



Dramatic Increase in Number of Tor Clients from Iran: Interview with Tor Project and the EFF

by Timothy M. O'Brien | @tobrien | +Timothy M. O'Brien | Comments: 2 | June 19, 2009

Anonymous proxies are in the news this week as Iranians are using proxies outside of Iran to communicate information about ongoing protests to others within the country. I've received several queries this week from non-technical colleagues about proxy servers. Is it legal to run a proxy server? Does running a proxy server violate my agreement with my broadband provider? I decided to track down some experts and get some perspective on different proxy servers and the laws surrounding them. In this entry, I speak with Andrew Lewman, the Executive Director of the [Tor Project](#) about Tor and I also get some legal guidance from Peter Eckersley of the [Electronic Frontier Foundation](#).

[Flash Player upgrade required](#)

You may also [download this file](#). Running time: 00:06:15

In this interview I ask Andrew to [briefly introduce Tor](#) and talk about some [interesting usage statistics that show adoption of this anti-surveillance technology from within Iran](#). He answers a question about [whether Tor is "unstoppable"](#) and comments on the [legality of running a Tor node](#). For the full interview, [listen here](#).

The Tor Project

First, what is Tor? From [The Tor Project](#):



“ Tor is free software and an open network that helps you defend against a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security known as traffic analysis.

Tor protects you by bouncing your communications around a distributed network of relays run by volunteers all around the world: it prevents somebody watching your Internet connection from learning what sites you visit, and it prevents the sites you visit from learning your physical location. Tor works with many of your existing applications, including web browsers, instant messaging clients, remote login, and other applications based on the TCP protocol.

When you run a Tor node, you are adding another node to a grid of computers that are used to establish random encrypted paths between each node to satisfy any given request. Law enforcement, military agencies, intelligence networks, journalists, and dissidents frequently use Tor to bypass restrictions and avoid surveillance. Andrew Lewman, Tor's Executive Director, wanted to be very clear that the Tor Project itself does not take positions on conflicts, and does not involve itself in resisting oppressive regimes. In response to a question about traffic from Iran, Andrew Lewman produced the following data:

“ New client connections from within Iran have increased nearly 10x over the past 5 days. Overall, Tor client usage seems to have increased 3x over the past 5 days. There are a lot of rough numbers in these statements, and they are very conservative. However, the source data we're reviewing continues to show these results.

For more information, see Andrew's blog post from last night: ["Measuring Tor and Iran"](#). Here's a graph from Andrew Lewman of Tor client count over the past few days, it appears that Tor is becoming an increasingly popular way for people in Iran to use the network to avoid surveillance.



But is it legal? The Legality of Running a Proxy Server

Peter Eckersley, Staff Technologist at the EFF, took some time to answer some very simple questions about EULAs, Tor, and the legality of running a proxy server.

Q: Various broadband providers state in EULAs that a customer must secure the equipment used to provide access to the Internet. What is the position of the EFF with regard to the legality of these EULAs? Are people breaking the law by providing an open access router?

Peter Eckersley: It's impossible to comment on broadband EULAs in general; each of them has different specific language and ISPs deploy them in different ways. We aren't aware of any case in which a broadband subscriber was sued for running an open wireless router, a proxy, or similar technology for sharing their connection with others.

Q: The last update to the Tor FAQ from the EFF on the Tor site was from 2005. Have there been any developments with the EFF in relation to Tor? Since 2005 is there more clarity as to the legality of running an Exit Node in a Tor network?

Peter Eckersley: The EFF Tor FAQ still reflects our opinions about the legality of Tor. It hasn't changed since 2005 because there haven't been any published cases or other events that have changed our views.

Q: What advice would the EFF have for anyone new to setting up a proxy server this week (as many have done to support protestors in Iran)? Is it legal? What issues do people need to be aware of?

Peter Eckersley: EFF's advice at this point is that people should consider setting up Tor bridge nodes or Tor routers instead of proxy servers. Several thousand new proxy servers have appeared in the past week, but we fear that unencrypted proxies leave Iranians vulnerable to surveillance and continued censorship by the Iranian government. SSL encrypted proxies are better in this respect, but they are harder to set up than Tor routers, and there are some reports that the Iranian government has succeeded in blocking access to at least some encrypted proxies.

Fixed Typo @ 3:23 PM Central Saturday: One of my questions for the EFF had a rather important typo – I had typed Iraq instead of Iran. Fixed.

tags: [encryption](#), [government](#), [privacy](#), [security](#)



Disqus seems to be taking longer than usual. [Reload?](#)

