



(/EN_US?TRK_SOURCE=HEADER-LOGO)

The People Who Risk Jail to Maintain the Tor Network

WRITTEN BY JOSEPH COX (/AUTHOR/JOSEPHCOX)

April 27, 2015 // 10:10 AM EST



Image: Flickr/Mycatkins (<https://www.flickr.com/photos/bigmikeyeah/5353647273/in/photolist-pbB4Yd-oWayq3-9a5QPk-5FkfjC-adr9Az-4vnTeR-33fGbC-oW3LQq-Fa5Cy-dpsaTu-8XxE4q-5bm4LW-oV9nEw-oW7p6e-iYysDH-iYKFrn-oVyHA6-oYz2jo-iYKUVR-iYF9SK-nfckUq-nfdbBe-nuDoQA-nuDT75-nytcFV-oV7FV5-5BPbDz-h5cX3N-h5d5P9-h5efnn-8478Av-jV7hNZ-6CbTTP-85Sx74-85Sx7k---h5dWp8-8Q2W7w-8RT6wA-h5cZ9S-h5cVus-h5cRBW-h5e6sZ-h5cF8S-h5MhdU-h5d1YS-h5cPYN-h5cSXn-7u85kX/>)

Richard* had a long drive ahead of him. About an hour earlier, at 5:30 AM, his wife Lisa* had phoned.

"The house is filled up," she said in a calm but audibly tense voice. Richard, having just woken up and now trying to make sense of the call, thought there must have been another water leak in the basement.

Instead, his wife told him, the house was full of FBI agents and they wanted to talk to Richard.

"Okay, I'm on my way," Richard said. He threw on some clothes, grabbed his laptop and phone as requested by the FBI, and stepped out into the night. The interstate drive from Milwaukee, where he was working as a software engineer, back to his home in Indianapolis would take a good five hours, more than enough time to figure out what this was all about.

It was something to do with computers, Lisa had said. The only thing Richard thought may be linked to that was his Tor exit node.

The Tor network—originally a project funded by the US Navy (<https://www.torproject.org/about/sponsors.html.en>)—is a collection of servers, some big, some smaller, spread across the world. When a user connects to the network, her internet traffic is randomly pinged between at least three of these servers, all the while covered in layers of encryption, making it near impossible for anyone monitoring the traffic to determine who is sending it or where it is going to.

It allows dissidents to communicate anonymously, citizens to bypass government censorship, and criminals to sell drugs or distribute child pornography. Tor also facilitates special sites called "hidden services," part of the so-called dark web. These allow the owners of websites and their users to remain largely anonymous.

The final set of servers that Tor uses in this process are called "exit nodes," because they are the points at which a user's traffic exits the Tor network and joins the normal web that we use everyday.

Rather than being run by one company, most of these exits are set up by volunteers,

or “operators.” A few organizations maintain the larger exits, a number of universities have their own, and individual activists run some too. Edward Snowden reportedly had one (<http://boingboing.net/2014/05/21/edward-snowden-hosted-a-crypto.html>).

Richard was one of these operators.

Richard’s exit could have been implicated in just about anything

Although Richard, 57, assumed the call was related to his exit, he still didn’t know what specifically the FBI was investigating as he started the drive home.

“A child porn ring had been busted? Or a hacking attack? Or a bomb threat called in? I had no idea what it was,” Richard later told me over the phone.

When someone uses Tor, his IP address is that of the exit node he has been randomly assigned. This means that if someone emails a death threat, or sends a barrage of spam, it is the exit node’s IP that appears when the authorities start investigating the digital fingerprints of the crime. Richard’s exit could have been implicated in just about anything.

However, Kurt Opsahl, the deputy general counsel (<https://www.eff.org/about/staff/kurt-opsahl>) of the Electronic Frontier Foundation (EFF), believes that running a Tor exit is legal, at least under US law.

But if an operator runs an exit from his or her home, and on their own internet connection, “they may be confused with being the source of the traffic, instead of an exit node of the traffic,” Opsahl told me. To anyone looking at activity flowing from the exit—whether that’s child abuse material, or an attempt to hack a website—it looks

one and the same as the operator's own personal usage. This could lead to a raid on the operator's house, even though running an exit is arguably legal.

For this reason, and others listed (<https://blog.torproject.org/running-exit-node>) on the Tor Project website, operators are strongly advised to only run their exits remotely, by renting out server space.

This is what Richard did. Through a St. Louis-based company, his Tor exit had been whirring away in a German data centre for 18 months. But it appears that wasn't enough to stop a raid on his house.

- (2) evidence of software that would allow others to control the digital device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- (3) evidence of the lack of such malicious software;
- (4) evidence of the attachment to the digital device of other digital devices or similar containers for electronic evidence;
- (5) evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the digital device;
- (6) evidence of the times the digital device was used;
- (7) passwords, encryption keys, and other access devices that may be necessary to access the digital device;
- (8) documentation and manuals that may be necessary to access the digital device or to conduct a forensic examination of the digital device;

A section of the search warrant obtained by Motherboard, showing that the FBI were searching for malware, computer forensics programs and other pieces of evidence.

Back in suburbia, the FBI agents questioned Lisa. Why did the family rent so many cars? Why was Richard renting so many computers? Lisa, a salesperson for the computer networking firm 3Com Corporation, breezed through the more technical questions from the agents.

The raid had started before dawn. After turning up in eight unmarked law enforcement vehicles, the FBI agents pounded on the door and swarmed the house, automatic weapons drawn. They didn't even let Richard's sister-in-law turn on the coffee pot until the area was declared "secure." A team of computer experts entered

the property after the initial FBI squad. According to the search warrant obtained by Motherboard, they were looking for evidence of unauthorized access of a computer, theft of trade secrets, or conspiracy to do the same.

The experts seized the household server and a personal desktop computer, both running Linux. Noticeably, they left the other two Windows machines. After taking the computers, the agents conducted a more thorough search. One agent even looked behind a painting to see if anything was hidden. Although the rest of the house was left in a tidy state, Richard's office had been torn apart, he told me after he had seen the effect of the raid.

This wasn't the first time an operator had received a visit from law enforcement.

In 2013, police raided the home of William Weber, an Austrian IT administrator, and confiscated 20 computers, gaming consoles and other devices because child pornography had been transmitted across one of his many exits.

The following year, Weber was found guilty (http://www.theregister.co.uk/2014/07/04/austrian_tor_exit_relay_op_found_guiltily_for_ferrying_child_p0rn/) of distributing that illegal material. He decided not to appeal the ruling because he had already used all of his savings on legal fees. Before that, Weber claimed he had received threats (<https://rdns.im/court-official-statement-part-1>) of being extradited to Poland to face separate hacking charges, and police had subjected his friends and colleagues to questioning.

Another man in Germany, Alex "Yalla" Janßen, decided to shut down his exit (<https://itnomad.wordpress.com/2007/09/16/tor-madness-reloaded/>) after being raided twice by police.

"I can't do this anymore, my wife and I were scared to death," he blogged shortly after (<https://itnomad.wordpress.com/2007/09/16/tor-madness-reloaded/>). "I'm at the end of my civil courage. I'll keep engaged in the Tor-project but I won't run a server anymore. Sorry. No."

There aren't any concrete figures for how many operators have been raided due to running an exit, because the events aren't always reported. On top of that, it isn't clear how many operators there are in the first place. Although just over 1,000 exit nodes are up and running (<https://metrics.torproject.org/relayflags.html>) at the time of writing, an operator may maintain more than one node at a time. Regardless, out of the likely hundreds of people running exits, "I think it's a handful" that are raided, Andrew Lewman, former executive director of the Tor Project, told me over the phone. (Lewman recently left the Tor Project (<https://blog.torproject.org/blog/new-era-tor-project>) for another job).

"Law enforcement are given quotas and in this day and age, cybercrime is on the up and up"

Sometimes, an operator's home isn't raided, but her exit node is either shutdown, seized, or somehow tampered with by law enforcement. After noticing some strange activity on his exit, Thomas White, a UK based activist, took to a Tor mailing list.

"Having reviewed the last available information of the sensors, the chassis of the servers was opened and an unknown USB device was plugged in only 30-60 seconds before the connection was broken," White wrote in December (<https://lists.torproject.org/pipermail/tor-talk/2014-December/036067.html>). "From experience I know this trend of activity is similar to the protocol of sophisticated law enforcement who carry out a search and seizure of running servers."

When I asked White to elaborate on what exactly had happened, he said couldn't without facing legal consequences.

However, he did tell me that law enforcement have taken around 14 of his 40-something servers, and analysed many more.

"I suspect the reason behind most seizures or trouble is they want to be seen to be doing something," White continued. "Law enforcement are given quotas and in this day and age, cybercrime is on the up and up. Why spend millions on a large operation to catch a hacker when they can just seize a server and add another notch to the tally on their quotas?"

This month, another operator claimed (<https://lists.torproject.org/pipermail/tor-relays/2015-April/006804.html>) that he or she had been issued a subpoena (<http://www.scribd.com/doc/262490157/Alistar-Security-Subpoena-41715-1>) in order to track down a Tor user, despite the operator not being able to do that.

As well as running the exit remotely, another protective step for avoiding any hassle is to join an operator organisation, which is also recommended (<https://trac.torproject.org/projects/tor/wiki/doc/TorExitGuidelines>) by the Tor Project.

Moritz Bartl, who has maintained exits since 2006, heads an umbrella group that networks about a dozen different organisations (<https://www.torservers.net/partners.html>) that run exits. Called Torservers.net, the group deals with any abuse complaints that arise from the use of its members' exits, as well as reimbursing some operators with the cost of running them.

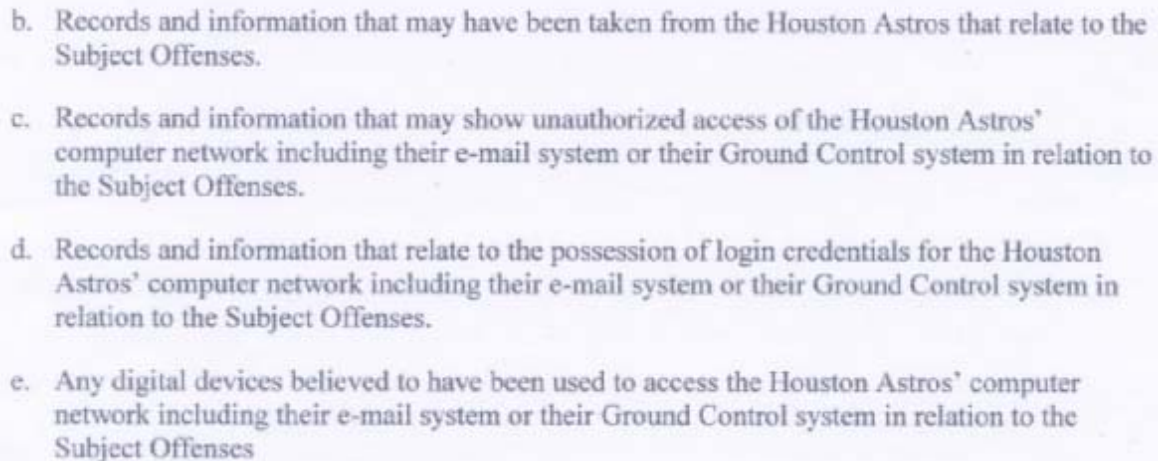
Most of the complaints that Bartl receives are to do with pirated content, and typically don't result in any raids or server seizures. Even then, Bartl said they don't receive that many.

"We get a police inquiry roughly every month," he said. "We just reply that we don't have any user data, and that we're legally not allowed to collect that kind of data, and even if we were, it wouldn't make sense technically."

But those who do get raided or otherwise harassed are the minority of Tor exit operators, and some feel the precarious situation around their work is exaggerated.

"In total, I've received around 50 DMCA infringement notices, 20 abuse complaints,

and zero visits from the feds,” Lewman from the Tor Project, using the pseudonym phobos, wrote in 2008 (<https://blog.torproject.org/blog/five-years-exit-node-operator>). “Sorry to disappoint you if you were expecting SWAT teams and black helicopters and mad car chases through the streets. Real life is much more boring.” Lewman no longer runs Tor exits.

- 
- b. Records and information that may have been taken from the Houston Astros that relate to the Subject Offenses.
 - c. Records and information that may show unauthorized access of the Houston Astros' computer network including their e-mail system or their Ground Control system in relation to the Subject Offenses.
 - d. Records and information that relate to the possession of login credentials for the Houston Astros' computer network including their e-mail system or their Ground Control system in relation to the Subject Offenses.
 - e. Any digital devices believed to have been used to access the Houston Astros' computer network including their e-mail system or their Ground Control system in relation to the Subject Offenses

A section of the search warrant obtained by Motherboard, showing that the FBI were investigating unauthorized access of the Houston Astros' computer network.

The FBI's questioning continued. The agents asked what interest Richard had in the Houston Astros, the baseball team? None, his wife replied. Richard didn't watch sports at all.

By this time, the sun had risen, although there was a cold bite in the air. Richard, still driving, received a second call from Lisa, who said the raid was something to do with the Astros. Specifically, the agents were looking for records of access into the Houston Astros' computer network, including their email system or their Ground Control system—an in-house database used to record baseball statistics (<http://www.fool.com/investing/general/2014/03/15/major-league-baseball-the-business-is-a-changin.aspx>)—as well as any login credentials, according to the search warrant.

The system administrator of the Houston Astros did not answer my questions concerning any hack of their systems, and directed me to the company's media representative, who also declined to comment.

Richard was still baffled. "I've never hacked a website in my life," he later told me.

When I asked Richard why he set up his exit, he said it could be summed up in one word: guilt.

"I've been increasingly concerned about surveillance for an entire decade, and then I got a job," he continued. "It turned out I was doing sub-contracting work for the NSA." Richard, being a contractual software engineer, had been working on secure satellite communications (http://www.drs.com/news/51111_2.aspx), he said.

That was three years ago, before Edward Snowden exposed various mass surveillance programmes being run by the NSA, as well as its Five Eyes counterparts in the UK, New Zealand, Canada, and Australia. In the years prior to Richard's decision to become an operator, it had already been revealed that the NSA maintained secret rooms (<http://arstechnica.com/uncategorized/2006/04/6585-2/>) in a number of AT&T facilities, and that George W. Bush had authorised a warrantless wiretapping program (<http://www.nytimes.com/2005/12/16/politics/16program.html?pagewanted=all>) in the wake of September 11. Richard has since left that NSA-affiliated position, and is currently working on a military project.

However, Richard emphasised that it was not the NSA in particular that pushed him over the edge. "I could just as easily have found myself in a job working for Google or some sort of data mining credit bureau, or some such thing," he told me. His decision was more in response to the growing trend of surveillance in general.

"I've long been concerned about it, and suddenly I realised I was part of the problem, and that it was good for me to take proactive steps to try to claw back some of the privacy that we've lost in recent years," he said.

White, the UK-based operator, had a different motivation for setting up his exit: he wanted to return the favor to the Tor network by running an exit.

"I have used Tor for a long time now, since 2008," he said. "I guess after years of using

it, finally contributing back to the network was something I am in a good position to do. Besides, we need people who act as the bedrock of the network, to not act in a malicious way and to protect the users of the network.”

Another operator I spoke to, who went under the pseudonym of “Kura,” rarely even uses Tor.

“I support the project in every way but, I myself don't use it that much,” Kura said over encrypted chat. “I am more concerned with providing nodes [so] that people who need them can use [them], than use them myself.”

"I'm allowing people to communicate ideas. And I don't feel I need to apologise for that"

After the FBI got what they wanted, they left the house and phoned Richard to ask him to come to a local field office for questioning.

Hidden behind a shopping mall, it looked just like a regular office building, Richard later told me, except it was “surrounded by iron bars and had a guard shack.”

After emptying his pockets and having his possessions X-rayed, Richard was led into a small room to be interviewed. The first agent was locally based, while the other was from the cybercrime unit in Houston, Richard told me.

“They were asking me why I was renting this server, and what my motivation was,” recalled Richard, who nervously answered the agents’ questions. “Why did I select Germany? Was it to evade law enforcement? I explained that bandwidth is so much cheaper in Europe.”

Richard rents the server for his exit in his own name and pays for it with his own bank account, he told me. A simple lookup of the IP address would reveal that it was a Tor exit node, he added.

Special Agent Joshua Phipps, the local Indianapolis agent who interviewed Richard, declined to provide comment for this piece. A media representative from his field office also declined to comment on whether investigating a Tor exit node operator has produced any fruitful results.

A spokesman for the local police department, which had officers on standby to assist the FBI, said that his force was not given any details on what the raid on Richard's house concerned.

"[The Houston agent] didn't seem very knowledgeable. He seemed more like a law enforcement guy that had been given some classes than a techie who developed an interest in law enforcement later," Richard said.

But Tor's Lewman said that the FBI in particular is very knowledgeable when it comes to the ins and outs of Tor.

"The FBI spend a lot of time reading through the source code, reading up on operations," Lewman told me. The Tor Project educate various law enforcement agencies (<https://blog.torproject.org/blog/trip-report-tor-trainings-dutch-and-belgian-police>) in what exactly Tor is, as well as how to use it themselves.

When I asked whether the sort of raids that Richard faced can be eliminated, Lewman said, "probably not." Sometimes "it is up to the individual department," on how they act against an operator, Lewman added, or they "do it on purpose, as in to make a show of force."

"Other times, the operators may not be [as] clean as they think they are," Lewman said, meaning that the operator may indeed be implicated in a crime.

Today, Richard's exit is still running; routing chats, photos, and, perhaps, more nefarious pieces of data from all over the world. "If ISIS videos are going across my exit node, I don't feel responsible for those murders," he said.

Opsahl from the EFF thinks this lack of accountability should also be reflected legally. "I think it's extraordinarily important for the functioning of the internet and for freedom of expression online, to allow service providers to operate without being held responsible for the acts of their users," Opsahl said. This could apply to internet service providers, hosting companies, or, indeed, Tor exit operators.

Richard, who is now awaiting a development in the case, is confident that nothing more will come of it, because of the public record of his IP address being a Tor exit node.

However, "it is traumatic to have an armed group of men show up at your house and start making threats," Richard told me. He does think that the FBI should investigate the owner of the server implicated in the hacking, but he doesn't agree with the raid on his home.

"What is unreasonable, is for them to show up in the pre-dawn hours, with bulletproof vests and waving firearms around, in the course of investigating a non-violent crime," he told me.

Since I spoke to Richard in March, he has not received any more visits from law enforcement. He also hasn't had his computers returned yet.

"I'm allowing people to communicate ideas," he said. "And I don't feel I need to apologise for that."

** Names have been changed. Richard did not want to become a target for people to focus their anger around child pornography, terrorism, or anything else that may be negatively associated with the use of Tor.*

--

TOPICS: The Operators (/tag/The+Operators), tor (/tag/tor), encryption (/tag/encryption), The Onion Router (/tag/The+Onion+Router), machines (/tag/machines), power (/tag/power), FBI (/tag/FBI), Internet (/tag/Internet), nodes (/tag/nodes), exit nodes (/tag/exit+nodes), Houston Astros (/tag/Houston+Astros), dark web (/tag/dark+web)

SHARE

1 COMMENT ([HTTP://MOTHERBOARD.VICE.COM/READ/THE-OPERATORS#DISQUS_THREAD](http://motherboard.vice.com/read/the-operators#disqus_thread)) FACEBOOK TWITTER GOOGLE PLUS TUMBLR REDDIT STUMBLEUPON

RECOMMENDED



After Hacks, A Dark Web Email Provider Says a Government Spied on Its Users (/read/after-hacks-a-dark-web-email-provider-says-a-government-spied-on-its-users?trk_source=recommended)

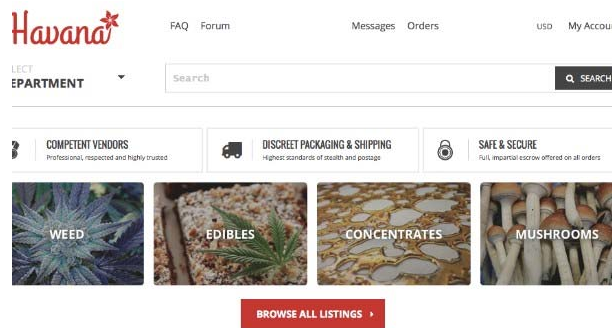
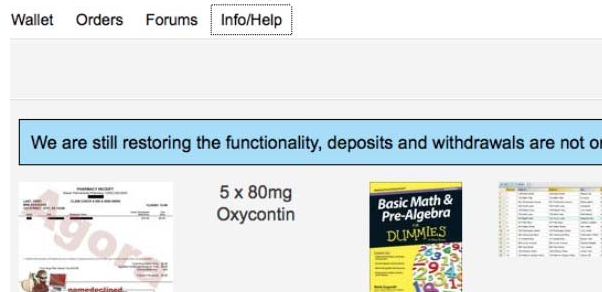
Small-Time Hackers Can Be Deanonymized Even When Using Tor (/read/even-tor-cant-save-small-time-hackers?trk_source=recommended)





The FBI Keeps Demanding Impossible Solutions to Its Encryption Problem (/read/the-fbi-keeps-demanding-impossible-solutions-to-its-encryption-problem?trk_source=recommended)

NASA IT Guy to White House: Please Don't Make Us Encrypt All Our Websites (/read/nasa-it-guy-to-white-house-please-dont-make-us-encrypt-all-our-websites?trk_source=recommended)



The Top Dark Web Drug Market Is Borked for 4/20 (/read/the-top-dark-web-drug-market-is-borked-for-420?trk_source=recommended)

The New Invite-Only Dark Web Market for All-Natural Drugs (/read/the-new-invite-only-dark-web-market-for-all-natural-drugs?trk_source=recommended)

COMMENTS

1 Comment motherboard.vice.com

1 Login ▾

♥ Recommend 2  Share

Sort by Best ▾



Join the discussion...



Sam E. Lawrence · 5 hours ago

Tor is the new printing press. Remember when they (the fearful, powerful few) used to smash those in underground print shops? Remember how they completely lost that war? Make sure to be on the right side of history, even if that's the wrong side of the law.

4 ^ | ▾ · Reply · Share ▸

© 2015 Vice Media LLC

[About](#) | [Contact](#) | [Privacy Policy](#) | [Terms of Use](#)

▪ print