800 words

Rauf Bolden

July 27, 2017

Anonymous Web Browsing

Shopping on the Internet is your choice, protecting your family's and your company's data is your obligation, effectively using no-cost software for banking and credit-card purchases is a chance to do both.

Privacy's demise is on the horizon, requiring ordinary citizens to take precautions, protecting their personal information and their families from marketers and identity thieves. One way is with the Tor Browser, preventing people from learning your family's location or your browsing history.

Tor is the German word for gate. The Tor Network is comprised of gateways called nodes, routing your traffic through at least three-separate nodes. The entry node knows who you are but not where your site request is going, the middle node relays the information from the entry node to the exit node, the exit node knows where the site request is going but not who you are, according to Ermin Kreponic, IT Expert at Udemy.

"The Tor Browser is slower than a normal point-to-point browser and sites may not work as well because tracking scripts are blocked", said Kreponic, "but it hides your system IP (Internet Protocol Address) by creating layers, using an encrypted tunnel called a VPN (Virtual Private Network)".

You can find this free download at: https://www.torproject.org, making it very hard for a hacker to piece together your location or your browsing history, helping anonymize the trail of your family and your company on the Internet.

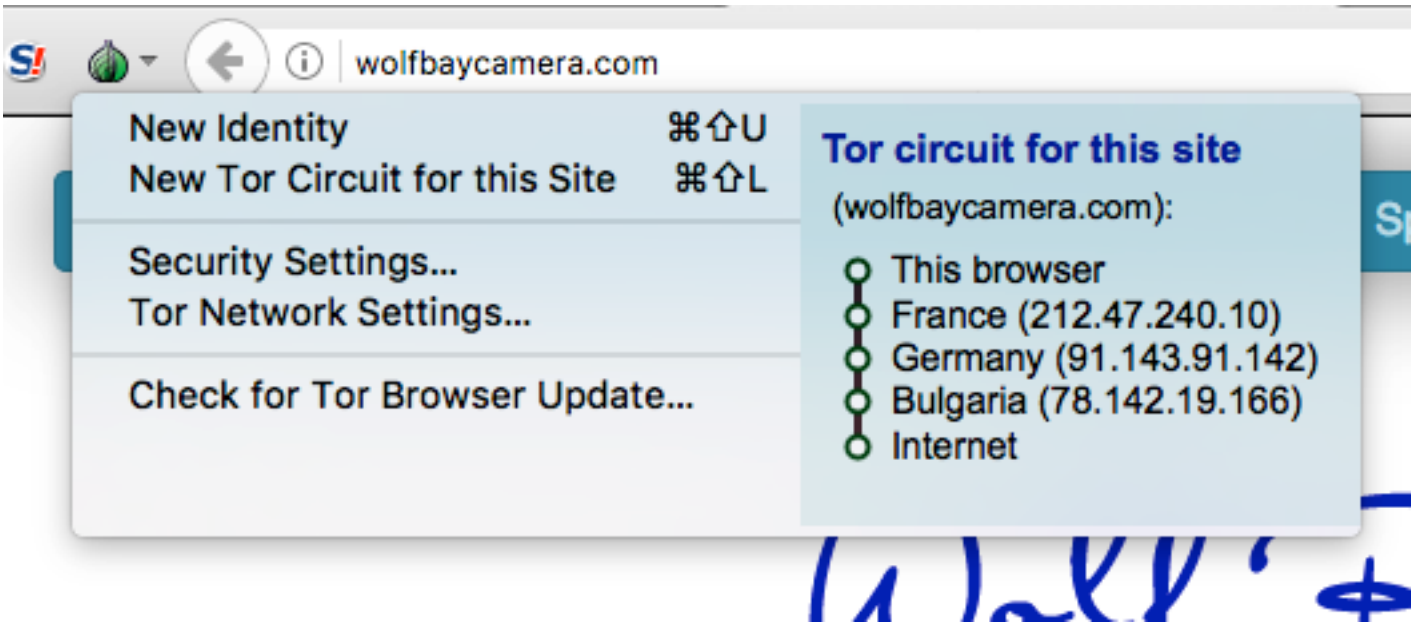
The early Internet was a source of information sharing between governments, growing to academic interactions between universities then private citizens, relying on self-restraint and respect for others to protect privacy. These rules were not enshrined in law. The ecosystem has evolved since then, sprawling across every jurisdiction on the planet, making it impossible to regulate, giving advertisers access to private information they can re-sell.

When you read a magazine at home you do not expect to see the same items pop-up on your phone, but when you shop online, the items you are interested in pop-up on your phone and other web pages. Some like this and some find it intrusive, basically Internet Service Providers (ISPs) can now sell your online data to search advertisers, providing a nice little revenue stream for them, taking the choice to opt-in away from the consumer.

Of course, making it more difficult for governments to track your Internet activity is your right as a citizen, but may raise more questions than it answers about what have you got to hide? Realistically, the option to protect your Internet location and your family's browsing history is your business, as much as it is your right to defend your home and bear

arms. Consider the Tor browser as an arm against invasion, because identity thieves can rob you from half-a-world away with no redress on your part.

The graphic below is an example of the multiple hops the Tor browser takes, masking your IP location and getting you to the Internet, going from Orange Beach to France to Germany to Bulgaria to the Internet, making it very difficult to track your family's or your company's browsing history.



In a world where we have a collective responsibility to keep each other safe from terrorism, submitting to voting-records collections and private-browsing inspections is arguably necessary, but I do not think we are there yet. I see ultra inspections by government as an intrusion not framed by the founders. No matter how altruistic the motives of government are in protecting us from terror, opening up our private data leads to exploitation by financial bandits, stealing identities with the government taking no responsibility for the personal pain this causes.

Some refute my opinion. On March 23, Congress passed a law dismantling Internet Privacy Rules (Senate Joint Resolution 34 (S.J.Res.34)). On April 3, President Trump quietly signed the bill into law, arguing privacy regulations are burdensome. ISPs are no longer required to get explicit permission before collecting-customer data and re-selling it.

"While everyone was focused on the latest headline crisis coming out of the White House, Congress was able to roll back privacy," said former Federal Communications Commission chairman Tom Wheeler.

So you see the time is upon us, forcing the rank-and-file to defend their privacy without built-in-protections from government. You have the choice of subscribing to a paid VPN service or using the free Tor Browser, doing nothing leaves your family, your company and you exposed.