computers. The project was expanded in 2001 by two Massachusetts Institute of Technology students who made the technology more accessible to civilians. An added feature called "hidden services," launched in 2004, allows people to publish and visit websites without being identified.

In 2005, federal agencies started funding the project with the goal of making the technology easier for the public to use, Lewman said. The next year, it was established as a nonprofit.

Government officials say they support the project because it provides potentially life-saving online security and privacy in places - such as Iran and Syria - where political dissidents often are dealt with harshly. The State Department and two federal agencies - the Broadcasting Board of Governors and the National Science Foundation - are major contributors.

The Tor Project currently has a \$1.3 million annual budget, with about 15 full-time and contract employees. It also relies on 3,000 volunteers around the world who provide access to their computers. That allows the company to bounce data from one server to another, making it difficult to track.

"Tor is a publicly available tool. It is used by activists and bloggers, by average US citizens protecting against identity theft, and by military and law enforcement officers conducting investigations and intelligence gathering," a State

Department spokesman said.

Lisa-Joy Zgorski, a National Science Foundation spokeswoman, also cited the value of the software. "Any technology can be used for ill," she said. "It is not a reason not to fund the science."

The popularity of the Tor Project technology among pedophiles gained media attention last fall when a group of computer hackers associated with the online collective known as Anonymous took aim at child porn websites hidden on the darknet. The so-called hactivists claimed to have disabled several child porn sites as part of an effort dubbed "Operation Darknet" or "To catch a predator." As part of its campaign, Anonymous posted a video on YouTube pledging to fight sexual abuse.

"The darknet is a vast sea with many providers, however, we fully intend to make it uninhabitable for these disgusting degenerates," a narrator says in the YouTube video. "We will never turn a deaf ear upon the screams of innocent children."

John Shehan, executive director of the Exploited Child Division of the nonprofit National Center for Missing and Exploited Children in Virginia, said its investigators first discovered Tor's software about 1 1/2 years ago after receiving tips about pornographic images of children sent over the Internet by people who could not be identified. Center officials met with Lewman to figure out how Tor worked.

"It confirmed our suspicions that this product masks identity and it will be a major challenge for law enforcement," Shehan said.

Last June, democratic US senators Charles E. Schumer of New York and Joe Manchin of West Virginia called on federal officials to shut down the website Silk Road, which they called an "online marketplace for illegal drugs" that uses Tor technology. Schumer and Manchin were responding to an article by the media site Gawker.com that detailed drug dealing on Silk Road using a digital currency called "bitcoins."

Despite the senators' call for action - addressed to US Attorney General Eric Holder and MicheleLeonhart, the administrator of the Drug Enforcement Administration - Silk Road was still up and running Wednesday.

Representatives from Silk Road did not respond to an e-mail seeking comment Wednesday.

DEA spokesman Rusty Payne said the agency couldn't comment on the senators' letter because it is "is part of an ongoing investigation."

A Boston Globe editor and reporter were able to access the site after downloading Tor Project software and registering as Silk Road users. Described as an "anonymous marketplace," the site promotes its ability to "protect your identity through every step of the process, from connecting to this site, to purchasing your items, to finally receiving them," through the use of Tor technology. The homepage features pictures of various drugs for sale - including heroin and cocaine - and allows buyers to place them in a shopping cart, similar to those on Amazon and other consumer sites.

In addition to drugs, the site purports to provide access to other illegal products, including forged documents, and links to a separate marketplace called the Armory, designated for "small arms weaponry for the purpose of self defense."

Federal law enforcement officials acknowledge that Tor technology makes investigations of suspected illegal online activity more difficult, but they emphasize that it doesn't mean criminals can avoid detection. For instance, they say, even though an online drug deal may be anonymous, real money eventually has to be exchanged and the buyer must receive a physical package.

Investigators also have become more sophisticated in their efforts to hunt down criminals, they said.

"With any technology, it is going to add complexity to the investigative process," said Russ Brown, supervisor of the Boston Cyber Criminal Squad for the FBI. But Tor, he added, "is certainly not going to end our investigative efforts."

Mathematician Paul Syverson, an inventor of Tor technology at the Naval Research Laboratory in Washington, D.C., said it is unfortunate that the software is used to do harm. But while unsavory people already have various ways to disguise their identities, he said, fewer options are available for Internet users such as domestic abuse victims seeking to avoid stalkers or whistle-blowers trying to dodge online surveillance.

"There are lots of different reasons why somebody wants to protect the network location of what they are doing," Syverson said. "There are people doing bad things, but that is not what we made [Tor] for. There's lots of people using it for good things, too."

Jenifer B. McKim can be reached at jmckim@globe.com.

© Copyright 2012 Globe Newspaper Company.
