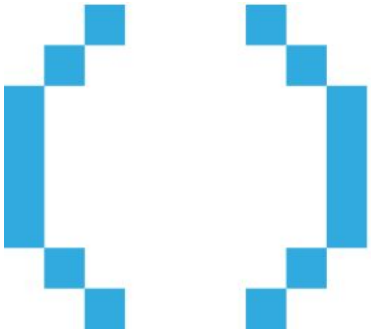


OPEN TECHNOLOGY FUND

2016 Annual Report

Open Technology Fund

The Open Technology Fund (OTF) is a global internet freedom program working to advance the free flow of information online in the world's most closed, repressive places. In an effort to promote open societies and human rights, OTF supports open technologies and communities that increase free expression, circumvent censorship, and obstruct repressive surveillance. A program of Radio Free Asia (RFA), OTF is funded by an annual grant from the Broadcasting Board of Governors (BBG).

Every project or person that OTF supports is working to achieve a primary outcome that fits within one or more of the following focus areas and objectives:

Focus Areas:

- ***Access*** to the internet, including tools to circumvent website blocks, connection blackouts, and widespread censorship;
- ***Awareness*** of access, privacy, or security threats and protective measures, including how-to guides, instructional apps, data collection platforms, and other efforts that increase the efficacy of internet freedom tools;
- ***Privacy*** enhancement, including the ability to be free from repressive observation and the option to be anonymous when accessing the internet;
- ***Security*** from danger or threats when accessing the internet, including encryption tools.

Objectives:

- Advance ***research*** about repressive internet interference in modern communication networks and the methodologies and technologies to best circumvent it;
- Foster ***development*** of technologies that circumvent repressive censorship and surveillance or increase communication access and safety; and
- Enable widespread ***implementation*** of solutions in an effort to free people from repressive internet interference.

Table of Contents

Executive Summary

The Open Technology Fund's ("OTF") fifth year of operation saw a staggering increase in the adoption of OTF-incubated technologies by internet users around the world.[1] 2016 began with over a billion people already utilizing OTF-supported technologies, but ended with nearly two billion doing so. Given the rapid, global expansion of everyday digital usage, the Broadcasting Board of Governor's ability to "Inform, Engage and Connect" people around the world in support of freedom and democracy is dependent on their ability to have unrestricted access to a free and open internet. OTF received more support requests in 2016 than in any prior year of operation. As such, OTF support significantly increased global internet freedom, as measured by the number of people able to experience a more open, secure internet, and by advancing the usability and effectiveness of emerging technologies and techniques. OTF-supported projects accomplished this in the face of increasingly sophisticated online censorship.

Internet freedom declined globally for the sixth consecutive year in 2016.[2] This continued backslide manifested itself in various forms, including a rise in internet shutdowns, increasingly repressive censorship and surveillance, and curtailed use of communication apps. The global community of internet-connected citizens continues to be hamstrung by government-imposed limits on internet accessibility, user privacy, and the ability to engage in online spaces in a free and secure manner. Despite these formidable challenges, the internet freedom community, including projects and individuals supported by OTF, made strides this year to combat repressive internet censorship worldwide.

OTF-supported projects work to ensure a resilient and open internet by identifying and addressing emerging threats to internet freedom, exposing platform based censorship, mitigating the use of social media sock-puppets, and hardening key technologies to protect people from digital attacks. OTF prioritizes increasing the accessibility of U.S. government internet freedom funds by removing unnecessary barriers to entry, directly engaging with emerging talent and those already carrying out the work, and building internet freedom capacity. As a result, in 2016, the OTF team reviewed and responded to nearly 700 funding requests totaling over $85 million, and spent 85 percent of the program's $7.5 million budget to support over 100 projects.[3]

In doing so, the OTF team listened to the field and global communities most at-risk, leveraging their collective knowledge and capacity to continually update OTF's program to better address evolving forms of censorship and surveillance. OTF Labs adapted to dynamic online freedom threats experienced in closed societies throughout the year.[4] And OTF's fellowship programs maintained a focus on the hyper-local needs of communities under threat, harnessing their collective knowledge and capacity, and promoting analysis and applied research in collaboration with the internet freedom community.

Pursuant to OTF's congressional mandate, the program continued to leverage government funds in order to benefit the greater global internet freedom effort. OTF proactively worked with funding sources outside of the U.S. government to unlock millions of dollars to support Internet freedom either directly or through joint funding on OTF projects.[5]

[1] This annual report covers the expenditure of OTF's FY2016 funds. These activities occurred from Spring 2016 until Winter 2017.
[2] Freedom House, "Freedom on the Net 2016," *Freedom House*, https://freedomhouse.org/report/freedom-net/freedom-net-2016.
[3] This figure encompasses all directly funded projects, including general internet freedom projects, all fellowships, and rapid response support, as well as indirectly supported projects through OTF Labs.
[4] OTF Labs are in-kind, technical assistance programs.
[5] Consolidated Appropriations Act, 2017, P.L. 115-31, p. 579, Global internet freedom Sec. 7078. (a), https://www.congress.gov/bill/115th-congress/house-bill/244/text "That funds made available pursuant to this section shall be matched, to the maximum extent practicable, by sources other than the United States Government, including from the private sector."

Challenges to Internet Freedom in 2016

By the end of 2016, nearly half of the world's population was online.[6] The past decade's connectivity boom has enabled unprecedented free-flowing communications, shifted societies, altered lifestyles, and boosted economies. Increased knowledge among internet adopters has created a platform for people to speak, learn, educate, and find community. As a 2016 UN agency report found, "many people no longer *go* online, they *are* online."[7] For connected populations worldwide, the internet has served as an invaluable source of news, information, and communication. The internet's knowledge-sharing platform has been quickly embraced and integrated into the heart of societal functions around the globe. In short, the internet has become an essential building block of human civilization.

But in some countries, this increase in connectivity has been hampered by authoritarian governments seeking to weaken or eliminate the internet's potential to be an open, secure, and global medium for communication. Rather than seeking to embrace an open internet, repressive states have sought instead to close off their societies and pull the plug on access to non-state controlled media, timely news, and freedom of expression. Global internet freedom declined for the sixth year in a row in 2016.[8] Around the world, people were routinely denied the ability to express themselves freely, access uncensored media and unbiased information, or network online with like-minded peers . These netizens often faced harassment, intimidation, and harsher forms of offline reprisal for their actions online.

Only a third of all internet users live in places where voicing online opposition to state institutions is not subject to censorship.[9] Consistent with the broader worldwide crackdown on freedom of expression, essential civilian institutions like the press also faced significant challenges in 2016. At least 48 journalists and nine netizens were killed for their work,[10] as press freedom declined globally to a 13-year low.[11] In total, 67 countries saw downturns in overall political and civil rights.[12] Given how connected the world has become, these issues inevitably play out in online contexts as the internet is fast becoming the primary medium by which people communicate, share information, and learn about the world around them.

Trending Threats: Shutdowns, Censorship, Harassment, and Collusion

Internet Shutdowns

Authoritarian governments around the world have increasingly utilized internet shutdowns as a way to restrict access to information and silence free expression online. This approach has become especially prevalent during times perceived by authorities to be politically volatile, such as during elections (a common trend in Africa in 2016)[13] or in response to protests (as happened in countries like Bahrain, Ethiopia, Zimbabwe, and Gabon in 2016). Internet shutdowns come in a variety of forms - from the strategic blocking of certain apps and websites, to widespread, blanket blackouts. They can last for hours, days, weeks, or even months.

---

[6] This figure has been steadily and sharply increasing over the past decade. International Telecommunication Union, "Measuring the Information Society Report," *International Telecommunication Union*, Chart 6.6, p. 187, 2016, http://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2016/MISR2016-w4.pdf.
[7] *Ibid,* p. 209.
[8] Freedom House, "Freedom on the Net 2016," *Freedom House*, https://freedomhouse.org/report/freedom-net/freedom-net-2016.
[9] *Ibid.*
[10] *See* Committee to Protect Journalists, "48 Journalists Killed in 2016/Motive Confirmed," *Committee to Protect Journalists*, https://cpj.org/killed/2016/; Reporters Without Borders, "Violations of press freedom barometer," *Reporters Without Borders*, https://rsf.org/en/barometer?year=2016.
[11] Freedom House, "Freedom on the Net 2017," *Freedom House*, https://freedomhouse.org/report/freedom-press/freedom-press-2017.
[12] *Ibid*.
[13] Hilary Matfess, "More African countries are blocking internet access during elections," *Quartz*, June 1, 2016, https://qz.com/696552/more-african-countries-are-blocking-internet-access-during-elections.

Governments imposing shutdowns have sought to justify their actions through a wide array of premises, at times veering on the absurd. An election-time shutdown in Uganda was said to combat the spread of "misinformation";[14] an internet-wide shutdown in Bangladesh was claimed to be conducted as part of an "Internet shutdown drill";[15] and a massive communications blackout in the Republic of Congo was allegedly meant to preempt any "illegal" election reporting.[16] Similarly, the Ethiopian and Iraqi governments have shut down their countries' internet over a dozen times in purported attempts to prevent students from cheating on school exams.[17]

> **"Social media is a lifestyle, you can't just switch it off and on. It's a priority to a lot of our lives and we have to live on even as we are in the electoral process. We have to keep in touch with our businesses, our friends and family."**[18]
>
> \- Uganda-based photographer Daniel Gilbert Bwete

In response to this rise in state-facilitated internet disruptions, the UN Human Rights Council passed a consensus resolution condemning "measures to intentionally prevent or disrupt access to or dissemination of information online."[19] Though non-binding, the UN resolution makes clear the Human Rights Council considers such internet blockages to be an issue that transcends the digital realm, connecting the "human rights violations and abuses" including violence and harassment that have been "committed against persons for exercising their human rights and fundamental freedoms on the Internet[.]" The resolution called "on all States to refrain from and cease such [blocking] measures," and reaffirmed the internet as a medium to facilitate the exercise of basic human rights.

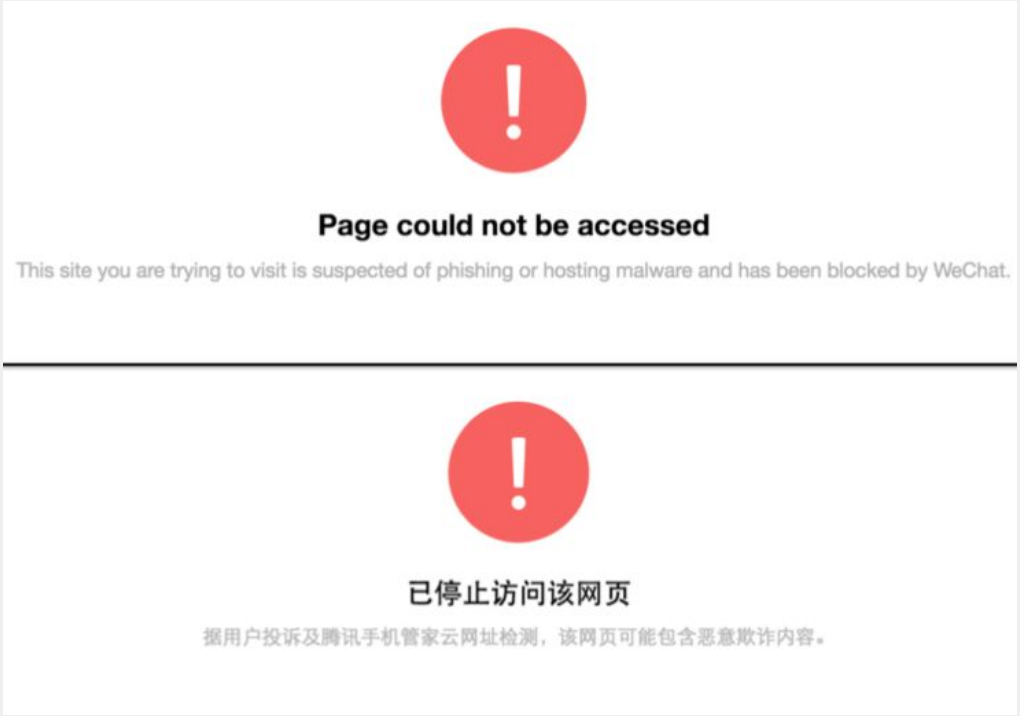
Beyond violating individual user rights, government leaders who choose to restrict internet access are also causing immense collateral damage to their country's economies, given the internet's function as a hub for commercial transactions. In an examination of 81 internet shutdowns between 2015 and 2016, a Brookings Institute study estimated shutdowns to have resulted in the loss of at least $2.4 billion in GDP.[20]

Censorship of Social and Alternative Media

Social media and communication platforms are common targets of censorship for authoritarian states looking to restrict the free flow of information and free expression online. These digital platforms pose a threat to authoritarian governments because of their ability to provoke discussion, foster knowledge-sharing, and spread alternative views. This type of censorship is implemented in a variety of ways, including blocking a website's accessibility or cracking down on free expression exercised on such mediums. Authoritarian states, however, are not afraid to utilize such platforms to advance their own interests. In what appeared to be a highly

[14] G.S. Phillips and Grace Atuhaire, "How Ugandans Overturned An Election Day Social Media Blackout," *Motherboard*, February 24, 2016, https://motherboard.vice.com/en_us/article/uganda-election-day-social-media-blackout-backlash-mobile-payments.
[15] Zara Rahman, "Bangladesh Shuts Down the Internet, Then Orders Blocking of 35 News Websites," *Global Voices Advocacy*, August 4, 2016, https://advox.globalvoices.org/2016/08/05/bangladesh-shuts-down-the-internet-then-orders-blocking-of-35-news-websites/.
[16] Committee to Protect Journalists, "Congo imposes total communications blackout during election," *Committee to Protect Journalists*, March 22, 2016, https://cpj.org/2016/03/congo-imposes-total-communications-blackout-during.php.
[17] Matt Burgess, "How Iraq turned off the internet," *Wired*, July 4, 2016, https://www.wired.co.uk/article/iraq-internet-blackout-censorship.
[18] Phillips and Atuhaire, "How Ugandans Overturned An Election Day Social Media Blackout."
[19] United Nations General Assembly Human Rights Council, Resolution 32/L.20, "The promotion, protection and enjoyment of human rights on the Internet," June 27, 2016, https://www.article19.org/data/files/Internet_Statement_Adopted.pdf.
[20] Darrell West, "Internet shutdowns cost countries $2.4 billion last year," *Brookings*, October 6, 2016, https://www.brookings.edu/research/internet-shutdowns-cost-countries-2-4-billion-last-year/.

coordinated effort, an onslaught of Chinese netizens flooded newly elected Taiwanese President Tsai Ing-wen's Facebook page with pro-China comments in an attempt to drown out proponents of Taiwanese independence, despite the fact that Facebook is blocked in China.[21] Facebook, along with Twitter and YouTube, continue to be blocked outright in countries like China and Iran, while other governments selectively restrict access to such sites, usually during times of heightened political tension when citizens need them most. Turkey, for example, blocked access to Facebook and Twitter during an attempted military coup;[22] Russia blocked LinkedIn for failing to follow its new, harsh data localization law;[23] and Brazil blocked WhatsApp inside the country over the company's refusal to turn over user information that WhatsApp says it does not have access to in the first place.[24] Notably, other countries have also been active in their attempts to block similar websites and apps.[25]



Blocked website access on Chinese messaging application WeChat. Image Credit: The Citizen Lab at the Munk School of Global Affairs, University of Toronto.

In today's increasingly interconnected world, social platforms (like Facebook) are practically synonymous with the internet itself. Yet users living under repressive regimes who utilize these sites to express their political,

[21] Marco Huang, "Chinese Netizens Flood Tsai Ing-Wen's Facebook Page With Anti-Taiwan Independence Posts," *Wall Street Journal*, January 21, 2016, https://blogs.wsj.com/chinarealtime/2016/01/21/chinese-netizens-flood-tsai-ing-wens-facebook-page-with-anti-taiwan-independence-posts.
[22] Devin Coldewey, "Facebook, Twitter and YouTube blocked in Turkey during reported coup attempt," *TechCrunch*, July 15, 2016, https://techcrunch.com/2016/07/15/facebook-twitter-and-youtube-blocked-in-turkey-during-reported-coup-attempt/.
[23] Ingrid Lunden, "LinkedIn is now officially blocked in Russia," *TechCrunch*, November 17, 2016, https://techcrunch.com/2016/11/17/linkedin-is-now-officially-blocked-in-russia/.
[24] Cynthia M. Wong and Maria Laura Canineu, "Brazil's Digital Rights Contradictions," *Human Rights Watch*, May 16, 2016, https://www.hrw.org/news/2016/05/16/brazils-digital-rights-contradictions.
[25] For example, authorities in Indonesia called for Grindr and 17 other gay dating apps to be banned. Mary Emily O'Hara, "Police call for Grindr and other gay-friendly apps to be banned in Indonesia," The Daily Dot, September 9, 2016, https://www.dailydot.com/irl/indonesia-grindr-ban-facebook-gay-investigation/. Similarly, Egypt and the United Arab Emirates have attempted to block access to secure messaging app Signal. Andy Greenberg, "Encryption App Signal Fights Censorship With a Clever Workaround," Wired, December 21, 2016, https://www.wired.com/2016/12/encryption-app-signal-fights-censorship-clever-workaround/.

social, or religious views often risk legal retribution, intimidation, harassment, and physical violence from government or government-affiliated actors and their supporters. Journalists in Tanzania have resorted to using WhatsApp to securely reach their audiences and report the news, while also avoiding the risk of going to jail for insulting their president on social media.[26] Many users in Tanzania now "think of WhatsApp as being synonymous with owning a mobile phone."[27] Meanwhile, the government of Thailand charged multiple users with sedition for criticizing the ruling military junta on Facebook;[28] a newspaper editor in Pakistan faced defamation charges after "tarnishing the image" of a government minister in a Facebook post;[29] and Cambodian authorities oversaw a rise in internet-related arrests for users expressing themselves online, often via Facebook, as the government further restricts free speech online;[30] Similar forms of government intimidation occurred in Zimbabwe, where access to several social media sites and apps, including WhatsApp, was blocked in response to protests over widespread corruption by the the Mugabe regime;[31] and in China, where ethnic Mongolian herders were detained for discussing protests on popular Chinese messaging app WeChat.[32]

> **"I was a hipster who didn't pay attention to political or social issues. The restrictions of the Great Firewall changed me."**[33]
>
> \- 33-year-old Chinese internet user Lily Wang

Controlling the flow and dissemination of individual online speech on social media is often part of a broader information control strategy that also targets the press. Alternative, non-state-controlled news outlets and independent journalists offer citizens critical stories that fall within the public interest, but outside the government's desired narrative, on topics like government corruption, human rights, and opposition politics. The websites of important media outlets, therefore, are increasingly the targets of government-mandated censorship online. In 2016, this trend continued, as Bangladesh blocked 35 news websites;[34] Russia's largest search engine, Yandex, announced it would no longer feature results from any news organization not registered with the Russian government;[35] and Azerbaijan blocked the websites of Radio Free Europe/Radio Liberty (RFE/RL) and Voice of America.[36] Similar actions took place in Thailand, where site blockages spiked

[26] Yomi Kazeem, "Tanzanians are being sentenced to jail for insulting their president on social media," *Quartz*, June 22, 2016, https://qz.com/713463/tanzanians-are-being-sentenced-to-jail-for-insulting-their-president-on-social-media.
[27] Omar Mohammed, "How Tanzanian journalists use WhatsApp to report the news," *International Center for Journalists*, May 27, 2016, https://ijnet.org/en/blog/how-tanzanian-journalists-use-whatsapp-report-news.
[28] Human Rights Watch, "Thailand: 8 Charged for Mocking Junta Leader on Facebook," *Human Rights Watch*, May 9, 2016, https://www.hrw.org/news/2016/05/09/thailand-8-charged-mocking-junta-leader-facebook.
[29] Kamran Reza Chowdhury, "Bangladesh Police Upgrade Defamation Charge Against Editor," *BenarNews*, April 20, 2016, http://www.benarnews.org/english/news/bengali/Probir-Sikder-04202016182333.html.
[30] Mong Palatino and Sopheap Chak, "The Troubling Rise of Internet-Related Arrests in Cambodia," Global Voices, February 11, 2016, https://globalvoices.org/2016/02/11/troubling-rise-of-internet-related-arrests-in-cambodia/.
[31] Jeffrey Moyo and Norimitsu Onishi, "Robert Mugabe Seizes on the Latest Political Threat to His Zimbabwe: WhatsApp," *New York Times*, October 2, 2016, https://www.nytimes.com/2016/10/03/world/africa/zimbabwe-robert-mugabe-whatsapp.html.
[32] Qiao Long and Lam Lok-tung, "WeChat Discussions Prompt Chinese Authorities to Detain Mongolian Herders," *Radio Free Asia*, March 24, 2016, http://www.rfa.org/english/news/china/weshat-discussions-prompt-chinese-authorities-to-detain-mongolian-herders-03242016134553.html.
[33] Li Yuan, "Chinese Voice Frustration Over 'Great Firewall'," *Wall Street Journal*, April 7, 2016, https://blogs.wsj.com/chinarealtime/2016/04/07/chinese-voice-frustration-over-great-firewall/.
[34] Zara Rahman, "Bangladesh Shuts Down the Internet, Then Orders Blocking of 35 News Websites."
[35] Isaac Webb, "Russian Search Engine Will Only List Top News Stories from State-Registered Media," *Global Voices Advocacy*, October 25, 2016, https://advox.globalvoices.org/2016/10/25/russian-search-engine-will-only-list-top-news-stories-from-state-registered-media/.
[36] Reporters Without Borders, "Azerbaijan - Renewed use of trumped-up charges censor journalists," *Reporters Without Borders*, December 5, 2016, https://rsf.org/en/news/azerbaijan-renewed-use-trumped-charges-censor-journalists.

dramatically after the death of King Bhumibol Adulyadej (over 1,300 websites were blocked - more than the previous five years combined);[37] Malaysia, where publishing platform Medium was blocked after The Sarawak Report posted stories detailing alleged government corruption;[38] and China, where several popular independent news outlets were ordered to cease operations or "clean up" their operations,[39] and Apple was forced to remove apps for the New York Times from the Chinese version of its App Store.[40]

Online Harassment

Hate speech, targeted hacking, troll attacks, and threats of violence are among the types of online harassment increasingly used to censor, intimidate, and silence underrepresented voices in repressive contexts. Such harassment serves as a reprisal tactic against those who freely express themselves online, and a means by which the state and its sympathizers can control online discourse to drown out opposition voices and distract the public from critical discussions.

In 2016, this type of behavior was documented around the world. Coordinated, paid "troll gangs" harassed activists and journalists in Mexico with death threats and violent warnings to cease their activities,[41] research found that China fabricates nearly half a billion social media posts per year in an attempt to deter meaningful dialogue through distraction rather than engage in debate with those who express opinions that run contrary to the Party line;[42] and troll networks in Azerbaijan continued to try to silence independent journalists and alternative political perspectives through a variety of online harassment tactics.[43] In the United Arab Emirates, human rights activist Ahmed Mansoor was the target of a highly sophisticated iPhone exploit, developed by a private sector government contractor and sent via text message.[44]

> **"Everything in my life went to hell thanks to the trolls."**[45]
>
> - 35-year-old Finnish investigative journalist Jessikka Aro

Looking to manage dissent, the government of Thailand instituted a "Cyber Scouts" initiative that encouraged young internet users to spy on their friends and report possible "lèse majesté" violations to authorities.[46] In

[37] Associated Press, "Thai website shutdowns soar after king's death," *Associated Press*, November 17, 2016, https://www.usnews.com/news/world/articles/2016-11-17/apnewsbreak-thai-website-shutdowns-soar-after-kings-death.
[38] Parker Higgins, "Medium's Sitewide Encryption Confronts Censorship in Malaysia," *Electronic Frontier Foundation*, January 28, 2016, https://www.eff.org/deeplinks/2016/01/mediums-sitewide-encryption-confronts-censorship-malaysia.
[39] Michael Forsythe, "China Clamps Down on Online News Reporting," *New York Times*, July 25, 2016, https://www.nytimes.com/2016/07/26/world/asia/china-media-sina-sohu-netease-phoenix.html.
[40] Katie Benner and Sui-Lee Wee, "Apple Removes New York Times Apps From Its Store in China," *New York Times*, January 4, 2017, https://www.nytimes.com/2017/01/04/business/media/new-york-times-apps-apple-china.html.
[41] Tanya O'Carroll,* "Mexico's misinformation wars: How organized troll networks attack and harass journalists and activists in Mexico," *Amnesty International*, January 24, 2017, https://medium.com/amnesty-insights/mexico-s-misinformation-wars-cb748ecb32e9.
*O'Carroll is a member of the OTF Advisory Council.
[42] Merrit Kennedy, "Study: China's Government Fabricates About 488 Million Social Media Posts Every Year," *National Public Radio*, May 22, 2016, http://www.npr.org/sections/thetwo-way/2016/05/22/479057698/study-chinas-government-fabricates-about-488-million-social-media-posts-every-ye.
[43] Arzu Geybulla, "In the crosshairs of Azerbaijan's patriotic trolls," *openDemocracy*, November 22, 2016, https://www.opendemocracy.net/od-russia/arzu-geybulla/azerbaijan-patriotic-trolls.
[44] Lorenzo Franceschi-Bicchierai, "The 'Million Dollar Dissident' Is a Magnet for Government Spyware," *Motherboard*, August 26, 2016, https://motherboard.vice.com/en_us/article/ahmed-mansoor-million-dollar-dissident-government-spyware.
[45] Andrew Higgins, "Effort to Expose Russia's 'Troll Army' Draws Vicious Retaliation," *New York Times*, May 30, 2016, https://www.nytimes.com/2016/05/31/world/europe/russia-finland-nato-trolls.html.
[46] David Gilbert, "Thailand's government is using child 'Cyber Scouts' to monitor dissent," *Vice News*, September 19, 2016, https://news.vice.com/article/thailands-royal-family-is-using-child-cyber-scouts-to-monitor-dissent.

Finland, a journalist investigating Russian troll factories found herself the target of online harassment so extreme, her life was reduced to a form of "hell."[47] And in Iran, hackers likely working on behalf of the Iranian government targeted human rights activists, exiles abroad, and Iran-based political dissidents.[48] In Pakistan, harassment took the form of blackmail as men threaten to release lewd, doctored photos of the women they targeted in an attempt to extort money from them.[49] Perhaps most troubling of all, in Bangladesh several secular activists and bloggers were murdered for expressing their religious opinions online, prompting increasing self-censorship;[50]

Collusion Between States and Internet Sovereignty

With its elaborate, multifaceted censorship mechanism known as the Great Firewall, China is a world leader in censorship capabilities. Authoritarian state leaders around the globe, including Russian President Vladimir Putin, have taken notice of China's ability and sought to mimic it in their own country.[51] In addition to pursuing a legislative agenda that includes strict data localization and retention laws, as well as government backdoors to encrypted communications, Russia has also sought out the expertise of the minds behind China's Great Firewall, hoping to implement more stringent control over the internet in Russia. High-level meetings have reportedly taken place between Moscow and Beijing as Russia seeks to acquire the technological means to increase its surveillance and censorship capabilities.[52] In 2016, Russia unveiled a new information security doctrine that called for "managing the Russian segment of the Internet."[53]

Elsewhere, Zimbabwean President Robert Mugabe expressed his desire to emulate Chinese-style internet "security measures,"[54] while Iran launched its own in-country intranet, shut off from the rest of the world and built to "encourage less dependency on the worldwide Internet."[55] In a move representative of the global proliferation of restrictive data localization laws, the Iranian government also ordered all social media sites and messaging applications with Iran-based users to move their data to servers inside the country, prompting concerns about users' security and privacy.[56]

> **"China and Russia have industrialized the process of censorship. We have the Open Technology Fund. It's sad how different the level of resources are."**[57]
>
> \- Johns Hopkins University cryptologist Matthew Green*

[47] Andrew Higgins, "Effort to Expose Russia's 'Troll Army' Draws Vicious Retaliation."
[48] Elias Groll, "Spear Phishing in Tehran," *Foreign Policy*, August 9, 2016, https://foreignpolicy.com/2016/08/09/spear-phishing-in-tehran/.
[49] Simon Parkin, "Pakistan's Troll Problem," *The New Yorker*, June 28, 2016, http://www.newyorker.com/tech/elements/pakistans-troll-problem.
[50] Arafatul Islam, "Blogger killings leading to 'self-censorship' in Bangladesh," Deutsche Welle, March 5, 2016, http://www.dw.com/en/blogger-killings-leading-to-self-censorship-in-bangladesh/a-19231816.
[51] *See, e.g.*, Bethany Allen-Ebrahimian, Foreign Policy, June 28, 2016, http://foreignpolicy.com/2016/06/29/the-man-who-nailed-jello-to-the-wall-lu-wei-china-internet-czar-learns-how-to-tame-the-web/.
[52] Andrei Soldatov and Irina Borogan, "Putin brings China's Great Firewall to Russia in cybersecurity pact," *The Guardian*, November 29, 2016, https://www.theguardian.com/world/2016/nov/29/putin-china-internet-great-firewall-russia-cybersecurity-pact.
[53] Robert Coalson, "New Kremlin Information-Security Doctrine Calls For 'Managing' Internet In Russia," *Radio Free Europe/Radio Liberty*, December 6, 2016, https://www.rferl.org/a/russia-informaiton-security-internet-freedome-concerns/28159130.html.
[54] L.S.M Kabweza, "Chinese style internet censorship coming to Zimbabwe – President Mugabe," *Techzim*, April 4, 2016, http://www.techzim.co.zw/2016/04/china-style-internet-censorship-coming-to-zimbabwe-president-mugabe.
[55] Radio Free Europe/Radio Liberty, "Iran Inaugurates Its Own Intranet," *Radio Free Europe/Radio Liberty*, August 29, 2016, https://www.rferl.org/a/iran-inaugurates-its-own-intranet/27951780.html.
[56] Reuters, "Iran orders social media sites to store data inside country," *Reuters*, May 29, 2016, http://www.reuters.com/article/internet-iran-idusl8n18q0in.
[57] Elias Groll, "How Hillary Clinton Helped Build WhatsApp's State-of-the-Art Encryption," *Foreign Policy*, April 6, 2016, https://foreignpolicy.com/2016/04/06/how-hillary-clinton-helped-build-whatsapps-state-of-the-art-encryption/.
* Green is a member of the OTF Advisory Council.

Key Results from 2016

OTF continued to expand the reach and impact of its support in 2016, investing in original research, real-time interventions, and beneficial partnerships with other organizations in the internet freedom community.

Expanding the Internet Freedom Community

- Nearly two billion people are now regularly using OTF-supported technology to circumvent restricted internet connections, strengthen online security, and enhance digital privacy.

- OTF's Localization Lab enabled translations of internet freedom tools and ensured their accessibility to a global audience. The Lab supports 60 tools with over 5,400 participating volunteers contributing to the submission and verification of more than half a million translated words into over 200 languages and dialects.

- To meet the expanding need for individuals to work on internet freedom technology, OTF offered numerous fellowship programs, receiving nearly 150 applications for support to improve individual research, analysis, development, and implementation work critical to the future growth and capacity of the internet freedom community.

- While expanding the space necessary to address the needs of affected communities, the OTF Community Lab supported individuals as they participated in working discussions and roundtables, and shared new information and findings to inform solutions. This included the Internet Freedom Festival, Citizen Lab Summer Institute, Iran Cyber Dialogues, Forum on Internet Freedom in Africa, Rapid Response Summit, RightsCon, Reproducible Builds Summit, OONI ADINA 15, Allied Media Conference, Chaos Communication Congress, Black Hat, and the OTF Summit.

- In October 2016, OTF held its fifth annual OTF Summit in Towson, Maryland. More than 200 people attended, including individuals from OTF-supported projects, Advisory Council members, funders, and experts from the greater internet freedom community. Participants discussed current and emerging challenges, innovations, strategies, and priority needs in the field of global internet freedom.

- OTF supported security audits of 12 internet freedom projects, identifying 171 privacy and security vulnerabilities. Since its inception, OTF has supported 77 audits identifying and patching a total of 1,870 security vulnerabilities.

Organizational Efficiency

- 85 percent of OTF's program budget was used to directly support and manage over 100 projects, initiatives, and lab support.

- The OTF team reviewed and responded to nearly 700 requests for funding, totaling over $85 million.In doing so, the team provided valuable substantive feedback to those seeking support for their work and, when necessary, referred proposals to more appropriate funders.

- OTF expanded the knowledge base and scope of its review process expertise by increasing the subject matter experts on OTF's volunteer Advisory Council. The Council added leading experts in internet freedom fields, such as Jared Spool (Founding principal of User Interface Engineering), Roya Ensafi (postdoctoral researcher), and Karen Renaud (Usable Security & Privacy Lead, School of Computing Science, University of Glasgow).

Civil Society and Governmental Outreach

- OTF supported Rapid Response engagements across the globe, assisting at-risk individuals (journalists, human rights activists, and NGO workers) in response to digital attacks and other forms of targeted online censorship in Tibet, Azerbaijan, China, Thailand, Bahrain, Sudan, Ethiopia and Pakistan.

- OTF supported numerous individuals and organizations producing ground-breaking analytical and research reports, such as: *Detecting DNS Root Manipulation*; *Zambia: Internet Censorship during the 2016 General Elections?*; *Kenya: Censorship-free Internet?*; *The State of Internet Censorship in Malaysia*; *Ethiopia: Evidence of Social Media Blocking and Internet Censorship*; *The Gambia: Internet Shutdown during 2016 Presidential Election*; *Tor's Usability for Censorship Circumvention*; *SNI proxies*; *A Tough Nut to Crack: A Further Look at Privacy and Security Issues in UC Browser*; *Privacy and Security Issues in BAT Web Browsers*; *Harmonized Histories? A Year of Fragmented Censorship Across Chinese Live Streaming Applications*; *An Uneven Balance: Analysis of Internet Censorship in Zimbabwe, Zambia, and Swaziland*; and *Journalists in Distress: Assessing the Digital Viability of a Global Emergency Assistance Network*.

- OTF routinely convened and participated in meetings to increase collaboration and coordination with other internet freedom and human rights technology funders, and to leverage public funds to obtain the maximum private funding available.

- Representatives of projects supported by OTF engaged with internet freedom technologists, researchers, and policymakers while participating in key conferences, including the Internet Freedom Festival, RightsCon, Hackers on Planet Earth (HOPE), Iran Cyber Dialogue, Privacy Enhancing Technology Symposium, USENIX Workshop on Free and Open Communications on the Internet, USENIX Hot Topics in Privacy Enhancing Technologies, Freedom Online Conference, Privacy and Security Forum, Linux Foundation Collaboration Summit, Decentralized Web Summit, Re:publica, Citizen Lab Summer Institute, Latin America and Caribbean Internet Governance Forum, Mozilla Festival, IETF 96, Oslo Freedom Forum, Decentralized & Encrypted, ISC Global Workshop, Deutsche Welle Global Media Forum, Internet Freedom Festival, Africa Internet Freedom Forum, Internet Governance Forum, Silicon Valley Community Foundation, Chaos Communication Congress, Stockholm Internet Forum, Forum on Internet Freedom in Africa, Global Media Forum, and the DG7 internet freedom working group.

Strengthening Funding Collaboration

- OTF continued to advance efforts to diversify support for internet freedom beyond U.S. government funding programs by engaging with private foundations, tech companies, startup incubators, like-minded foreign government funders, and venture capitalists.

- OTF raised awareness of the need for greater internet freedom funding around the world and helped increase globally available funding by unlocking new sources, bringing the total amount of private funds set aside for internet freedom related efforts since 2012 to more than $100 million.

- Through active coordination and direct collaboration with other private and public donors, OTF has succeeded in leveraging a tenfold increase from the program's initial investment in a number of projects. Since 2012, OTF has invested 4 million dollars which have in turn been leveraged by projects to receive more than 50 million additional dollars from other sources.

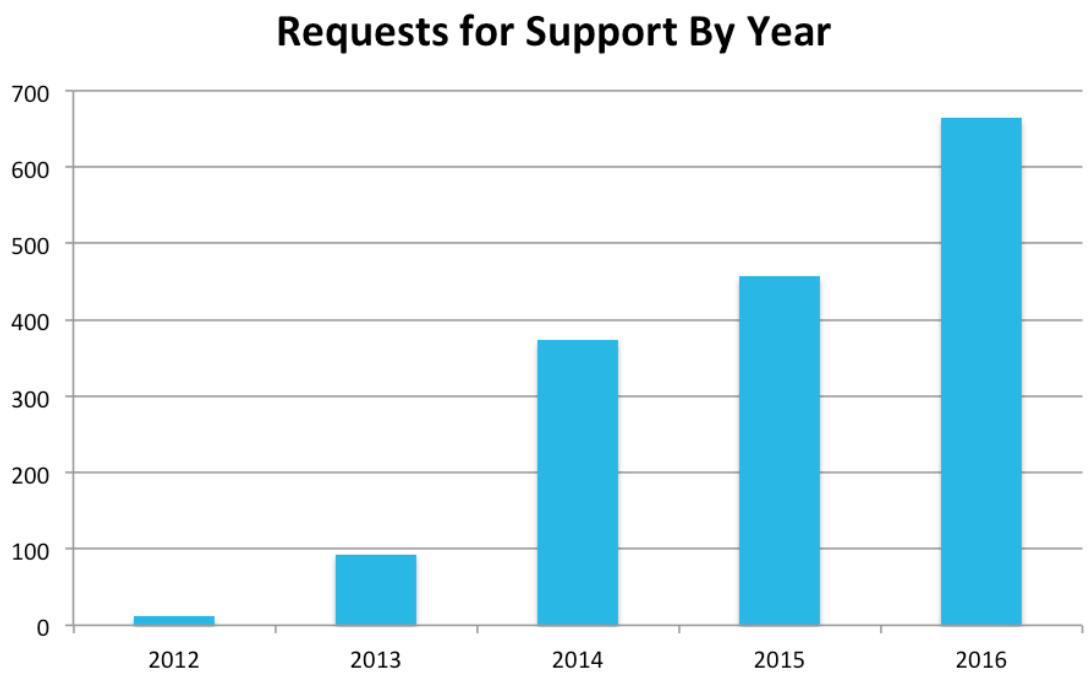
- OTF actively participated in numerous external review panels of related technology proposals, including the State Department's Internet Freedom Program, National Science Foundation's Secure and Trustworthy Cyberspace Program, Linux Foundation's Core Infrastructure Initiative, Access Now, Media Democracy Fund, Ford Foundation, Open Society Foundations, MacArthur Foundation, Knight

Foundation, Mozilla Foundation, British Broadcasting Corporation, Deutsche Welle, Swedish International Development Agency, and the German Federal Foreign Office.

- OTF expanded collaboration on capacity building through fellowships hosted at premier organizations and research institutions, including University of Toronto's Citizen Lab, International Computer Science Institute, Harvard University, University of New Mexico, and Coding Rights.

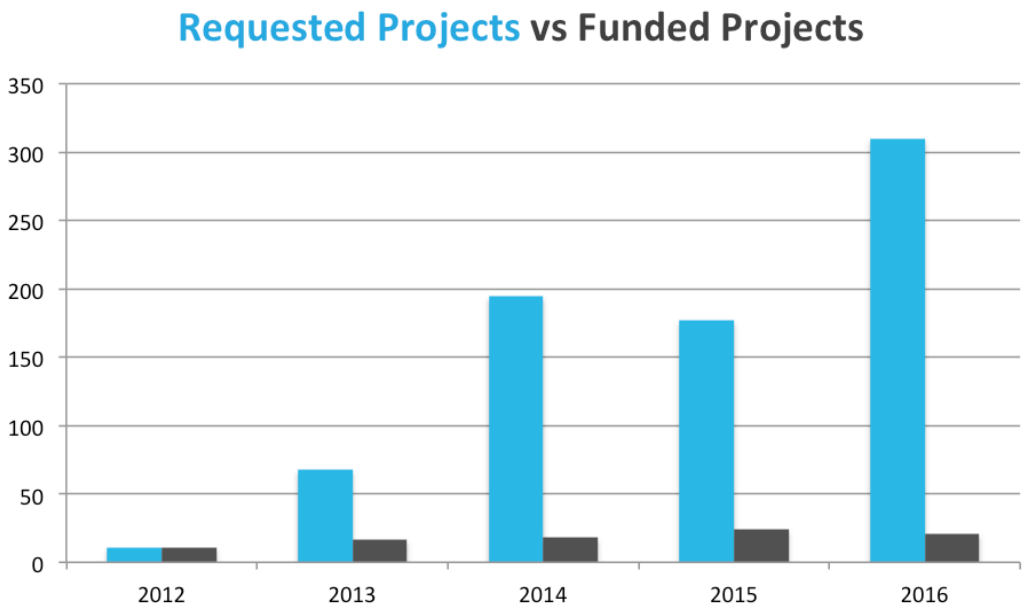
Trends from 2016

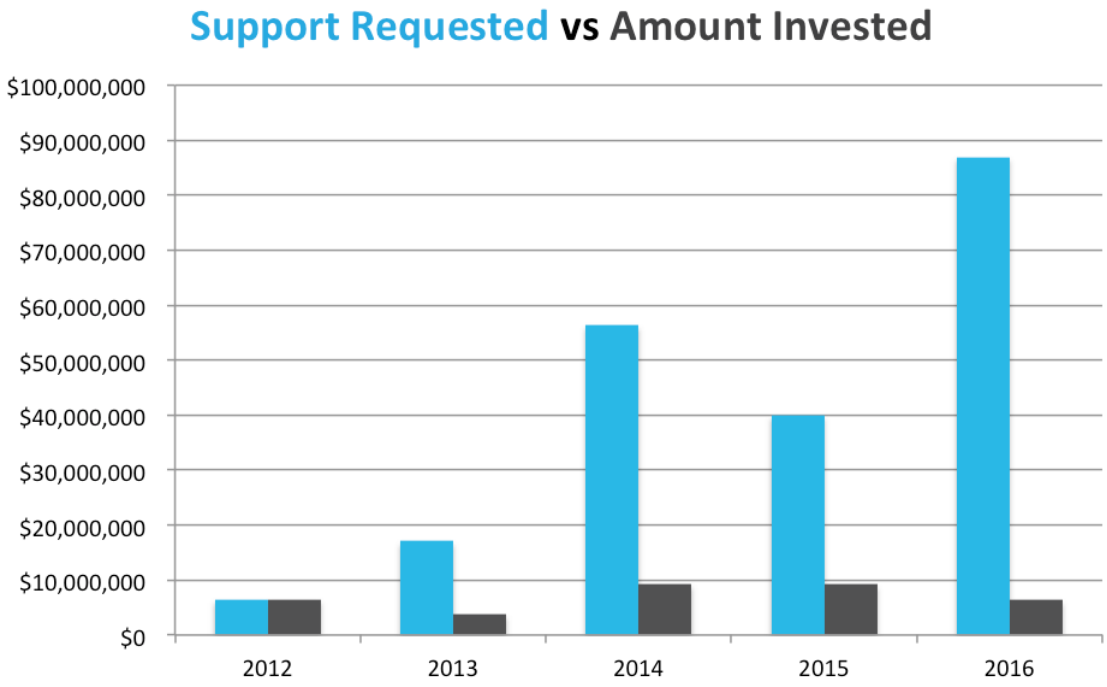
As in years past, OTF once again experienced significant growth in requests for its support. In 2016, OTF received the highest number of support requests in its history. Overall, OTF received nearly 700 submissions requesting a total of over $85 million.



Concept Note Submissions and Increased Need

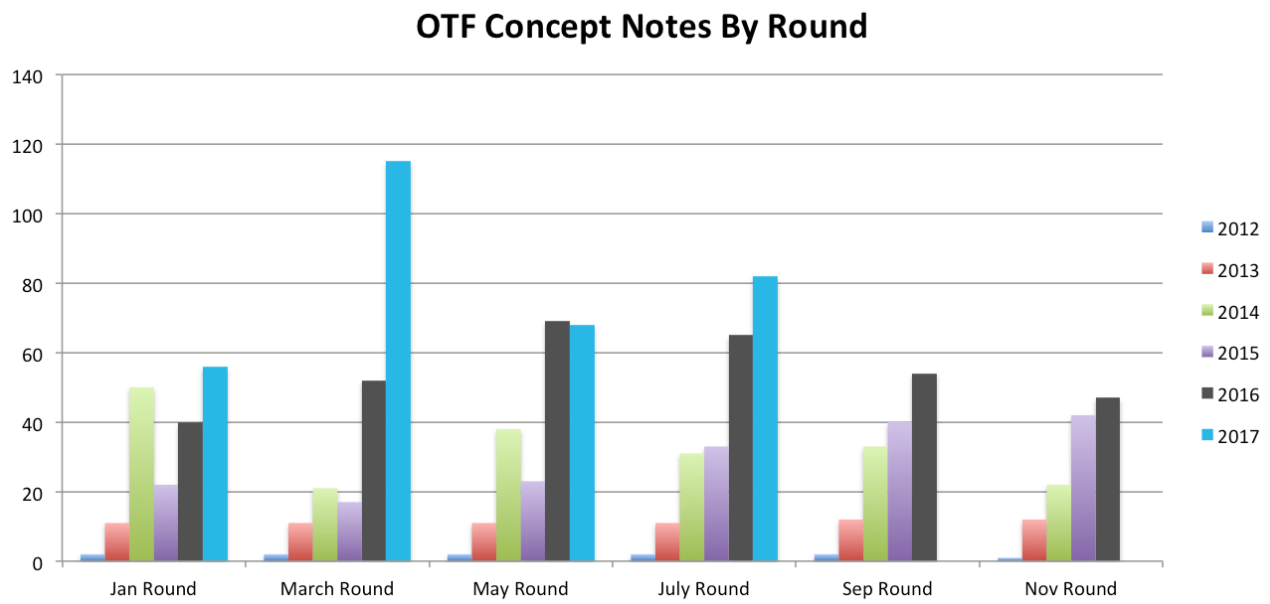
Unfortunately, with a significantly lower budget than in years past (see below), OTF was not able to dedicate the same level of funds to projects applying to the Internet Freedom Fund as in previous years. The overwhelming majority of applicants for OTF support had to be declined despite a wealth of creative and worthy projects. If OTF's budget does not expand, this trend will continue as both the quantity and quality of applicants continues to increase.





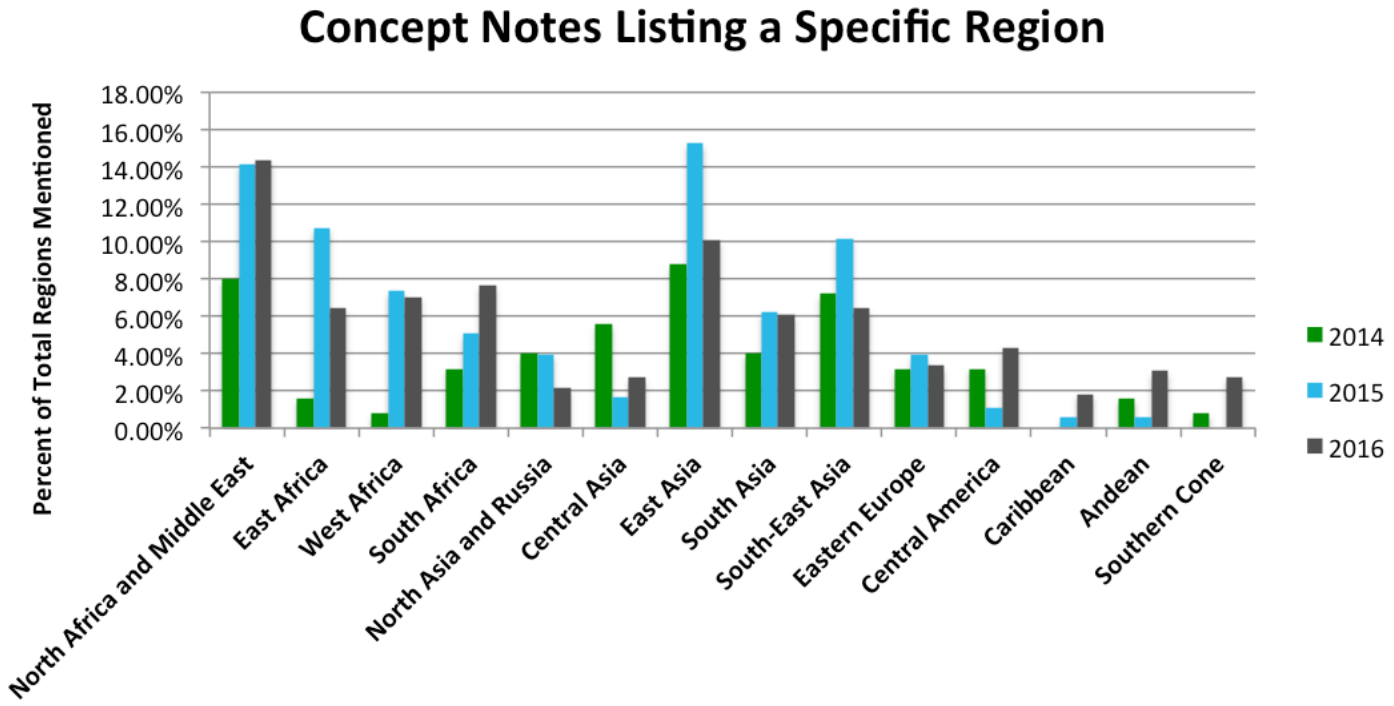
In 2016, OTF witnessed continued growth in the level of interest in the program and in the field of internet freedom technology. This led to a dramatic increase in concept note submissions, particularly from new and diverse applicants.[58] During 2014 and 2015, OTF was able to fund approximately 10 percent of the concept note submissions it received.[59] In 2016, this figure dropped below 5 percent. By comparison, the National Science Foundation funds approximately 25 percent of submissions it receives.[60] OTF's overall budget has not increased in step with authoritarian investment in online censorship, nor with the demand to combat internet censorship. Barring an increase in funding, the disparity between submissions received and projects funded will continue to expand.

[58] The OTF team responds to all submissions every two months.
[59] Concept notes include applications submitted to the Internet Freedom Fund and the Core Infrastructure Fund.
[60] "NSF receives approximately 40,000 proposals each year for research, education and training projects, of which approximately 11,000 are funded." https://www.nsf.gov/funding/aboutfunding.jsp



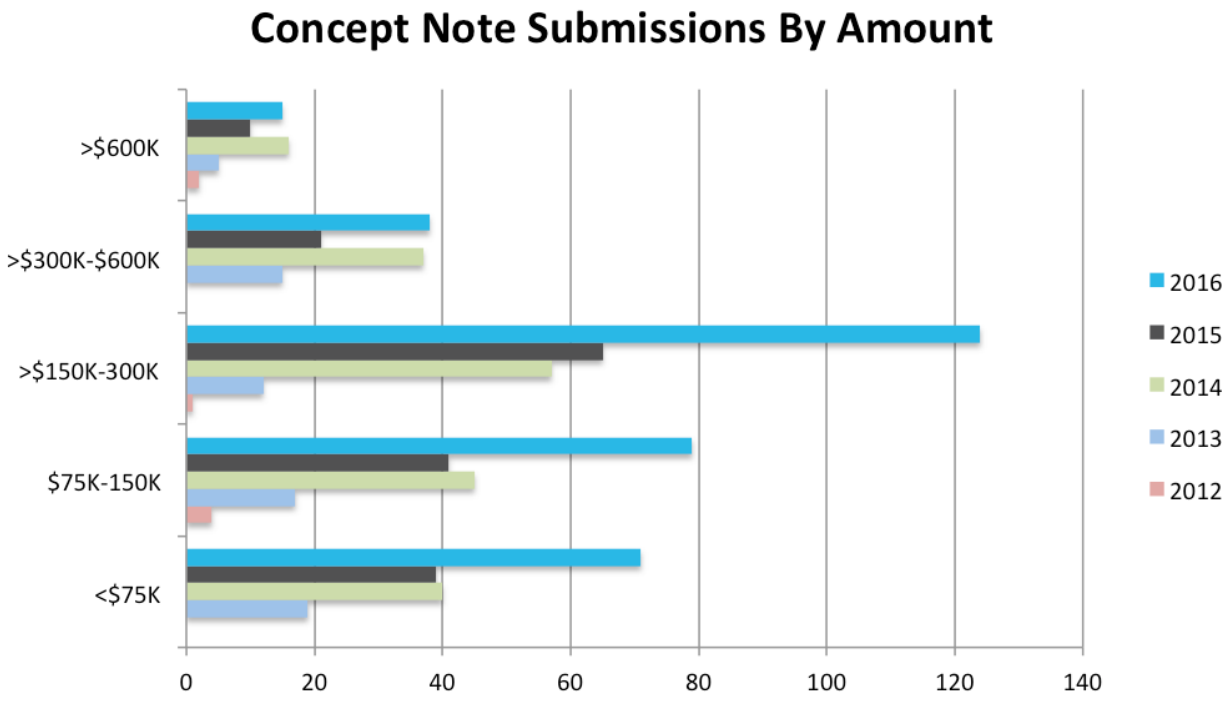
Note: OTF did not have concept note rounds in 2012 and much of 2013. Thus, the total concept notes for those years have been evenly distributed across all rounds.

Budget constraints result in a lack of support for projects all across the globe. While nearly 60 percent of concept notes submitted to OTF listed a global focus in 2016, many proposed to focus on a specific geographic area. As shown below, the two most prevalent geographic focus areas for concept notes are North Africa and Middle East and East Asia.

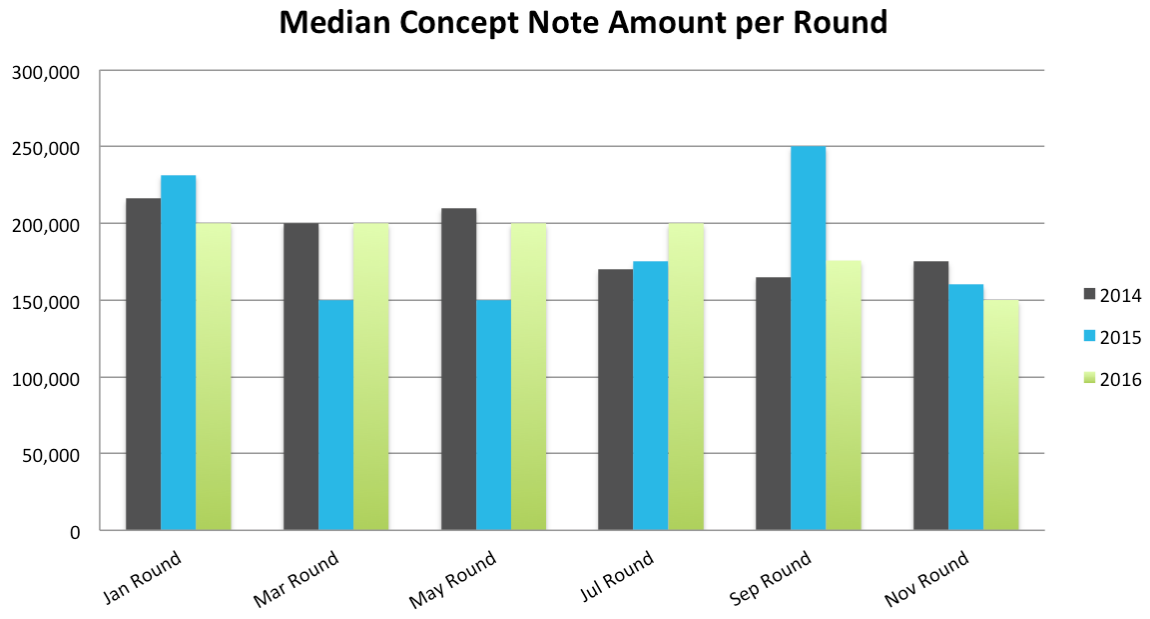


Finding a Low Cost Niche

Despite the increased number of concept note submissions, the proportion of submissions requesting less than $300,000, which is the target ceiling of OTF support, grew. This approach complements the strategies of the program's partner U.S. government funders. In 2016, more than 80 percent of concept notes submitted fell within this range, OTF's highest level ever.

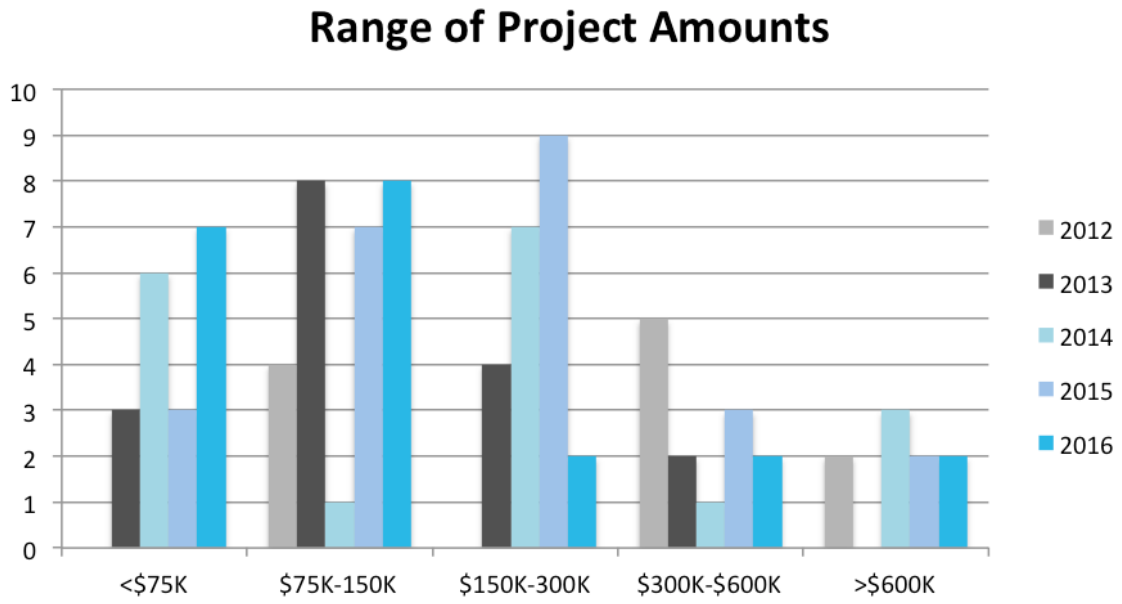


Overall, the median request level per concept note round has remained consistent throughout the past three years.



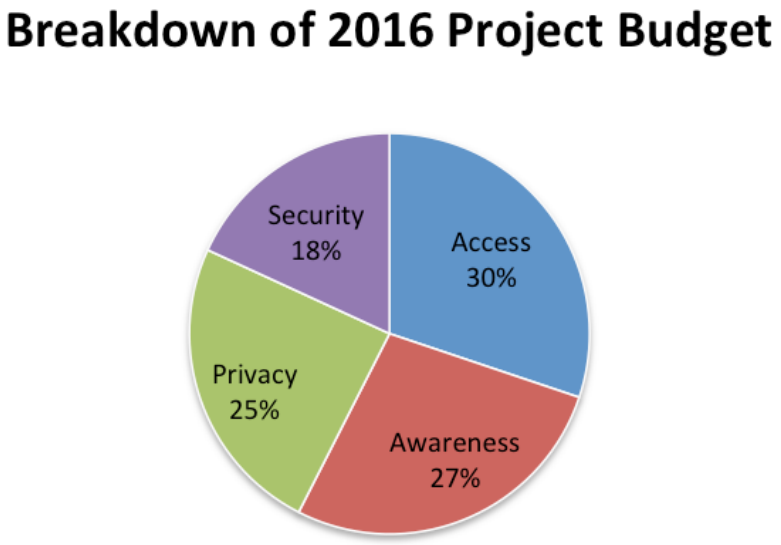
OTF prioritizes increasing the accessibility of U.S. Government internet freedom funds to emerging talent by removing unnecessary barriers to entry, directly engaging with those carrying out the work, and continuously building internet freedom capacity. The request levels detailed above demonstrate the program's

attractiveness to projects that do not meet the minimum levels necessary to receive support from other U.S. government internet freedom funders. OTF's process ensures it is open and accessible to those that would otherwise be turned away from more restrictive programs. This includes individuals, small team innovators, entities based outside of the United States, those unable to incur the typical overhead costs accompanying a U.S. government grant or contract, and applicants lacking professional writing skills or unwilling to incur substantial overhead by acting as a subcontractor to a previous recipient. As demonstrated below, OTF continued to primarily support projects in this range.

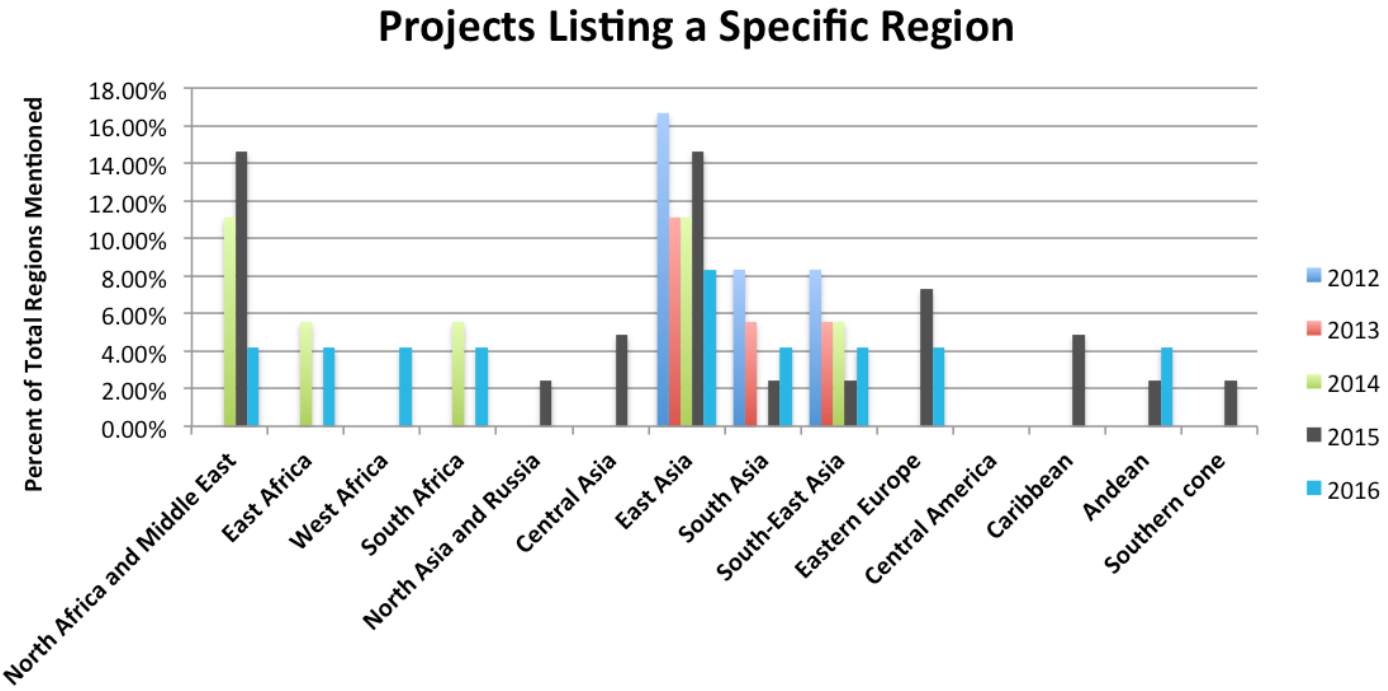


Project Breakdown

While the overall project numbers remained consistent, OTF supported a slightly higher proportion of access and awareness projects in 2016. The rise in support for these projects reflects the increase in censorship and internet shutdowns, and the growing need to ensure censored individuals understand that no-cost solutions are available. Overall, OTF-supported projects spanned a wide range of focus areas, as described in the Program Overview section below.

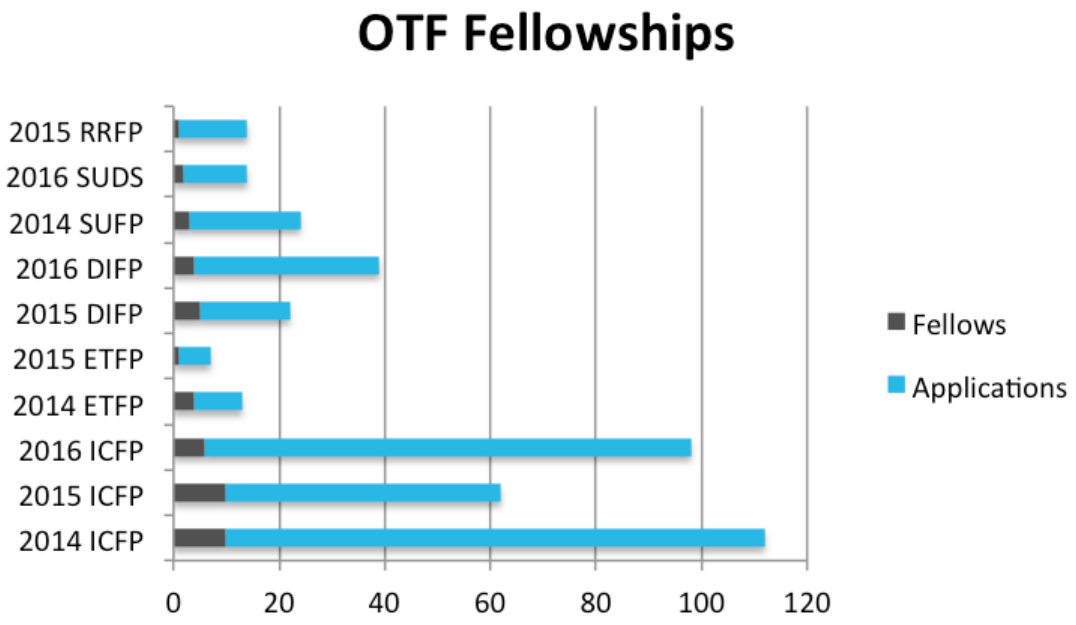


Since the program's creation, the regional focus areas of the concept notes OTF has received are largely consistent with the projects OTF has supported. Approximately 60 percent of projects supported by OTF listed a global focus. Of the remaining 40 percent that listed regions, North Africa and Middle East, and East Asia were the two most common, with South-East Asia also receiving a noteworthy amount.



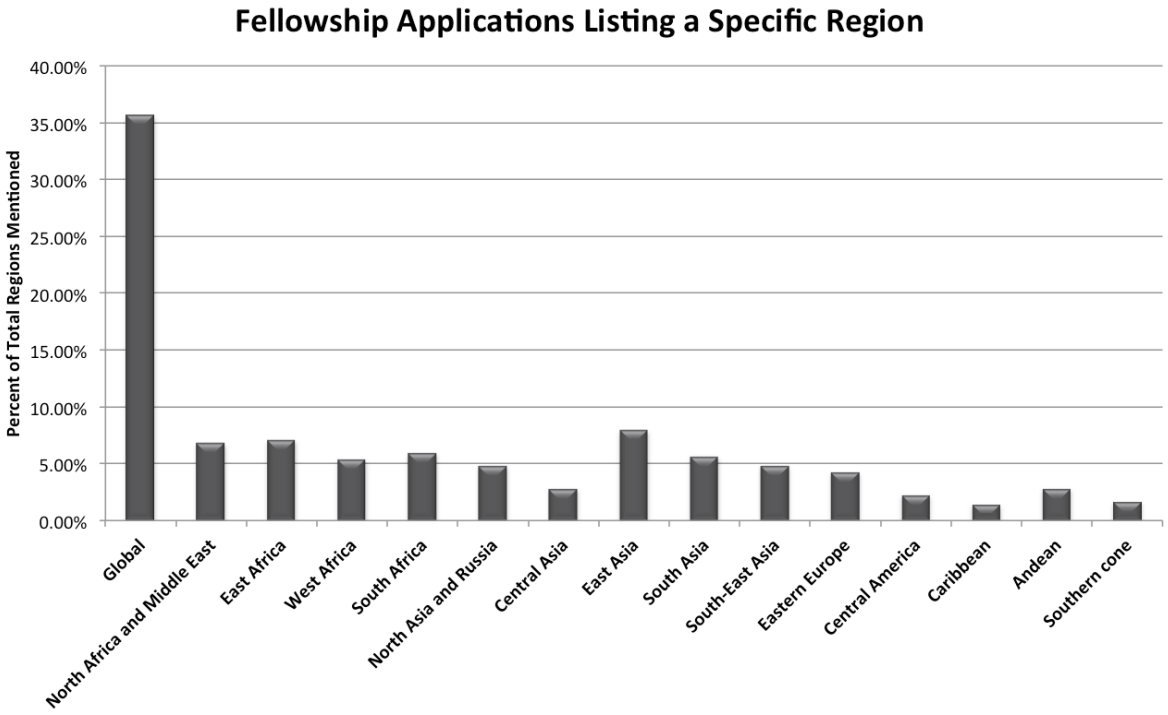
Fellowship Breakdown

OTF's fellowships continued to bring in new applicants and directly support a host of talented individuals with minimal cost and maximum impact. OTF operated multiple fellowship programs in 2016 spanning a variety of focus areas described in more detail in the next section.

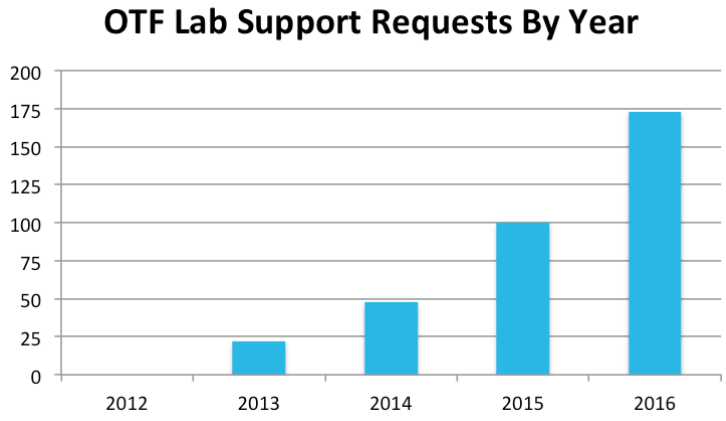


Note: The fellowship programs abbreviated above are Rapid Response (RRFP), Secure Usability (SUFP & SUDS), Digital Integrity (DIFP), Emerging Technology (ETFP) and Information Controls (ICFP).

As seen in the chart below, fellowship applicants more frequently propose a focus on a specific region than applicants to OTF's concept note rounds.[61] This pattern is consistent with OTF's strategy to promote indigenous capacity building, and mirrors the country-specific focus of many of the fellows in the Information Controls and Digital Integrity Fellowship Programs.



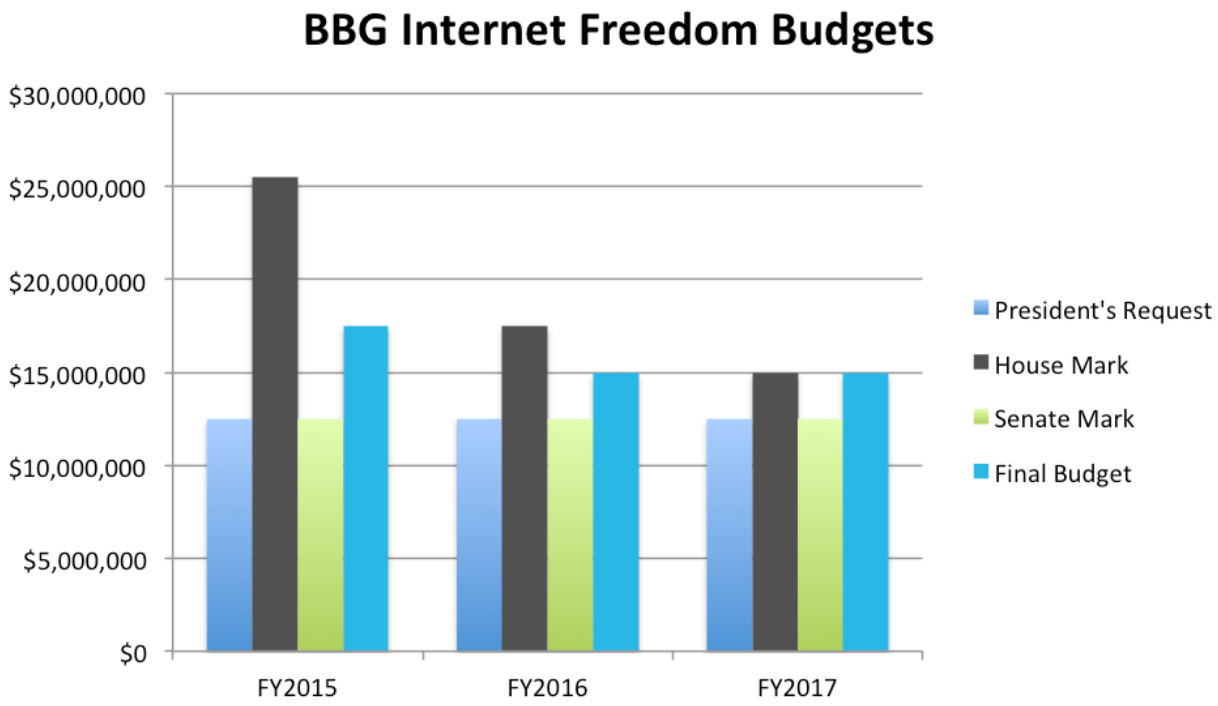
OTF labs continue to see increasing levels of interest and utilization from both OTF-supported and unsupported projects. Each lab is supported by one or more service partners. Rather than one-off agreements between a partner and an applicant in need, OTF maintains a single service agreement with each service partner -- often with bulk discounts -- on behalf of multiple applicants. This ensures that both OTF and a lab participant (or developer) save substantial costs while still receiving the professional assistance necessary to serve end users. These labs have offered critical services for hundreds of internet freedom projects since 2012. As in years past, interest in these services continued to grow in 2016.



[61] The chart reflects applicants to any OTF fellowship program between late May 2015 and the end of 2016. OTF began requesting this information from fellowship applicants in May 2015.

Decreasing U.S. Government Support

Since Congress increased the Broadcasting Board of Governors' budget for internet freedom to its highest level in FY2014 ($25.5 million), the subsequent fiscal years have been defined by precipitous drops. By FY2016, funding had declined to $15 million. The FY2017 budget maintained the level of funding at $15 million.[62]

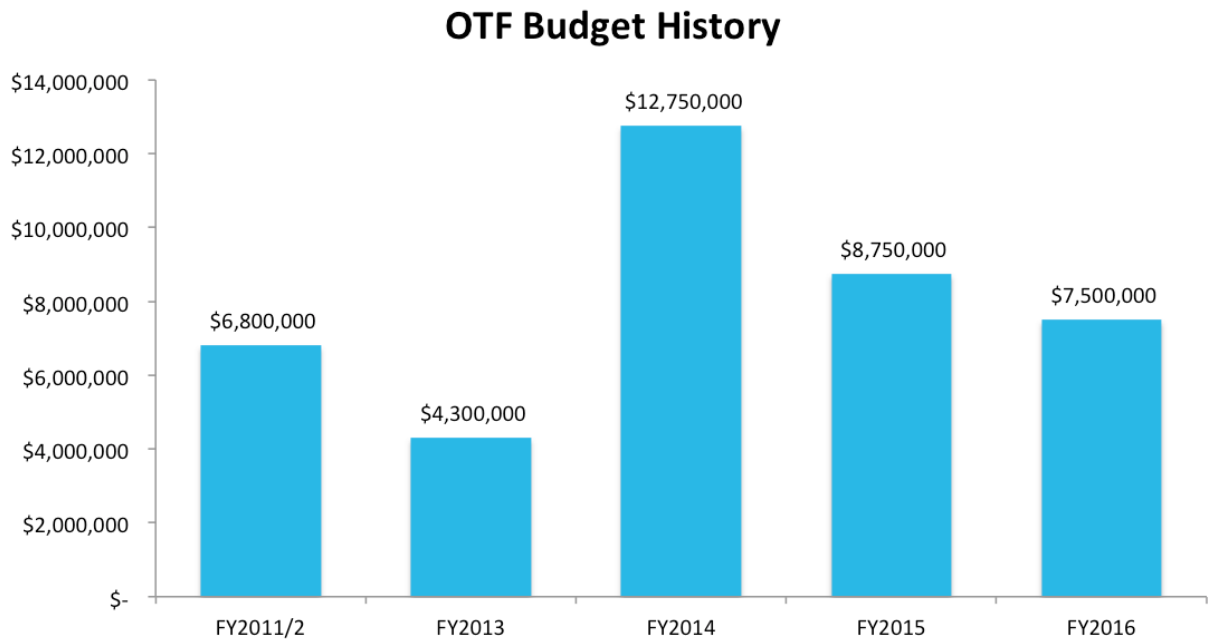


Numerous entities sought significant reductions from the FY2014 level. While a justification for these past decreases has not been provided, the levels remain consistently and significantly higher than those proposed by the Administration. In the three fiscal years since 2014, the Administration requested that Congress fund internet freedom at half of FY2014 levels ($12.5 million).[63] This reduced figure was ultimately included in the White House budget submission and reflected in the marks from the Senate Appropriations Committee.[64] The House Appropriations Committee generally sought a higher level of funding.[65]

Similar to previous years, the final budget for internet freedom in FY2016 split the difference between the House of Representatives figures and those from the Senate, White House and BBG. This resulted in a

[62] Congress explicitly allocated $1.2 million to Radio Free Asia "for the personnel costs associated with Internet freedom activities" with the remaining $13.8 million allocated to the BBG for internet freedom programmatic activities.
[63] Broadcasting Board of Governors, Fiscal Year 2015 Congressional Budget Request, March 25, 2014, p. 10, http://www.bbg.gov/wp-content/media/2014/03/FY-2015-BBG-Congressional-Budget-Request-FINAL-21-March-2014.pdf; Broadcasting Board of Governors, Fiscal Year 2016 Congressional Budget Request, March 10, 2015, p. 11, http://www.bbg.gov/wp-content/media/2015/03/FY2016Budget_CBJ_Final_WebVersion.pdf; Broadcasting Board of Governors, Fiscal Year 2017 Congressional Budget Request, February 9, 2016, p. 14, http://www.bbg.gov/wp-content/media/2011/12/FY-2017-Budget-Submission.pdf.
[64] Budget of the U.S. Government, Appendix, Fiscal Year 2015, p. 1262, https://www.gpo.gov/fdsys/pkg/BUDGET-2015-APP/pdf/BUDGET-2015-APP.pdf; Budget of the U.S. Government, Appendix, Fiscal Year 2016, p. 1220, https://www.gpo.gov/fdsys/pkg/BUDGET-2016-APP/pdf/BUDGET-2016-APP.pdf; Budget of the U.S. Government, Appendix, Fiscal Year 2015, p. 1240,, https://www.gpo.gov/fdsys/pkg/BUDGET-2017-APP/pdf/BUDGET-2017-APP.pdf; Senate Report 113-195, Department of State, Foreign Operations, and Related Programs Appropriations Bill, 2015, p. 30, https://www.gpo.gov/fdsys/pkg/CRPT-113srpt195/pdf/CRPT-113srpt195.pdf; Senate Report 114-79, Department of State, Foreign Operations, and Related Programs Appropriations Bill, 2016, p. 20, https://www.congress.gov/114/crpt/srpt79/CRPT-114srpt79.pdf; Senate Report 114-290, Department of State, Foreign Operations, and Related Programs Appropriations Bill, 2017, pp. 17-18 ,https://www.appropriations.senate.gov/imo/media/doc/FY2017-State-Foreign-Operations-Appropriations-Bill-S3117.pdf.
[65] House of Representatives Report 113-499, State, Foreign Operations and Related Programs Appropriations Bill, 2015, p. 28, https://www.congress.gov/113/crpt/hrpt499/CRPT-113hrpt499.pdf; House of Representatives Report 114-154, State, Foreign Operations and Related Programs Appropriations Bill, 2016, p. 29, https://www.congress.gov/114/crpt/hrpt154/CRPT-114hrpt154.pdf; House of Representatives Report 114-693, State, Foreign Operations and Related Programs Appropriations Bill, 2017, p. 32, https://www.congress.gov/114/crpt/hrpt693/CRPT-114hrpt693.pdf.

minimum allocation to the BBG of $17.5 million in 2015 declining to $15 million in FY2016 (and FY2017).[66] OTF funding declined consistent with the BBG's internet freedom allocation.



Programs in FY2016

The core of OTF's mission is to increase unrestricted access to the internet. OTF's work consists of providing critical funding and services to projects and people. Funding provides direct support to a project or a person via a contract. Services are resources made available by OTF to assist the internet freedom community.

Supported Projects

General Internet Freedom Fund

The General Internet Freedom Fund continued to be the primary open call for OTF-supported projects that promote free press, free expression, and human rights through the free flow of information online. These projects support anti-censorship and secure communications technology, increase censorship awareness, improve digital safety, and research emerging threats. The majority of OTF's budget was expended on applications received through this program fund. OTF encourages organizations and individuals creating or sustaining internet freedom technology and interested in potential funding to submit a concept note for their project. The projects that were approved are listed below in the following categories: Access, Awareness, Privacy, and Security. The dollar amount OTF provided to each project in 2016 is listed after the project's name.

[66] Consolidated and Further Continuing Appropriations Act, 2015, P.L. 113-235, p. 128 STAT. 2580, https://www.congress.gov/bill/113th-congress/house-bill/83/text; Consolidated Appropriations Act, 2016, P.L. 114-113, p. 129 STAT. 2712, https://www.congress.gov/bill/114th-congress/house-bill/2029/text, Consolidated Appropriations Act, 2017, P.L. 115-31, p. 462, https://www.congress.gov/bill/115th-congress/house-bill/244/text.

Access

Tor
$707,300
This project builds on OTF's previous support for Tor, ensuring Tor software can continue to provide worldwide best-in-class anonymity and censorship circumvention solutions.Tor currently serves approximately two million users each day. OTF support has focused on core Tor development work (to make sure the underlying technology remains resilient), and Tor Browser development work (to ensure safety and usability for Tor's packaging and interface side). OTF's 2016 support focused on making it easier for third-party organizations to use and build support for Tor's privacy and anonymizing technologies, empowering users with limited access to powerful devices and fast networks, making Tor easier and more attractive for non-technical and mainstream users, and developing and implementing defenses against online profiling and attacks.

Counterpower Lab
$300,000
Working with the University of California-Berkeley's Anti-Censorship Lab and Incubator, this project is focused on (1) researching and developing user-friendly, high-performance and secure circumvention tools; (2) exploring new circumvention directions; (3) experimenting with innovative technical solutions to distribute tools and censored contents back to users in hostile Internet environments; and (4) conducting outreach and collaboration with other Internet freedom community projects to expand adoption of circumvention technologies.

Clatter
$45,000
Clatter is a suite of extremely lightweight and stand-alone libraries, aimed at creating common protocols and standards for existing projects to add in secure nearby communication without sacrificing their unique approach and use-cases. Clatter draws together many threads of work from different development projects to create a toolkit for local, device-to-device communication, consisting of a set of clear, concise, and well-documented software libraries that allow anyone to add secure device-to-device networking to their own projects.

Awareness

OONI-Probe
$305,000
Ooni-probe, the Open Observatory of Networking Interference, is an open source network testing framework and associated tests for detecting internet censorship. It has collected millions of high-quality measurements from nearly 200 countries using open methodologies and Free and Open Source Software (FL/OSS) to share observations and data about the kind, methods, and amount of surveillance and censorship in the world. OTF support increases the global coverage of ongoing measurement of censorship events, improves detection mechanisms, enhances safety for users in repressive environments, and expands the information available to non-technical audiences including country-specific reports.

Vietnam Open Internet Project
$167,600
This project builds on previous OTF support to scale-up the capacity of the existing Viet Tan Vietnamese language helpdesk and launch public awareness campaigns to target Vietnam's Facebook users, inclusive of journalists, human rights defenders, and at-risk users who are increasingly being targeted for malware attacks.

Open Integrity Index
$108,100
Open Integrity is a platform allowing the collaborative fact-checking of software security and privacy claims. With a lack of accessible information about complex technology issues underlying privacy and security, users have few resources to be discerning about their communication choices, especially those users in vulnerable

communities who need them most. OTF support focuses on launching a beta version of the site that includes assessments of 25 tools to provide reliable and evidence-based answers to common questions.

NetBlocks
$100,000
NetBlocks is a modular technology framework for transparent internet governance and real-time monitoring of network controls. The platform combines probe hardware, remote scans, and other data sources to provide an enhanced view of internet health that is aggregated and statistically analyzed in real-time with the goal of rapidly detecting interference affecting entire regions and populations, such as during periods of political unrest. NetBlocks is the technology project of Turkey Blocks, a network observatory which focuses on internet shutdowns and social network availability.

DG7 Internet Freedom Landscaping Report
$83,200
Many international broadcasting agencies produce content that is blocked or censored by repressive governments, raising the question of how to reach audiences living in these kind of environments. Inside different international media agencies there are teams or individuals working to overcome these challenges and find alternative solutions to make content available in repressive environments. Within this context, this landscaping report will examine and highlight the work that is currently being done by a number of broadcasting agencies to fight censorship and to advance freedom of expression among audiences. This provides a framework for further work to bypass censorship. The report aims to demonstrate the important role that these anti-censorship divisions can play by advancing the overall mission of their respective agencies in addition to contributing to the internet freedom and human rights ecosystem.

Freedom from Government Intimidation in Belarus
$64,890
For over 20 years, Belarusian citizens, and in particular human rights defenders, have been operating in an increasingly repressive environment. This project aims to increase the capacity building among the Belarusian journalists, human rights defenders, and civic activists to protect themselves from risks associated with digital communication, including unauthorized access to information and persecution on the basis of information retrieved by authorities via illegal access to sensitive information. The project seeks to create a new culture of following simple rules and codes of conduct to ensure security of information and increase the security of these targeted groups.

Sub Saharan-Africa Cyber Regionalism and Elections
$56,000
The project is carrying out a detailed comparative analysis of information controls in The Gambia, Rwanda, Angola, and Democratic Republic of Congo. The study focuses on understanding high-risk periods around elections in these countries with various forms of repressive governments.

MeasurementKit
$37,000
The project is enhancing the sustainability and cross-platform compatibility of the OONI-probe platform through improvements to MeasurementKit. It is focused on expanding the mobile version of specific tests to encompass all the testing occurring via desktop computers. This not only increases the types of tests being carried out on mobile networks but also streamlines the codebase to limit the amount of code upkeep for the OONI platform.

Journalists in Distress
$32,735
This project conducted a complete assessment of the digital security practices being used by the Journalists in Distress network, a group of free expression organizations that operate similar emergency response programs to help journalists and human rights defenders around the world. Through this six-month data collection, assessment, and knowledge sharing effort, the project allowed a transnational network of

organizations to comprehensively understand the state of its digital practices and the potential risks and vulnerabilities to the journalists and human rights defenders they help.

Privacy

Signal
$700,000
Open Whisper Systems (OWS) produces Signal, one of the leading encrypted mobile communication tools. OTF's support enabled the OWS team to continue providing Signal at no cost around the globe and adapt their operations for a growing user base. OWS also implemented a numeric fingerprint format to improve localization, reduce the likelihood of a false comparison, and improve the user experience for users not reliant on the Latin alphabet.

Cryptographic Engineering
$150,000
This project will improve the engineering quality of cryptographic protocols of select circumvention tools, and cultivate and mobilize the cryptographic engineering community to work on select protocols and frameworks. This is being carried out by improving the Signal & Noise protocols and the documentation and organizing of cryptographers through community management via the ModernCrypto mailing list, and bringing together fifty of the world's top crypto implementers through the High Availability Crypto Software (HACS) workshop.

Security

Subgraph OS
$125,000
Subgraph OS is a desktop operating system designed to be usable for non-technical users and secure against active interference and targeted attacks. It is specifically designed to protect targeted users at risk of identification and surveillance by determined and capable network-borne adversaries. This project is supporting an improved user experience and various security enhancements leading up to a beta launch.

Umbrella
$107,400
Umbrella is a mobile app that seeks to provide all the information needed for journalists, sources, human rights defenders, and other at-risk individuals to operate safely. With step-by-step processes for every situation from sending a secure email to an emergency evacuation, Umbrella will provide these individuals with a one-stop-shop for all the latest know-how of how to operate securely as, and when, they need it. It will provide users with how-to guides, risk assessments, and checklists (along with optional customization), allowing users to securely and anonymously save their settings and track their progress. Following OTF support for its creation, the second phase integrates a number of additional features, increases its availability in native languages, and improves the mobile usability.

NoScript
$100,000
NoScript is a popular privacy and security enhancing browser extension for Mozilla Firefox and is pre-installed in the Tor Browser. OTF support allows for the leveraging of the new Chromium-compatible WebExtensions API provided by Mozilla and the closely related standardization effort in the W3C Browser Extensions Community Group in order to make NoScript support other major modern browsers including Google Chrome.

Venezuela Internet Monitoring Project
$89,130
This technical project monitors the state of the internet in Venezuela, documenting cases of internet blocks and shutdowns, along with the underlying technical mechanisms to do so. The project has developed tools to easily identify and contextualize cases, which is useful to show and alert the public about the increase of information controls, and the state of the internet in Venezuela.

Rights Action Lab
$50,678

The Rights Action Lab is building the capabilities of three targeted Tibetan organizations to better respond to emergency response situations quickly and effectively. To achieve this, Rights Action Lab will focus on enhancing local capacity, creating needed infrastructure, and institutionalizing a digital security environment and culture. This work is being carried out in partnership with Citizen Lab.

Mailvelope
$121,000
Mailvelope is an open source browser plugin that allows users to utilize the OpenPGP standard to encrypt their webmail email services provided by companies such as Google, Yahoo!, and others. This project focuses on improving the user experience, adding stability to the code base, and simplifying the installation process.

Tor BSD Diversity Project
$40,000
The Tor BSD Diversity Project (TDP) is an initiative seeking to extend the use of the open source BSD Unix operating systems in the Tor public anonymity network. The project is helping to foster a stronger Tor network through increasing operating system diversity. TDP's efforts are focused on numerous ongoing issues, including straightforward documentation specifically focused on BSD systems, the development of relevant software, and the improvement of publicly available statistics around operating system usage for Tor relays.

Supporting People

Digital Integrity Fellowship
$375,282
The information controls landscape is constantly changing, creating an increasingly difficult challenge for small and medium-sized organizations to maintain up-to-date digital security and safety strategies and policies (if they have them in place at all). Fellows provide organizations and communities most affected by internet freedom violations comprehensive internal support with their digital security expertise. For short-term needs, the program serves as a mechanism of support to individuals working to mitigate urgent digital threats to vulnerable groups like journalists, bloggers, human rights defenders, NGOs, activists, and others. For long-term needs, the program strives to build digital security expertise inside organizations, within the local communities they are a part of, and the global networks that connect them. These long-term engagements provide critical insights to better understanding the usability and localization barriers that limit the adoption of tools designed to counter various digital threats. The lessons learned are communicated to developers in order to increase adoption and strengthen the feedback loop. OTF provided initial support to six fellows working in repressive environments around the globe, and partnered with seasoned digital security practitioners to provide mentorship and advice as these fellows carried out their respective projects.

DIFP Fellow working in Venezuela
The internet and other digital tools help activists and organizations in Venezuela achieve their goals, but they also open new vulnerabilities. Antagonists can take advantage of the general lack of technical knowledge of non-technical organizations to seriously curtail or monitor their activity without their knowledge. Previous efforts to attack this problems have sometimes erred by being too general, or by focusing solely on auditing, training, or implementing. This project will evaluate the digital security needs of selected small, non-profit, at-risk organizations; and improve the digital security strategies of the selected organizations through training and implementation.

DIFP Fellow working in Colombia
The indigenous communities and organizations that advocate for improved agricultural and environmental rights in rural Southern Colombia have been the victim of systematic violence against their members. These individuals and their networks have been physically and digitally targeted by military, paramilitary, and guerrilla forces. In 2015, nearly 20 of the movement's members were killed and several of their political authorities detained. To safeguard their activities, this fellowship works to train the networks on various digital security protection measures.

Dhyta Caturani
In Indonesia, the most common digital harassment faced by women and LGBTI activists are doxxing, outing, harassment, threats, impersonation, blackmail, account hacking, website blocking, honey trap, data capture, and even imprisonment under the cyber laws. In addition, with strict pornographic laws, the government blocks access to many sites that contain important and useful information on gender and sexuality. With the lack of knowledge and skill on circumvention, most people in the groups face difficulties finding the information and knowledge they need. This is particularly true for young people. The project equips highly at-risk LGBTI activists with the right knowledge and skills to protect themselves online, and can be expanded to other at-risk users as well.

Nighat Dad
Nighat conducted digital safety trainings to educate journalists and human rights activists around the country on how to secure their online presence and safely store information. These trainings also covered communications security, tactics for prevention of cyber-harassment, and how to avoid digital surveillance. Other topics included sensitization and awareness on digital security, computer and mobile phone hygiene (protecting devices from malware and spywares), and using social media with a privacy-by-default mindset.

Azeenarh Mohammed
The project carried out a holistic security training for the tight-knit group of organizations and individuals that comprise the at-risk LGBTQI network in Nigeria. This community network within Nigeria provides health services, advocacy, counseling, legal services, and other efforts to defend basic human rights. As a result, they collect and store lots of sensitive data about members of the LGBTQI community, their funders, and other organizations they work with. This can be problematic because of the likelihood of raids by state actors, and the risks are increasing with Nigeria's growing collection of surveillance technologies.

Natasha Msonza
In Zimbabwe, the rapid increase in digital threats and surveillance creates the need for mechanisms to provide constant support in the context of complex and shifting challenges. Natasha worked on strengthening and sustaining a local trainer's knowledge base in digital security and safety, and developing and implementing a strategic plan at six organizations to strengthen the digital resilience of at-risk organizations.

Supporting Usability and Design in Security Fellowship
$75,400
The Supporting Usability and Design in Security Fellowship aimed to cultivate applied research, knowledge-building outputs, tangible improvements to open-source tools, and creative collaboration at different levels and across institutions on the topic of usable security, especially the usability of open-source secure-communication tools. The fellowship's host organizations included Simply Secure and University College London. At the end of 2016, OTF retired this fellowship program given the continued infancy of this unique field. OTF nonetheless gained an understanding that the best means of supporting those with relevant experience is through having them respond to the program's call for Usability Lab service partners.

Ruba Abu-Salma
Ruba Abu-Salma is a Ph.D. student in the Department of Computer Science at University College London (UCL) in the UK. Her research focuses on taking a user-centered approach to the design and use of secure communications. During her fellowship, Ruba is working towards creating foundational knowledge for the design of communication tools that support secure group chat in line with users' needs, mental models, perceptions, and computer security practices.

Yasmina López
Yasmina López is a service designer with a strategic mindset. As a senior fellow, Yasmina is collaborating with OTF and Simply Secure to conduct a yearlong research study. The initiative will introduce and train designers and developers who build internet freedom tools to the human-centered design methodology. By using this methodology in their development processes, they will be able to design more effective, usable, and useful tools for Internet Freedom.

Information Controls Fellowship

$256,800

The Information Controls Fellowship Program (ICFP) aims to cultivate research, outputs, and creative collaboration at different levels and across institutions on the topic of information controls—specifically examining information controls such as internet filtering, blocking, throttling, and surveillance, as well as the technical systems that enable or undertake all of the above to the detriment of internet freedom. OTF works with a multitude of host organizations for the fellowship ranging from prominent academic institutions to accomplished advocacy groups. After receiving nearly 100 applications, OTF selected six fellows in its third round of ICFP whose research spans much of this field (Selections for 2017 fellows are nearly complete and will be announced on OTF's website.)

Serene Han

Serene collaborated with University of Berkeley's International Computer Science Institute to advance the Snowflake pluggable transport through increased development and deployment. Snowflake lowers the costs and increases the usability of circumventing censorship in many highly repressive environments. At the conclusion of her fellowship, Snowflake was deployed in the Tor Browser.

Geoffrey Alexander

Geoff is working with Citizen Lab at the University of Toronto to develop new methods and tools for investigating malware enabled espionage operations against targeted actors like journalists and civil society groups. This project leverages the data resources of Citizen Lab to study malware campaigns and develop automated methods for analyzing, detecting, and tracking both the malware and the command and control infrastructure used to target these at risk communities.

Grace Mutung'u

Grace is working with the Berkman Klein Center at Harvard University to perform an analysis and publication of a report on freedom online in the Uganda elections of 2016, monitor information controls applied by the Kenyan government, and the analysis and publication of a report on freedom online in the Kenyan elections of 2017.

Daniel Riofrio

Daniel is being hosted by the University of New Mexico to work closely with Ecuadorian groups studying the characteristics of past DoS attacks and mitigate future attacks to limit participation during the Ecuadorian electoral year. This includes working closely with UNM to perform a content analysis of twitter accounts and activists' websites to measure content blocking, "sockpuppet" accounts, and DoS attacks.

Claudio Agosti

Claudio is working with Coding Rights to advance understanding around how advertising networks are being exploited by malicious actors. This project provides a deeper understanding of the threats these networks pose to at-risk populations. This builds on the applicant's existing work in this area and will serve as a critical public resource to both researchers and everyday users.

Diego Bravo

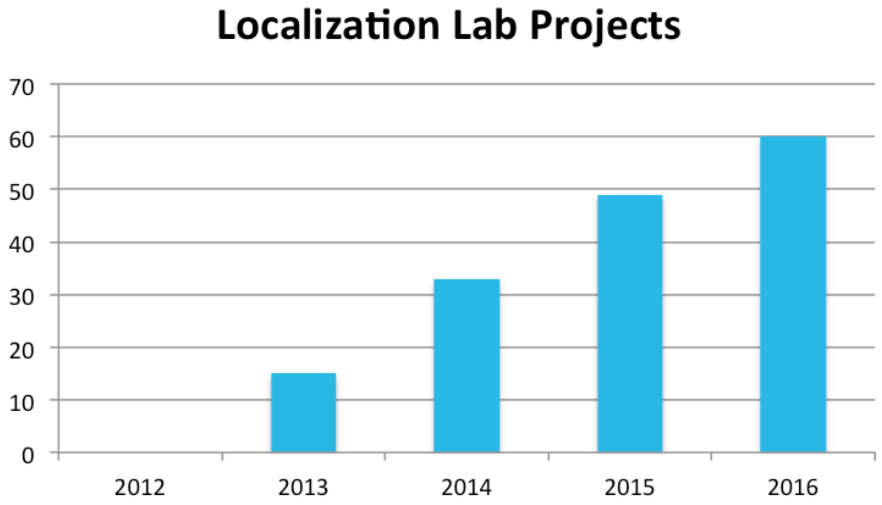
As a seasonal Information Controls fellow, Diego worked with University of Toronto's Citizen Lab over the summer of 2016 to contribute to their security analysis of popular browsers. Many browsers widely used in repressive environments fail to protect their users. Diego also developed a tool to analyze an Android application to look for hardcoded encryption keys.

Provided Services - OTF Labs

Localization Lab

$574,960

OTF's Localization Lab makes internet freedom tools relevant and usable to local conditions and local users. Prohibitive costs and limited availability of professional translators can prevent global deployment of internet freedom tools. To address these challenges, OTF supported the creation and growth of the localization hub, built with the help of Transifex. The management and cultivation of the hub were performed by Localization Lab. By the end of 2016, the hub included 60 projects with more than 5,400 participating volunteers contributing to the submission and verification of well over a half million translated words into over 200 languages and dialects including Arabic, Farsi, Korean, Tibetan, Mandarin, Spanish, Ukrainian, and Vietnamese.



Engineering Lab

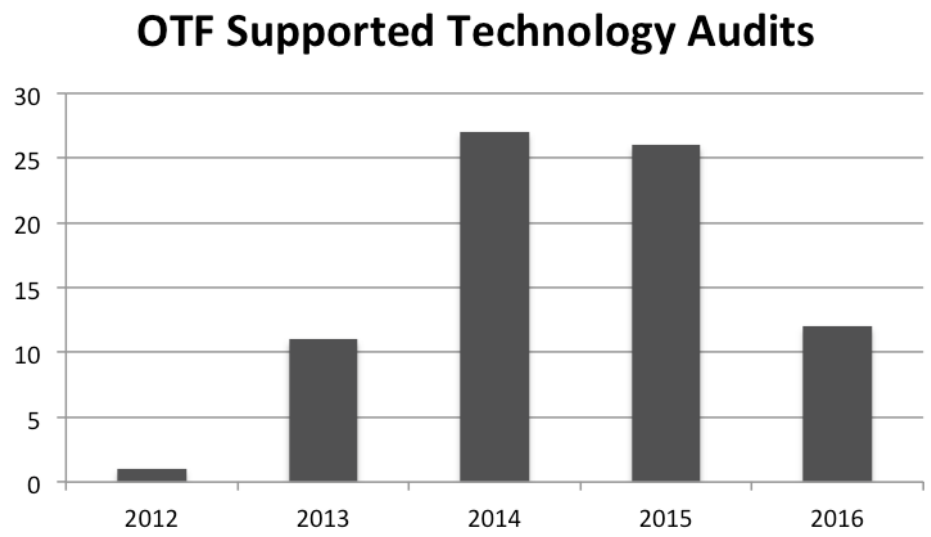
$164,478

The Engineering Lab includes Eclipsis, OTF-supported Secure Cloud Infrastructure, Amazon Cloud credits, Google Apps credits, and other engineering resources frequently needed by projects. Working with partners on the ground, OTF deploys high-capacity cloud infrastructure for use as close as safely possible to high-censorship areas in the Middle East, Northern Africa, and Asia. Once deployed, access is given to both OTF and non-OTF projects to research, develop, and deploy their tools and services in a secure environment. The result is greater access and lower overhead for projects. The Engineering Lab has witnessed significant growth with well over 100 projects utilizing Eclipsis in 2016 and dozens of others applying for other Engineering Lab services.

Red Team Lab

$650,000

The Red Team reflects OTF's commitment to establishing high standards for internet freedom technology to safeguard users in at-risk communities. One component of this commitment is conducting independent technology audits on all OTF technology-centric projects with the goal of finding and fixing vulnerabilities before illicit actors and repressive governments exploit them. These audits mitigate the risk inherent in funding cutting-edge technologies and strengthen the technical capacity of the project and the broader community of human rights and internet freedom technology developers. OTF currently offers in-kind audits to crucial non-OTF-supported internet freedom and human rights technology projects used in the field. Despite ever growing demand, the program reduced the number of audits performed due to the need to prioritize the auditing of projects being funded directly by OTF and limited funding.



Community Lab

$482,842

Community Lab brings together and strengthens the internet freedom community through initiatives cultivating deeper cooperative and collaborative relationships, improving knowledge sharing, taking advantage of synergies, and increasing diversity as more at-risk communities come online and under threat. As the internet freedom community grows, so do the needs and challenges that must be solved with community-wide strategies bringing to bear collective vision and action, and properly working beyond cross-cultural barriers. Community Lab generates and shares intelligence about the state of various segments of the field, enabling OTF and other internet freedom funders to better understand the ecosystem while gaining insight into where and how to target further investments. In 2016, the Community Lab supported the OTF Summit, Localization Summit, Internet Freedom Festival, Iran Cyber Dialogue, IF Comms Summit, Rightscon, Citizen Lab Summer Institute, and the Forum on Internet Freedom in Africa. In addition, the Lab provided community management consultation to various networks. Notably, the OTF Summit, which brings together OTF-funded projects and fellows, was the largest and most diverse version to-date. The Internet Freedom Festival, considered one of the largest and most inclusive events of its kind, brought together more than 1,200 people from 114 countries, featured over 220+ sessions and over 60 partners, and resulted in various collaborative projects and the sharing of important regional and technological knowledge.

Usability Lab

$0

There are many open-source software projects that aim to help journalists, activists, and ordinary citizens around the world communicate securely. Unfortunately, too few of these software development teams have the research expertise or design support to make tools that are easy enough to use by the majority of at-risk communities. These usability challenges hamper the widespread adoption of these tools. More critically, these challenges sometimes lead to user misconception about tools, which can give users a false sense of security and expose them to even greater risk. As a response, OTF created the Usability Lab to connect technology-centric projects with service providers capable of providing usability audits and advice that improve the overall user-friendliness and success of internet freedom and human rights technology. In 2016, Usability Lab partnered with Simply Secure to provide usability audits to help analyze and identify any pitfalls that might make it difficult for an average user to successfully use the audited internet freedom tool. Usability Lab also continued to support widely used circumvention tools such as I2P, and helped the Tor Project create a style guide that helps the project's developers and UX designers maintain a consistent and usable tool in order to build trust. In 2017, the Lab will seek to expand its services to better support the community as well as improve knowledge sharing around specific usability challenges facing internet freedom tools.

Legal Lab

$0

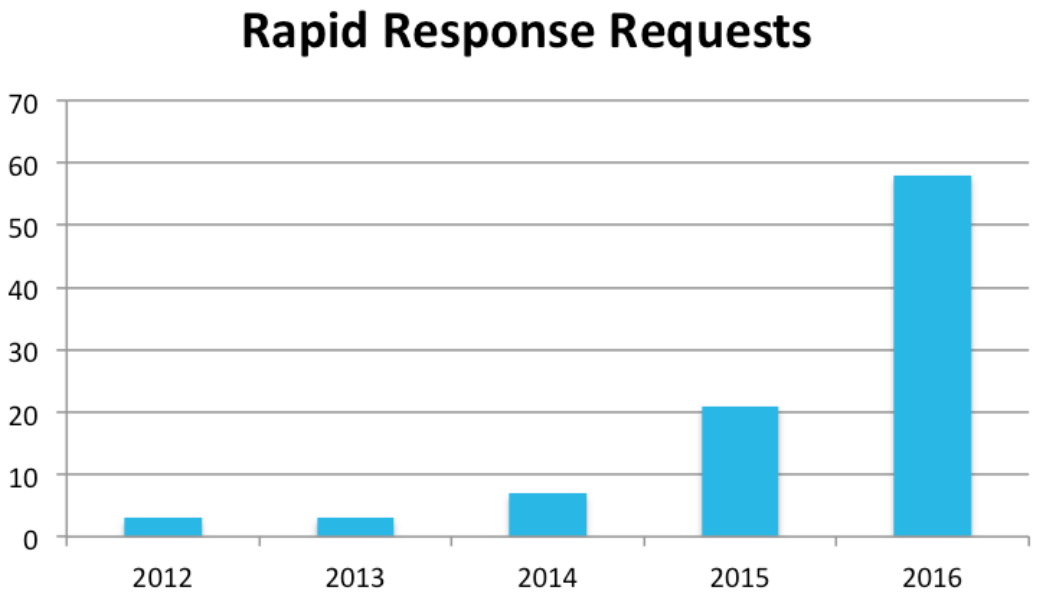
Legal Lab provides assistance for various legal issues unique to internet freedom projects in all stages. During the life of any project, a variety of legal questions can arise related to incorporation, IP issues, export laws, regional policy restrictions, mandatory Terms and Conditions, etc. The OTF Legal Lab connects internet freedom projects to legal professionals with relevant expertise at the Cyberlaw Clinic at Harvard Law School.

Rapid Response Fund

$199,400

The Rapid Response Fund is a broader initiative which facilitates the development of a strong digital emergency response community that can work together to resolve threats in a timely and comprehensive manner. In 2016, OTF provided emergency support for a variety of digital emergencies experienced by high-risk internet users and organizations, such as journalists, bloggers, cyber activists, and human rights defenders. OTF offers a permanently open application window to ensure it can act quickly when emergencies arise.

OTF's rapid response service providers offer assistance with secure and resilient hosting, website audits, forensic analysis of digital attacks, infrastructure improvements, and VPN services. The majority of support provided through these partners is in small (>$5,000) increments. Nonetheless, OTF provided direct support to numerous projects while staying below the $50,000 limit OTF has set for this Fund. The Rapid Response Fund has been utilized by entities around the globe, including those focused or residing in Azerbaijan, Angola, Bahrain, China, Colombia, DRC, Ethiopia, Gambia, Mexico, Myanmar, Pakistan, Sudan, Thailand, Tibet, Zimbabwe, and many others.[67] A few of these projects that can be discussed publicly are detailed below the following chart.



Online Harassment Hotline

$25,000

Digital Rights Foundation (DRF) founded the first 24/7, free, and confidential support service for anyone experiencing online harassment in Pakistan. They focus on four main program areas: User Support, Safety Planning and Technical Assistance, Navigating Tech Platforms and Policies, and Strengthening Networks.

[67] For more information on other countries and regions where OTF has provided rapid response assistance, please review previous annual reports.

Measuring Network Interference in Ethiopia During Political Processes

$3,000

Despite media and citizen reports on the intermittent targeted internet shutdowns in Ethiopia, there still is not enough credible evidence to support effective circumvention or advocacy campaigns. This contract gathered credible technical measurements on network interference in Ethiopia as part of wider reporting on internet shutdowns during political protests happening in the East African country.

Mesh Networking in Colombia

$5,000

Afro-Colombian and rural communities in Colombia are under frequent surveillance for their efforts to promote their rights. Organizations in this environment are often faced with limited connectivity to mobile networks, making it extremely difficult to communicate and organize with one another safely. This project creates a mesh network with local civil society that will allow the creation of secure digital practices in the field with its members. The mesh network allows for the updating of community websites, carrying out digital security trainings with members and secure communication with the outside world. The mesh network will also be used to connect smartphones through secure applications to make sure community members can safely communicate.

Collecting network measurements in the Gambia & DRC

$4,050

This rapid response project gathered credible technical measurements on network interference in The Gambia and the Democratic Republic of Congo, allowing civil society and other pro-democracy activists to push back against the increasing authoritarianism taking place on the internet in these countries.

Expenses Breakdown

Direct Support	**$ 4,397,005**
- *Projects*	*$ 3,490,123*
- *Access*	*$ 1,052,300*
- *Awareness*	*$ 954,615*
- *Privacy*	*$ 850,000*
- *Security*	*$ 633,208*
- *Fellowships*	*$ 707,482*
- *Rapid Response*	*$ 199,400*
Indirect Support (Labs)	**$ 1,872,280**
- *Red Team*	*$ 650,000*
- *Engineering*	*$ 164,478*
- *Community*	*$ 482,842*
- *Localization*	*$ 574,960*
Total Salaries and Benefits (6/16-2/17)	**$ 937,322**
OTF Administrative	**$ 114,836**[68]
RFA Administrative	**$ 74,936**
Travel	**$ 103,621**

FY2016 Total Expenditure	**$ 7,500,000**
Carryover from FY2015	**$ 0**[69]
FY2016 Budget	**$ 7,500,000**

Total Budget	**$ 7,500,000**

[68] The primary cost associated with this line item is maintaining and continuously improving OTF's proposal system, which seeks to increase the accessibility of applying for support.
[69] Given the reductions in annual funding, escalating levels of internet censorship and large number of submissions, OTF was unable to allocate any FY2015 funds for FY2016.

Looking to the Future

U.S. Government Support

As noted above, OTF has witnessed a significant decline in financial support in recent fiscal years. The budget reductions to date have harmed the program's ability to support the rapidly growing community of people committed to addressing the increasing array of digital interference techniques and threats around the globe. As a recipient of U.S. government funds through a grant to RFA, OTF is restricted in advocating for the benefits and impact of the program to those determining internet freedom funding levels. Nonetheless, the program will continue to identify means to highlight the growing importance of this funding and the tremendous disparity in financial and personnel resources invested by the U.S. government as compared to the high levels used by repressive governments to continually adopt, adapt, and advance information controls.

Diversifying Funding Pool

OTF has made significant strides in increasing support for internet freedom from sources outside of the U.S. government. Given the reductions in internet freedom funding discussed above, this work is more important now than ever before. In 2014, OTF experienced a significant uptick in interest from a variety of funders, and 2015 and 2016 were no different. Numerous private foundations continue to make internet freedom causes a primary focus. Globally, democratic governments continue to adapt existing sources of funding to address the growing importance of digital security.[70] Venture capitalists are also increasingly interested in these areas including security, privacy, and more fundamentally, decentralization.[71] This widespread attention has the potential to foster innovative new tools for at-risk communities.

Increasing Public Information

In OTF's 2012 annual report, the program committed to setting a new standard of transparency and open data for internet freedom technology funders. The OTF team has made good on many of these commitments, including disclosing extensive information on what OTF has funded, and maintaining an always open competitive application process, while soliciting and responding to public feedback. OTF has not exposed aggregate data on the applications, a formal document describing the metrics OTF uses to evaluate applications, or a monitoring and evaluation framework (with data) for measuring the outcomes of supported efforts. In 2017, the OTF team will advance these efforts with the development of a responsible data policy to ensure OTF safely releases as much data on the program's past five years as possible.

Looking to the Front-lines

OTF prioritizes efforts working closest to those directly experiencing internet freedom repression. Each year, applicants trend towards those creating solutions on behalf of a front-line group, or those creating solutions from within front-line groups. This is a trend OTF supports. In 2012, the program launched the Localization Lab to make it easier for efforts with multi-lingual communities to localize and translate their tools. In 2014, the program launched the Community Lab, Digital Integrity Fellowship, and a formal Rapid Response Fund in response to needs from the field, to give clearer on-the-ground insights and enhance OTF's technology-centered decisions. OTF will continue to support and evolve these initiatives as they continue to:

- Increase OTF's exposure to new, larger, and more diverse communities of technologists;
- Grow the body of knowledge informing how to decide which technologies to support; and,
- Allow for even better measurement of OTF's decisions through the experiences of those most affected.

To date, the result has been support for better technology with a more sustainable impact. In 2017, OTF intends to become even more relevant to the growing number of global technologists by engaging more

---

[70] *See, e.g.*, Lucian Armasu, "European Parliament Doubles Budget For 'Free' Software Audit and Bug Bounty Projects," *tom's Hardware*, December 1, 2016, http://www.tomshardware.com/news/eu-software-audit-bug-bounty,33123.html.

[71] *See, e.g.,* Jon Russell, "Stealth startup Privacy Labs raises $4M to give consumers 'control' of their data, *TechCrunch*, February 23, 2017, https://techcrunch.com/2017/02/23/privacy-labs/; Michael J. de la Merced, "Digital Security Provider, CrowdStrike, Raises $100 Million," *New York Times*, May 17, 2017, https://www.nytimes.com/2017/05/17/business/dealbook/crowdstrike-hacking-investment.html; Zavain Dar, "Investing in a Decentralized Web: Announcing Lux's Series A Investment in Blockstack," *Medium*, January 8, 2017.

partners to hone the program's diversity and inclusion efforts, further improve the localization of OTF's website, and implement changes to the program's application process to make applying to OTF more approachable for front-line groups.

Evolving the Application Process

Since 2012, OTF has utilized the same core workflow on the same application system: an always open to the public application form, where all approved applications are reviewed by an all-volunteer Advisory Council, providing extensive feedback to all applicants regardless of outcome. In 2012 OTF reviewed fewer than a dozen applications. Now, the program reviews more than 50 applications each month. In addition, OTF has received numerous suggested improvements from the field including: collaborative applications that allow for more more than one applying individual or entity; more multi-lingual support; the ability for peer and public review of applications, in addition to Advisory Council review; a streamlined application for those requesting smaller amounts of money; and the ability to aggregate application trends. In 2017, OTF will make as many of these available as possible. The OTF team will start by updating, modernizing, and fully open-sourcing the program's application system to make inclusion of these new features possible and address the increase of applications. By 2018, OTF hopes to have an application system capable of keeping pace with the innovations and needs of the field.

Core Infrastructure Fund

In 2015, OTF recognized that a number of internet freedom projects had become core components of multiple other internet freedom technologies. These projects are now core building blocks of everyday internet freedom tools, requiring alternate criteria for evaluation and support mechanisms. Notably, the target user for a Core Infrastructure project is often not an end-user, but rather a developer of end-user tools. Every year, OTF sees more technologies moving into this realm and more applications to OTF for their support. In 2017, the program continues to collaborate with other sustainers of these technologies to further refine OTF's criteria, leverage their support into the internet freedom field, and evolve OTF's support mechanisms to align with their needs. OTF will further refine the Core Infrastructure Fund application to better suite these technologists, and augment the program's Engineering Lab to support those existing service providers who are already regularly providing these technologies to makers of end-user tools.

Challenges Ahead

The various methods of restriction and censorship described in this report have already evolved and proliferated in 2016. The world is witnessing a rise in internet and app-specific shutdowns, knowledge and resource-sharing between repressive governments, data localization demands on intermediaries, growing sophistication of digital attacks, and other new methods of censorship. Each year, the increase in human resources and financial investments by those opposing Article 19 of the Universal Declaration of Human Rights dramatically affects those seeking internet freedom. The opponents have clearly and openly stated their priorities, demonstrating their dedication to further the development, sophistication, and expansion of repressive censorship mechanisms.

OTF responds by reaffirming the program's unremitting commitment to resist these efforts, by supporting the people and projects working to defend internet freedom. In this effort, OTF will continue to evolve and anticipate technological advancements, defend against injurious social or regulatory change, and circumvent repressive restrictions as long as threats against human rights, open societies, and internet freedom persist.

Appendix

The OTF Team in 2016

Lindsay Beck
OTF Senior Program Manager, RFA
Ms. Beck joined RFA in June 2014. As senior program manager, she is actively engaged in OTF's day-to-day operations and long-term planning. She manages numerous directly funded projects, OTF's Localization Lab and Usability Lab, and the Digital Integrity and Secure Usability Fellowship programs.

Bernadette Mooney Burns
General Counsel and RFA Board Secretary, RFA
Ms. Burns has been RFA's General Counsel since 2006, and was elected board secretary in 2008. She serves as the chief legal advisor for all RFA operations, programs, and initiatives, including OTF, and performs legal review ensuring compliance with applicable laws and regulations.

Chad Hurley
OTF Director of Technology, RFA
Mr. Hurley joined OTF in November 2014 as director of technology after serving at RFA for many years. He actively reviews technical aspects of proposals, leads the Red Team and Engineering Labs, and acts as OTF's internal technology and security expert.

Esther Lim
OTF Senior Program Manager, RFA
Ms. Lim joined RFA in November 2014. While at OTF she served as a senior program manager, actively engaging in the day-to-day operations of OTF. Among her many responsibilities, she headed the Legal Lab, led outreach with private sector companies, and managed a portfolio of funded projects. Ms. Lim departed OTF in mid-2016.

Libby Liu
President, RFA
Ms. Liu provides strategic and operational direction to OTF as it supports the development of global internet freedom tools. In addition to directing operational policies and procedures, she coordinates issues in these areas with the BBG, the International Broadcasting Bureau, other associated entities, and outside stakeholders. Ms. Liu performs executive review following the financial, legal and compliance reviews of all OTF-recommended proposals prior to contracting.

Adam Lynn
OTF Interim Deputy Director, RFA
Mr. Lynn joined RFA in April 2012 as OTF's inaugural program manager. He serves as interim deputy director. In 2016, he managed OTF's programmatic operations while leading OTF's research initiatives including the Information Controls Fellowship program.

Rohit Mahajan
Director of Public Affairs and Digital Strategy, RFA
Mr. Mahajan joined RFA in 2009. As director of public affairs and digital strategy, he is responsible for overseeing OTF's press outreach and public image. He manages communication with a multitude of external audiences and leads OTF's efforts to educate the public about OTF's program and projects.

Dan McDevitt
Communications and Outreach Coordinator, RFA
Mr. McDevitt joined RFA in December 2014 as the communications and outreach coordinator. His responsibilities include coordinating press relations efforts, increasing OTF's social media presence, tracking OTF-related press, and compiling the daily *OTF Today: News Related to internet freedom*.

Dan Meredith

OTF Principal Director, RFA

Mr. Meredith joined RFA in January 2012 as OTF's inaugural team member and director. He now serves as principal director. He is responsible for OTF's day-to-day operations and long-term planning, OTF's role in the internet freedom community, work with outside funding partners, coordination with other internet freedom technology implementers and stakeholders, and fostering of technology collaboration.

Denna Millet

OTF Program Manager, RFA

Ms. Millet joined RFA in October 2014 as a program manager with OTF. While at OTF, she was responsible for day-to-day program management, Rapid Response Initiatives, MENA and focused projects. She also served as a liaison to the Director General 7. Ms. Millet departed OTF in mid-2016.

Sandy Ordonez

OTF Director of Outreach & Community, RFA

Ms. Ordonez joined RFA in April 2015. As director of outreach & community, she is responsible for shepherding OTF's outreach efforts, managing the OTF Community Lab, and helping grow and diversify the internet freedom community.

Richard Smith

Budget Director and RFA Board Treasurer, RFA

Mr. Smith is responsible for advising RFA and OTF on matters related to contracting and operating budgets. His duties include the development of annual and multiyear budgets and financial plans, contract reviews, analysis of the fiscal impact of legislation, playing a central role in the annual budgeting process, and performing a financial review and compliance assessment of each project before contracting occurs.

OTF's Advisory Council

OTF's volunteer Advisory Council members assist with OTF's unique and highly technical due-diligence needs to ensure a comprehensive and holistic proposal evaluation process. Members of the Advisory Council give OTF a deeper understanding of current internet freedom challenges and opportunities, review project proposals, and assist in shaping the collaborative and collective work of the OTF program.

As the landscape defining internet freedom evolves, so does the expertise of the Advisory Council. Today's council brings experience in numerous areas of research, development, and disciplines. OTF maintains multiple panels where Advisory Council members review applications for specific funds and fellowships.

Since early 2016, the following individuals have joined the OTF Advisory Council: Frerieke van Bree, Daniel Kahn Gillmor, Matt Michell, Roya Ensafi, Leigh Honeywell, Bernard Tyers, Karen Renaud, Carrie Winfrey, Susan Farrell, and Jared Spool. Below is the current membership of the Advisory Council:

John Adams, *Independent Security Consultant*
J. Ayo Akinyele, *Research Scientist*
Collin Anderson, *Independent Researcher*
Kevin Bankston, *Policy Director, New America Foundation's Open Technology Institute*
Gustaf Björksten, *Technology Director, Access*
Wojtek Bogusz, *Digital Security Consultant*
Matt Braithwaite, *Google*
Frerieke van Bree, *Program Manager Digital Defenders Partnership, Hivos*
Cory Doctorow, *Author, Journalist, and Activist*
Alix Dunn, *Executive Director and Co-Founder, the engine room*
Peter Eckersley, *Technology Projects Director, Electronic Frontier Foundation*
Nadia Eghbal, *Investor, Social Researcher*
Roya Ensafi, *Postdoctoral Researcher*
Susan Farrell, *Senior User Experience Specialist, Nielsen Norman Group*
Joana Varon Ferraz, *Independent*
Michael Geist, *Law Professor, University of Ottawa*
Daniel Kahn Gillmor, *Senior Staff Technologist, ACLU*
Matthew Green, *Assistant Professor, Dept. of Computer Science, Johns Hopkins University*
Leigh Honeywell, *Senior Staff Security Engineer, Slack*
Gunnar Hellekson, *Chief Strategist, Red Hat*
Nadia Heninger, *Computer and Information Science, University of Pennsylvania*
Anthony D. Joseph, *University of California at Berkeley*
Zane Lackey, *Founder, Signal Sciences*
Ben Laurie, *Software Engineer and Crypto-plumber, Google*
Katherine Maher, *Interim Executive Director, Wikimedia Foundation*
Moxie Marlinspike, *Institute For Disruptive Studies*
Mohammed Al-Maskati, *Digital Security Consultant, Front Line Defenders*
Susan McGregor, Assistant Director, *Tow Center for Digital Journalism*
Andrew McLaughlin, *betaworks / Berkman Center for Internet & Society*
Haroon Meer, *Founder, Thinkst*
Stefania Milan, *Assistant Professor of New Media and Digital Culture, University of Amsterdam*
Matt Mitchell, Researcher
Mohamad Najem, *Advocacy and Policy Director, Social Media Exchange*
Bryan Nunez, *Program Officer at Open Society Human Rights Initiative*
Tanya O'Carroll, *Adviser on Technology and Human Rights, Amnesty International*
Kavita Philip, *Associate Professor of History at the University of California, Irvine*
Emily Ratliff, *Senior Director of Infrastructure Security, Linux Foundation*

Karen Renaud, *Usable Security & Privacy Lead, School of Computing Science, University of Glasgow*
Dr. M. Chris Riley, *Head of Public Policy, Mozilla*
Bruce Schneier, *Security Technologist and Author*
Ian Schuler, *CEO, Development Seed*
Jared Spool, *Founding principal of User Interface Engineering*
Sanne Stevens, *Program Officer, Hivos*
Bernard Tyers, *Interaction Designer and User Researcher*
Meredith Whittaker, *Founder and Lead, Open Research Group, Google*
Carrie Winfrey, *Design Strategist and User Experience Designer*