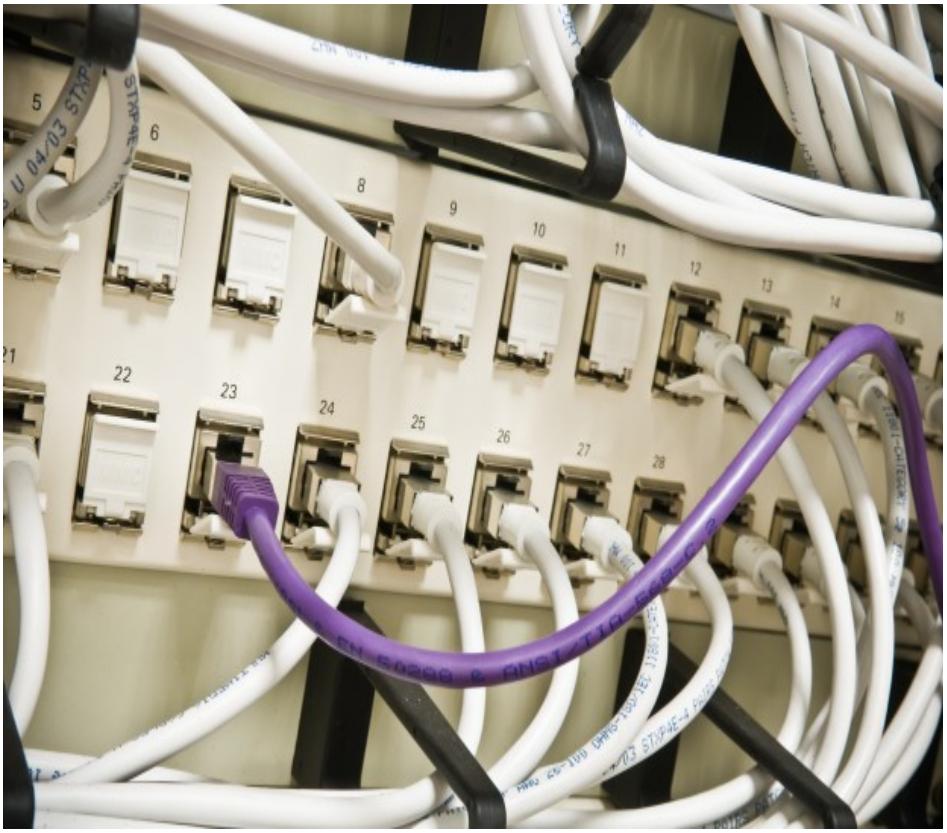
salon.com http://www.salon.com/2013/11/26/could_privacy_protecting_software_become_a_new_internet_standard_newscred/

TUESDAY, NOV 26, 2013 8:51 PM UTC

Could privacy-protecting software become a new Internet standard?

Software developers are rethinking how to protect users' locations and browsing

TECHNOLOGY



Following NSA surveillance revelations, talks advance on making the privacy-protecting tool Tor an Internet standard.

The Internet's main engineers have asked the architects of Tor—networking software designed to make Web browsing private—to consider turning the technology into an Internet standard.

If widely adopted, such a standard would make it easy to include the technology in consumer and business products ranging from routers to apps. This would, in turn, allow far more people to browse the Web without being identified by anyone who might be spying on Internet traffic.

If the discussions bear fruit, it could lead to the second major initiative of the Internet Engineering Task Force (IETF) in response to the mass surveillance by the National Security Administration. Already the IETF is working to encrypt more of the data that flows between your computer and the websites you visit (see "Engineers Plan a Fully Encrypted Internet").

Collaborating with Tor would add an additional layer of security and privacy. When Tor is successfully used, the websites you visit don't know the true address and location of your computer, and anyone watching traffic from your computer wouldn't know where you're browsing—a distinct layer of protection that goes beyond encrypting your communications.

Stephen Farrell, a computer scientist at Trinity College, Dublin, believes that forging Tor into a standard that interoperates with other parts of the Internet could be better than leaving Tor as a separate tool that requires people to take special action to implement. "I think there are benefits that might flow in both directions," he says. "I think other IETF participants could learn useful things about protocol design from the Tor people, who've faced interesting challenges that aren't often seen in practice. And the Tor people might well get interest and involvement from IETF folks who've got a lot of experience with large-scale systems."

Andrew Lewman, executive director of Tor, says the group is considering it. "We're basically at the stage of 'Do we even want to go on a date together?' It's not clear we are going to do it, but it's worth exploring to see what is involved. It adds legitimacy, it adds

validation of all the research we've done," he says. On the other hand, he adds: "The risks and concerns are that it would tie down developers in rehashing everything we've done, explaining why we made decisions we made. It also opens it up to being weakened," he says, because third-party companies implementing Tor could add their own changes.

The IETF is an informal organization of engineers that changes Internet code and operates by rough consensus. Internet service providers, companies, and websites aren't required to implement any standards the IETF issues. And even if security standards are implemented, they may not be widely deployed. For example, years ago the IETF created a standard for encrypting Web traffic between your computer and the websites you visit. Although this standard, HTTPS, is built into most software for serving Web pages and browsing the Web, only banks, e-commerce sites, and a number of big websites like Google and Facebook have elected to actually use it. The IETF hopes to make such encryption the default for a future Web communications standard known as HTTP 2.0.

The Tor Project is a nonprofit group that receives government and private funding to produce its software, which is used by law enforcement agencies, journalists, and criminals alike. The technology originally grew out of work by the U.S. Naval Research Laboratory aimed at protecting military users (see "Dissent Made Safer").

When someone installs Tor on his computer and takes other precautions, it supplies that computer with a directory of relays, or network points, whose owners have volunteered to handle Tor traffic. Tor then ensures that the user's traffic takes extra steps through the Internet. At each stop, the previous computer address and routing information get freshly encrypted, meaning the final destination sees only the address of the most recent relay, and none of the previous ones.

Leaks by Edward Snowden, a former NSA contractor, suggest that circumventing Tor was one of the NSA's goals, and that the agency had had some success (see "Anonymity Network Tor Needs a Tune-up to Protect Users from Surveillance"). "We are about 10 people, and have multibillion dollar agencies trying to break our technology," Lewman says.

View "Group Thinks Anonymity Should Be Baked Into the Internet Itself" and find more technology news from MIT Technology Review.

Technology
