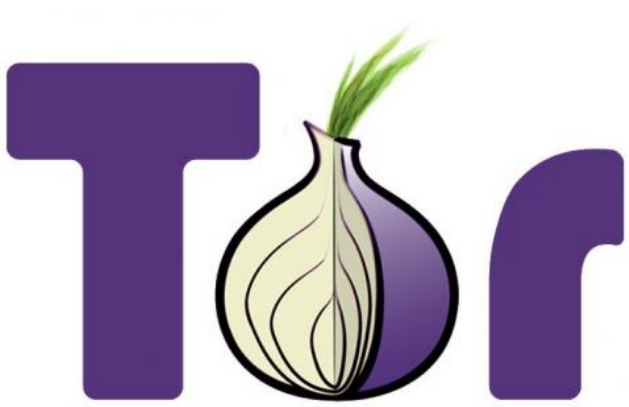
Judge's ruling confirms CMU engineers hacked TOR network

26 February 2016, by Bob Yirka



A recent ruling by U.S. District Court Judge Richard Jones reveals what many in the Internet business have known for some time—namely that the U.S. Department of Defense paid researchers at Carnegie Mellon University's Software Engineering Institute to look into ways of subverting the TOR network's ability to hide user IP addresses, and that the FBI subsequently forced SEI to hand over data (and possibly technical details) via subpoena, which led to the arrest of Brian Farrell, a man accused of using the TOR network to carry out a host of crimes anonymously.

The disclosure of the details that led to the arrest of Farrell, whose lawyer's are attempting to clear their client by suggesting that the actions taken by SEI and the FBI were illegal, opens up yet another can of worms regarding Internet privacy. News of this latest incident comes on the heels of the widely publicized case of the U.S. Government attempting to force Apple Computer to bypass the security codes on a phone used by one of the San Bernardino shooters last December. In this new case, the representatives of the TOR network argue that SEI engineers accessing their network and pulling out the IP address of one of its clients was not only illegal (which if true could spell legal trouble for the researchers at SEI) but immoral, as its network is used by more than just criminals trying to hide their activities—it is also used very heavily by dissidents in other countries, or people who are under other forms of duress. They claim their network helps undermine dictatorships and other authoritarian governments, which in turn, helps move the world towards freedom and tolerance.

Jones's ruling also sent shudders though the dark net, as he declared that users on the TOR network "clearly lack a reasonable expectation of privacy in their IP addresses.." because such users voluntarily give up their addresses to TOR operators in order to gain access to the network. That means that the FBI is free to use all the data it obtained from SEI to go after other TOR users, which could include people using the network to illegally download software, movies or music. And that is not the end of it—it is not clear just yet, but it appears that the FBI might have also obtained information, tools and/or software via their subpoena regarding the means by which the engineers at SEI hacked the TOR network, which means the FBI could use what SEI learned, to hack the TOR network, or others like it, on their own.