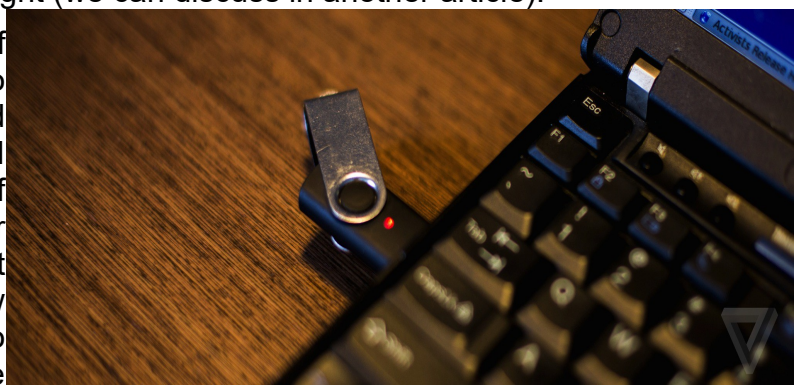
BIGGEST THREAT TO N.S.A.

Of course the biggest threat to the United States' National Security Agency (NSA) is privacy and secrecy; ironically, secrecy and privacy is the backbone of the NSA. It wants all the privacy and secrecy and it wants you to have none, as if it's a limited commodity or subject to regulation... as if!

The German weekly news magazine *Der Spiegel* published slides from an internal NSA presentation dating to June 2012 in which the NSA deemed “Tails” (The Amnesic Incognito Live System) on its own as a "major threat" to its mission, and when used in conjunction with other privacy tools was ranked as "catastrophic," leading to a "near-total loss/lack of insight to target communications, presence...". Yes! Read that again! Software can recover our privacy, and privacy is a property right (we can discuss in another article).



I recently called several of my congressman and spoke to interns who work in the offices and deliver messages to them. I explain that the recent efforts of the Congress to censor communication and conduct surveillance do not change the law requiring our government to protect free speech, but that we (people in general) were not really concerned with what Congress does to violate our privacy rights because we are using software and technology to recover and protect our rights. Basically, I told our members of congress that we can now ignore them and we will use technology (instead of “laws”) to protect our own privacy.

This is what you're getting with the PrivacyWorks anonymous USB. This is the most secure computer platform you can be using right now. In fact, it was used by Edward Snowden to maintain his privacy and security.

From the moment you boot up, your computer leaves footprints. websites leave tracking cookies, following you from page to page and session to session, alongside the usual traces left by your IP address. Persistent logins from Google and Facebook tie each site visit to your offline identity. If anyone really wants to go after you, they can also make a direct

John Jay Singleton, Aceofcoins.com, coins@aceofcoins.com
www.youtube.com/user/singletonpress; 352-342-1545
96 Kensington High Street, London

attack, targeting malware to track your movements in the background. With the right tools, a computer is an open book.

Not this computer platform (USB) though, it's running Tails, an open-source operating system designed to leave as little trace as possible. It's an amnesiac system, which means it's completely fresh every time you boot up. There are no saved files, no new programs, and most importantly, it becomes a blank slate the moment you shut down. It's the digital equivalent of using a brand new computer each time you boot up.

Even if the developers wanted to put in a backdoor, they couldn't. Over the previous five years, the code has been open for review at every stage, and after each release, auditors have found holes in its security, i.e., creative ways an attacker might circumvent the program. The holes are patched, then new holes are discovered, then those holes are patched, and this process has repeated more than thirty times. It's the nature of open-source development, a messy, public process that produces secure software through a slow grind of bug hunts. That parade of public security failings is meant to make users feel safe. If there's a problem in security at any level, you'll know about it, and the team will be under pressure to fix it as soon as possible. It's the same open workflow that built Tor and PGP, and stumbled more recently with the “Heartbleed bug”. But it means that even if the developers wanted to put in a backdoor, they couldn't. Now we have confirmation, an admission from the worst privacy violators on the planet, the NSA. The operating system and software suite on this USB is the biggest threat to the mission of the NSA to invade everyone's privacy. This is just one effective way to exclude yourself from the surveillance.

This USB gives you get an extreme level of anonymity. Keeping the operating system on a disk means you’re operating independent of the computer, picking nothing up and leaving nothing behind. It also makes your setup portable. You can launch Tails from an internet cafe and know that none of the programs on the public computer will get in the way of what you’re doing. It will even hide you within a local network, randomizing the computer’s “MAC” (Media Access Control) address to make you even harder to track. None of the methods are completely impenetrable, but together they add up to a major headache for anyone trying to follow you across the web.