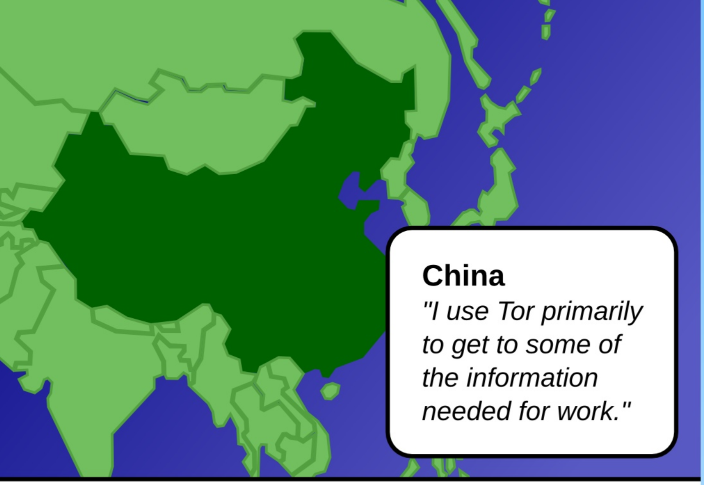
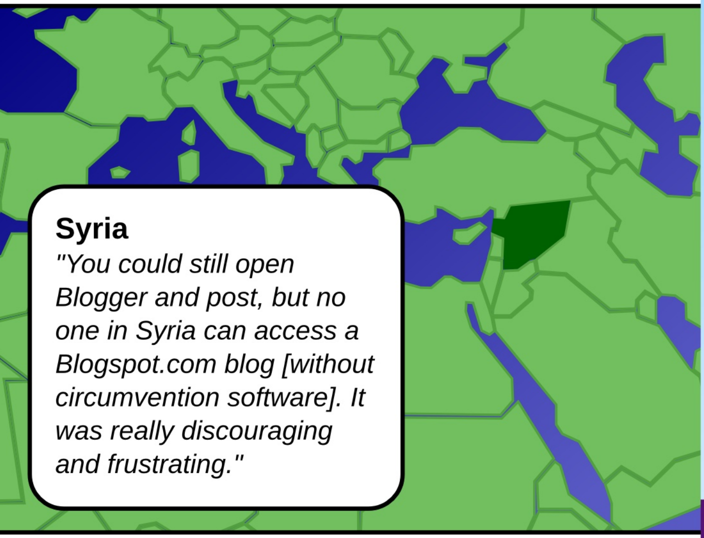
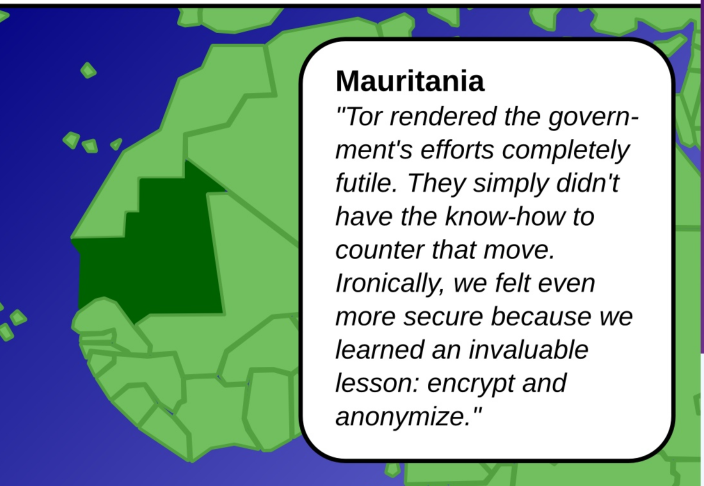


China
"I use Tor primarily to get to some of the information needed for work."



Syria
"You could still open Blogger and post, but no one in Syria can access a Blogspot.com blog [without circumvention software]. It was really discouraging and frustrating."



Mauritania
"Tor rendered the government's efforts completely futile. They simply didn't have the know-how to counter that move. Ironically, we felt even more secure because we learned an invaluable lesson: encrypt and anonymize."

TorProject.org

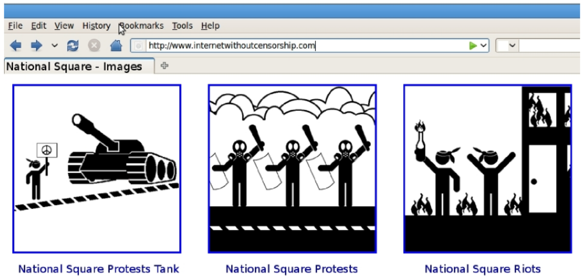
TorProject.org

969 Main Street, Suite 206
Walpole, MA 02081-2972 USA
https://www.torproject.org/

FREEDOM & PRIVACY ONLINE

Support Internet Freedom
Run a Tor Relay!

Internet censorship and monitoring are used by regimes across the globe. Some leaders think that their citizens cannot be trusted to determine which pages are appropriate to read. Some suppress dissent by rounding up bloggers, while many keep people from speaking out in the first place by making it known that the police are watching everyone. Others filter search results in order to rewrite history. For instance, this is what an image search for the scene of political unrest looks like on an uncensored connection:



http://www.internetwithoutcensorship.com

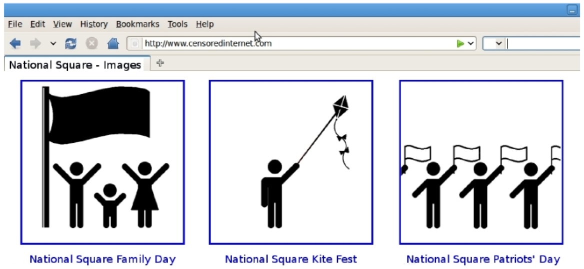
National Square - Images

National Square Protests Tank

National Square Protests

National Square Riots

When you add filtering, this is what the same search looks like:



http://www.censoredinternet.com

National Square - Images

National Square Family Day

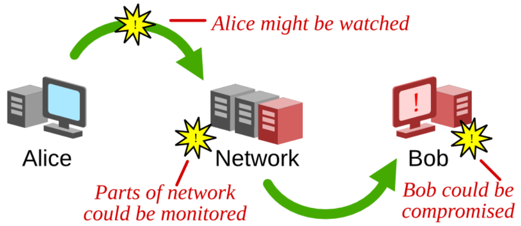
National Square Kite Fest

National Square Patriots' Day

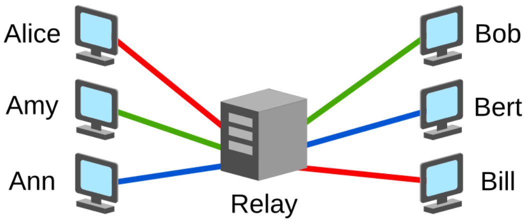
After a few years, it's almost as if nothing ever happened there. History is reduced to a rumor. In times of political unrest, journalists are deported, leaving reporting up to the citizens who use the internet to post videos and write to news organizations. Getting the news out ensures that the record of events can not be erased.

Tor allows people behind national firewalls to circumvent censorship and keep their governments from finding out what they are doing online.

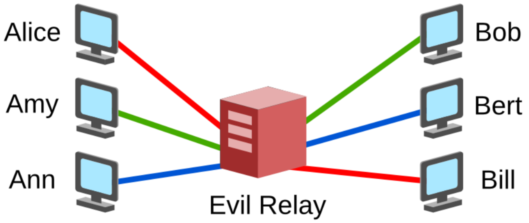
The internet usage of citizens can be controlled by governments in several ways. Alice can be watched as she connects to Bob, Bob can be watched, Bob can be working for the regime, or Alice can just be prevented from connecting to Bob's site.



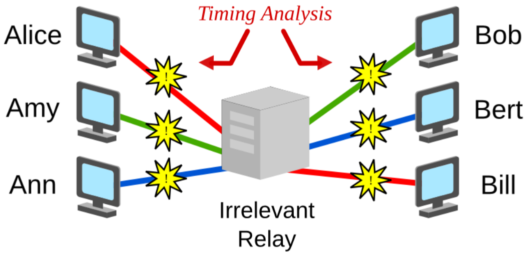
There are also several ways to get around restrictions. One, offered by some commercial proxy providers, is a single relay to hide connections. Here, Alice is connecting to Bill:



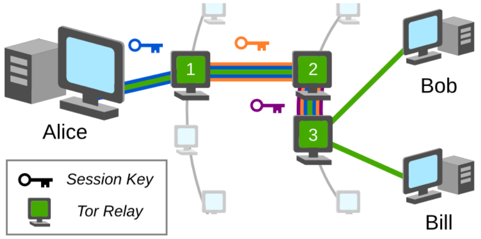
A single relay is a single point of failure, or it can be run by an eavesdropper. This is privacy by promise, and is only good as long as the proxy provider chooses not to reveal your information. Money can change hands, the relay can be hacked, or political pressure can lead to leaks.



If the proxy provider does not snoop, others can still get past a single relay. Timing analysis can still be used to bypass the relay and figure out what people are doing online.



Adding multiple relays means that no single relay can betray users. Tor's relays are run by volunteers across the world.



Alice makes a session key with the first relay, then tunnels to the second relay and then the third. No individual relay has all the information about Alice's activity online. This is privacy by design. A network cannot reveal information it did not gather in the first place.

Alice can still reveal too much information to Bill, Bob, or someone posing as friendly, but using Tor puts more control into her hands.

Our developers are working hard to make Tor safer and easier to use, but we need your help. To find out how, go to:

https://www.torproject.org