# OTF – The "Independent" Internet Freedom Organization that Makes All Your Favorite Privacy Apps – Is Staffed Full of Spies

By Alan MacLeod
Global Research, December 10, 2021
MintPress News 6 December 2021

Region: USA
Theme: Intelligence, Police State & Civil Rights



***

*While the OTF presents itself as independent internet freedom activists, their funding, staff, history and choice of targets all point to the conclusion that they are a digital weapon being used against Washington's enemies.*

The Open Technology Fund (OTF) is one of the most influential and celebrated organizations in the hacking and internet freedom communities. Well over two billion people globally use OTF-produced software, including communications app Signal and web browser Tor, services that are specifically marketed to privacy-conscious consumers looking to circumvent government censorship and surveillance. Yet its close links to the U.S. national security state raise many worrying questions about whether the world is making a mistake by trusting the organization and its products.

Through its research and sponsorship, the OTF is responsible for apps and services that can boast a massive reach. It is estimated that more than two-thirds of all smartphones are equipped with OTF offerings, apps that brand themselves as the obvious choice for privacy-minded users.

The OTF describes itself as "an independent non-profit organization committed to advancing global Internet freedom," adding that it "supports projects focused on counteracting repressive censorship and surveillance, enabling citizens worldwide to exercise their fundamental human rights online."

There is strong evidence, however, to suggest that the Open Technology Fund is not what it claims to be: that it is neither independent nor truly committed to online freedom and privacy.

First, while technically a private company, it is directly funded and controlled by the United States Agency for Global Media (USAGM), a government body responsible for overseeing

U.S.-funded state media outlets overseas, including *Radio Free Europe/Radio Liberty*, *Voice of America* and *Radio* and *Televisión Martí*. The OTF derives essentially all of its funding from USAGM, which, in turn, receives money from Congress through the Department of State, Foreign Operations and Related programs ($808 million in 2019).

Secondly, until 2019, the OTF was officially a government project managed by the infamous *Radio Free Asia*. Together, *The New York Times* described these outlets as a "worldwide propaganda network built by the CIA." Even a brief look at their content suggests that this is essentially an accurate description, with USAGM brought into existence to manage CIA-created media outlets.

This alone would be enough to raise questions. However, the OTF's definition of freedom should sound even more alarm bells. In its most recently published annual report, it describes its mission as:

> …Advanc[ing] internet freedom in repressive environments by supporting the research, development, implementation, and maintenance of technologies that provide secure and uncensored access to USAGM content as well as the broader internet. This critical support helps to counter attempts by authoritarian governments to restrict freedom online.

Internet freedom, according to the OTF, is explicitly defined in relation to access to U.S. state propaganda arms. If individuals in a country have access to *Voice of America* and *Radio Free Asia*, then their internet is free. If not, they live in a totalitarian state. Internet freedom boils down to the freedom of the U.S. government to reach you. Any other understanding of the concept is, at best, an afterthought.

The report also states that the OTF exists primarily for two purposes:

(1) to "[p]rovide unrestricted access to the internet to individuals living in information-restrictive countries to help ensure they are able to safely access USAGM content," and

(2) to [p]rotect journalists, sources, and audiences from repressive surveillance and digital attacks to help ensure they are able to safely create and engage with USAGM content." This is unlikely to be the idea of freedom that many privacy-conscious users of Signal and Tor have in mind.

That this operation is pointed specifically at U.S. enemies is made clear on the fund's website, which states that "leading censors like China and Russia" are "exporting their censorship and surveillance tactics to like-minded regimes abroad," and that the OTF must "capitalize on its unique capability within the U.S. government to support internet freedom efforts," thereby positioning Washington as the unquestioned defender of liberty around the world.

Of course, China and Russia do indeed have very serious censorship concerns, but they are hardly alone in that regard. Thus, while the fund speaks in the language of privacy and social justice, its targets are overwhelmingly U.S. enemy states. Meanwhile American allies with equally poor or worse free speech environments (such as Saudi Arabia or Qatar) are quietly overlooked.

A board of state functionaries

Not only was the Open Technology Foundation created by the national security state, it continues to employ high government officials in key positions. Its five-person board consists entirely of important state functionaries:

- Karen Kornbluh was formerly U.S. ambassador to the OECD, Barack Obama's policy director, deputy chief of staff at the Treasury Department, and a senior figure at the FCC during the Clinton administration.
- Ben Scott was previously policy adviser for innovation at the Department of State, where, in the OTF's words, he crafted the government's 21st Century Statecraft agenda.
- Top Democratic fundraiser Michael Kemper served as the DNC's deputy finance chairman as well as deputy finance coordinator for President Obama. He also held a position on the White House Council for Community Solutions from 2010 to 2012.
- William Schneider is a Republican who was Ronald Reagan's under secretary of state for Security Assistance, Science and Technology. He is also a member of the notorious neoconservative group, the Project for a New American Century. In 1998, he signed a letter to President Bill Clinton, urging him to attack Iraq. A science expert, he has consistently argued that the U.S. should use nuclear weapons as a standard part of its warfare.
- Even more central to the post-9/11 wars, however, is the fifth member of the board, Ryan Crocker. Crocker was United States ambassador to both Iraq (2007-2009) and Afghanistan (2011-2012). So important was he to the occupations that General David Petraeus, supreme commander of the occupation forces, said that he was merely Crocker's "military wingman." George W. Bush described him as "America's Lawrence of Arabia."

For such a group of individuals, who have spent their lives dedicated to enhancing U.S. state power, it appears unlikely that freedom from state surveillance would be high on their list of priorities. Underlining that the Open Technology Fund's concern with privacy and freedom of speech goes only so far is its choice of CEOs, who have included the former director of programming for *Voice of America*, the former president of *Radio Free Asia*, and an ex-State Department and National Endowment for Democracy official.

Thus the OTF – a "private" company that was created by government agencies and was a government body itself until 2019 – is staffed by top U.S. officials who have been chosen by the USAGM. The veneer of independence actually serves two important purposes: it provides the U.S. government a modicum of plausible deniability if any misdeeds are exposed and ensures that the organization is not subject to Freedom of Information Act requests, making the OTF far harder to scrutinize.

This semi-privatization technique is a new trend in U.S. statecraft. In recent years, the government has farmed out much of its most controversial clandestine work to NGOs and shadowy "private" companies that rely largely or solely on federal contracts. For example, NGOs like Creative Associates International have been employed to organize regime-change ops in Cuba or act as a front group for the CIA in Pakistan. Last year, a private American security firm was also responsible for a failed coup attempt in Venezuela.

OTF genesis

*Radio Free Asia* — the Open Technology Fund's former parent organization — was established by the CIA in 1951, in the wake of the American retreat from China. Between 1945 and 1949, the United States occupied mainland China in an attempt to support the nationalist Kuomintang forces and prevent Communist forces under Mao Zedong from coming to power. In this, they failed, and the Kuomintang fled to the island of Taiwan, just off China's coast. The powerful U.S. Navy prevented the Communists from pursuing them, allowing the Kuomintang to establish a one-party state on the island. This remains the basis of the current U.S.-China-Taiwan dispute.

During the 1950s, *Radio Free Asia* bombarded the mainland with anti-Communist propaganda in an attempt to weaken and, ultimately, unseat the Communist Party. However, results were poor and the project was put on ice, returning only in the 1990s after the fall of the Soviet Union, when U.S. planners began to believe a total eradication of communist states was possible.

Yasha Levine, an investigative journalist and author of "Surveillance Valley: The Secret Military History of the Internet," explained to *MintPress* that Beijing began blocking *Radio Free Asia*'s website almost as soon as it was launched in 1996. Consequently, its bosses began searching for a way of circumventing the Great Firewall of China. It was out of this project that the Open Technology Fund was born.

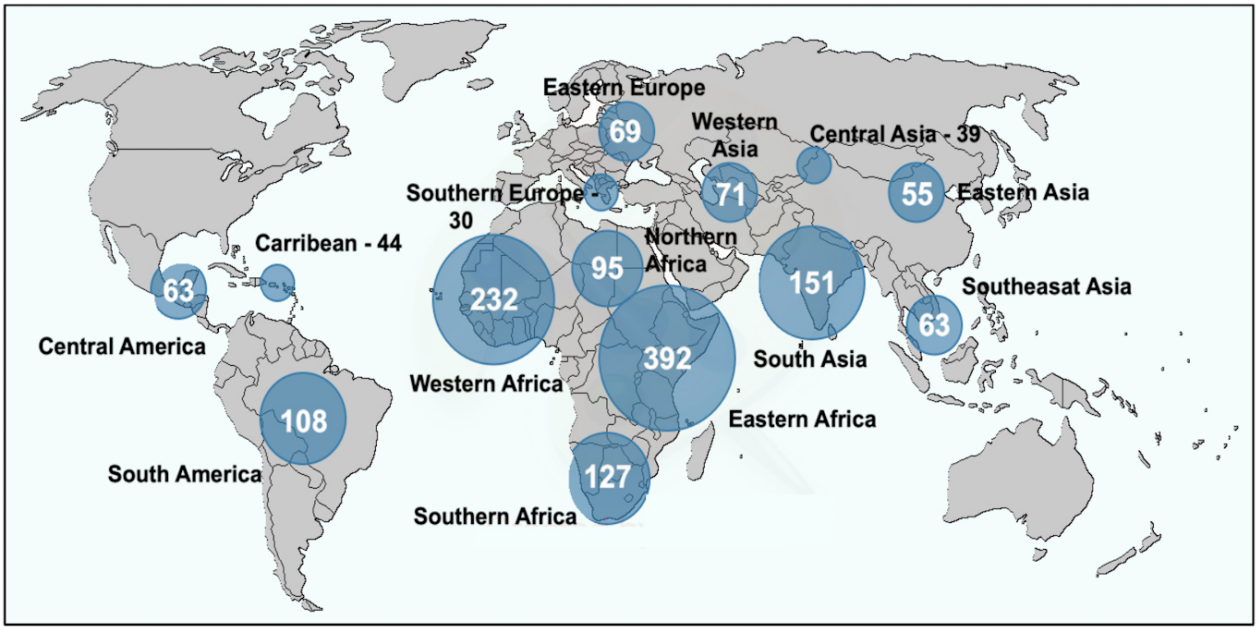
OTF's role in US-backed "pro-democracy" protests

The OTF has played a key role in U.S.-backed protest movements around the world. During the 2019-2020 Hong Kong protests, it was quietly channeling millions of dollars to protest leaders in an attempt to keep them going. It was also carrying out large-scale data-gathering operations on Chinese social media platforms Weibo and Wechat. CIA cutout organization the National Endowment for Democracy (NED) was engaged in similar activities.

For months, the Hong Kong protests dominated Western news media, with wall-to-wall positive coverage of the events. Yet locals themselves appeared to be far more split on the action. A poll conducted by *Reuters* showed that, by August 2020, only 44% of Hong Kongers supported the protest movement.

The Open Technology Fund has also been crucial to Washington's activities in Cuba. There, it sponsored the development of Psiphon, an open-source tool that allows users to hide their identity and bypass government restrictions.

The NED had, for years, been spending big to build and train a network of activists across the island. When the time came, they were ready. "During the protest in July, Psiphon enabled over 2.8 million users to connect to the uncensored internet, allowing them to share their stories on social media and messaging apps," boasted the company's CEO, Michael Hull. "Giving [Cubans] those tools so they can talk to each other is the most important thing that we can do," a senior Biden administration official told *McClatchy*'s D.C. Bureau. "We're looking to further expand our support for the Open Technology Fund and those sorts of [operations]," they added. As with Hong Kong, worldwide media coverage of the Cuban protests was intense. Yet the demonstrations fell apart even quicker, as few Cubans had an appetite for regime change.




A map from a 2018 OTF report shows regions where so-called "Internet freedom communities" have applied for OTF assistance

The OTF is also known to have supported similar recent actions in Belarus, Iran and Venezuela. In Belarus, it trained the opposition to President Alexander Lukashenko, its agents carrying out ten separate tours of the country, holding meetings with representatives of what it deemed "independent mass media, human rights defenders and civil activists." In total, it conducted at least 225 consultations with Belarussian groups in 16 months during 2017 and 2018 alone. They also provided training sessions for these activists. Sure enough, widespread demonstrations followed, with the goal of removing Lukashenko. The leaders of the movement were "installed and maintained" by the OTF, according to *The Guardian*.

While these operations are couched in the language of promoting democracy, it is clear at whom the OTF aims its tools. In its latest published yearly report, for example, the words "China" or "Chinese" appear 81 times, "Russia" or "Russian" 27 times, "Iran" 24 times and "Venezuela" 13 times. Yet Bahrain, Saudi Arabia and Qatar — three U.S. allies with particularly egregious media freedom records — are mentioned only once, in passing.

"An anarchist Lockheed Martin"

This long and sordid history certainly raises questions about the legitimacy and safety of the OTF's two most popular products, Signal and Tor. Between 2013 and 2016, the OTF channeled more than $3 million to Signal, while it gave twice that amount — more than $6 million — to Tor between 2012 and 2020. (Tor continues to be sponsored by a number of U.S. government agencies).

Certainly, all parties involved keep this information quiet. There is no mention of the OTF on Signal's website. Meanwhile, reading the three organizations' Wikipedia pages would barely clue an individual in on their connections. This is not a coincidence. Emails Levine obtained under the Freedom of Information Act show that Tor Project director and co-founder Roger Dingledine (who once interned at the NSA) was acutely aware of how bad the optics were.

“We also need to think about a strategy for how to spin this move in terms of Tor’s overall direction. I would guess that we don’t want to loudly declare war on China, since this only harms our goals?” he wrote to the director of OTF parent company USAGM. “But we also don’t want to hide the existence of funding from [USAGM], since ‘they’re getting paid off by the feds and they didn’t tell anyone’ sounds like a bad *Slashdot* title for a security project. Is it sufficient just to always talk about Iran, or is that not subtle enough?”

The wording of this email suggests Dingledine views Tor as a U.S. government weapon aimed at its enemies, and not as a neutral and independent privacy project, but was searching for a way to present it as such. The director of USAGM reassured him, responding that his organization would, “do any spin you want to do to help preserve the independence of Tor.”

Levine was highly critical of Tor’s role in society. “Tor is a military contractor that makes software for the U.S. government. They’re an anarchist Lockheed Martin; they give the U.S. government offensive capability on the internet. Of course, they are not making missiles, but they are making cyber weapons for Washington,” he told *MintPress*.

American agents use the browser to communicate. Ironically, the influx of new users actually helps them disappear into the crowd. Without the hackers, drug dealers, cyberpunks, crypto-enthusiasts, political activists and privacy-minded individuals using it, the identities and locations of U.S. agents would become obvious to foreign states monitoring online activities. In other words, when you use Tor, you’re helping the CIA.

Does Tor or Signal’s proximity to American intelligence mean that their products are fundamentally compromised? Enthusiasts point to their checkable, open source code as proof that they are secure. Even Levine does not challenge this. However, the enormous complexity of the operating systems they run on is a serious cause for concern. While many have checked Tor and Signal’s source code, few except state actors pore over the countless billions of lines of code of the software on our phones or computers — and they are doing it to find ways to exploit or attack the millions of holes and backdoors in the operating systems. Big governments can ultimately find a way to get to the data before it is encrypted, Levine argued, meaning that:

> Signal and Tor offer a false sense of security. It depends who you are trying to hide from. If it is your local police department and you are using Signal, it is probably good enough. But if you are engaged in some kind of political protest building, organizing and challenging state power on some level, I would not be dependent on Signal to do it.”

Since at least 2014, the FBI has been closely monitoring Tor, assessing users’ exit nodes (the false IP address that a server sees). Independent tests conducted by Columbia University found that researchers were able to identify over 81% of Tor users in real-world tests.

Ultimately, then, Signal and Tor could be compared to an expensive home security system. The product might be high quality and secure enough to stop petty thieves or even committed professional burglars. But if the FBI wants to enter your house, they will simply ram the door down. “On a fundamental level, I don’t think that privacy exists,” Levine said. “To think that, as a regular consumer, you can take on the state with some app that you download for free… It’s just ridiculous. It’s a joke.”

A dubious endorsement

Unfortunately, both Signal and Tor have developed large and devoted followings, being used the world over and endorsed by groups like the Electronic Frontier Foundation (EFF) and high profile privacy advocates. “The problem with Signal is not the technology, it is the marketing behind it. It has this *cachet* of being radical anarchist software that is backed by people like Edward Snowden. It has cultural capital,” Levine told *MintPress*; “They have created a cult of security around this app that does not exist. Not just for Signal, but for any other app.”

Perhaps more worryingly, the Electronic Frontier Foundation has also heartily endorsed the OTF, stating that the organization has “earned trust over the years through its open source ethos, transparency, and a commitment to independence from its funder, USAGAM.” “OTF’s funding is focused on tools to help individuals living under repressive governments,” EFF adds.

Unfortunately, the EFF is fundamentally intertwined with the national security state itself, with several of its staff serving on the OTF advisory council. In the 1990s, the EFF collaborated with the FBI to pass the so-called “Let’s Just Wiretap Everyone Bill,” rewriting the bureau’s draft legislation to make it sound more palatable to the public. That bill became the basis for a great deal of the FBI’s continuing invasive online surveillance. The OTF has also sponsored a number of EFF projects. *MintPress* contacted the EFF for comment, but did not receive a reply.

A concealed weapon in the global cyberwar

While at face value Tor and Signal may be robust, the fact that significant parts of the internet freedom and anti-surveillance movement are intertwined with the U.S. national security state does seem an absurd contradiction. The NSA lied for years, even under oath, that it was not spying on Americans. In reality, it was collecting reams of data on just about everyone. The U.S. was even intimately surveilling its closest international allies, such as German chancellor Angela Merkel. Given such a history, what could possibly be done to assuage fears that a similar operation is not currently being executed?

While the OTF presents itself as independent internet freedom activists, their funding, staff, history and choice of targets all point to the conclusion that they are a digital weapon being used against Washington’s enemies.

Thus, their talk of “freedom of information” is reminiscent of discussions about “free markets.” Freedom of information is currently being championed by the government that dominates and controls the internet and is in a position to use that leverage to carry out its international ambitions. And while the U.S. talks piously about freedom of information, whenever foreign-owned communications companies begin to succeed — such as Chinese-owned Huawei or TikTok — there is a meltdown, followed by an all-out attack from Washington, which fears they will be weaponized in similar ways Washington has weaponized Silicon Valley.

A silent war is being waged for control of cyberspace. And in war, truth is always the first casualty.

*

Note to readers: Please click the share buttons above or below. Follow us on Instagram, @crg_globalresearch. Forward this article to your email lists. Crosspost on your blog site, internet forums. etc.

*Alan MacLeod is Senior Staff Writer for MintPress News. After completing his PhD in 2017 he published two books: Bad News From Venezuela: Twenty Years of Fake News and Misreporting and Propaganda in the Information Age: Still Manufacturing Consent, as well as a number of academic articles. He has also contributed to FAIR.org, The Guardian, Salon, The Grayzone, Jacobin Magazine, and Common Dreams.*

*He is a frequent contributor to Global Research*

*Featured image is from Countercurrents*



---

**Comment on Global Research Articles on our Facebook page**

**Become a Member of Global Research**

*Articles by:* Alan MacLeod