OPEN TECHNOLOGY FUND

2015 Annual Report

Open Technology Fund

Executive Summary

The Open Technology Fund's ("OTF") fourth year of operation will be remembered by the staggering increase of people adopting technologies the program incubated.[1] With the rapid expansion of everyday digital usage, the BBG's ability to "Inform, Engage and Connect" people around the world in support of freedom and democracy is dependent on our ability to have unrestricted access to a free and open internet. At the close of 2015, the program received the highest level of support requests to date. Consequently, OTF supported more efforts than in any previous year. These efforts significantly increased internet freedom globally, as measured by the number of people able to experience a more open, secure internet, and by advancing emerging technologies and techniques. They did so in the face of more sophisticated online censorship than ever seen before. The year began with millions of people utilizing OTF supported technologies, and ended with over a billion.

Despite these gains, global internet freedom remains under threat with a widening gap in resources compared to the exorbitant amounts spent by repressive regimes to prevent access or otherwise threaten internet freedom. Sophisticated attacks continue to increase on those who seek to exercise their basic rights in repressive environments. In 2015 there was a tightening of censorship in countries such as Russia, Turkey, Bangladesh, Uganda, Colombia, Belarus, and China, which developed new and aggressive censorship capabilities for its Great Firewall, as instances of internet censorship rose globally for the fifth year in a row.[2] In response, OTF has continued its support of technology-centric efforts that increase global internet freedom.

OTF projects have made notable technological advances that ensure a resilient open internet, including 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 users from digital attacks. The OTF team reviewed and responded to nearly 450 requests for funding totaling close to $50 million in 2015 alone, and expended nearly 80 percent of our program budget on direct and indirect support for well over 100 projects.[3]

We listened to the field and communities most at risk, leveraging their collective knowledge and capacities to change with their needs. OTF Labs -- our in-kind, and technical assistance programs -- were adjusted and expanded as required. Our fellowship evolved to focus on the hyper-local needs of communities under threat, to harness their collective knowledge and capacity, and to promote the research and collaboration of individuals.

Finally, pursuant to OTF's congressional mandate to leverage government funds to the greater internet freedom effort globally, OTF helped other donors unlock nearly 100 million dollars of private funds to support these efforts since its creation four years ago.[4]

---

[1] This annual report covers the expenditure of OTF's remaining FY2014 funds and all FY2015 funds. These activities occurred from Winter 2015 until Spring 2016.

[2] Freedom House. "Privatizing Censorship, Eroding Privacy: Freedom on the Net 2015." October 2015. https://freedomhouse.org/report/freedom-net/freedom-net-2015

[3] This number 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] S.2130 - An Act Making Appropriations for National Security and for Other Purposes, Fiscal Year 2016
114th Congress (2015-2016), Global internet freedom Sec. 7078. (a) https://www.congress.gov/bill/114th-congress/senate-bill/2130/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 2015

This past year saw a number of disturbing developments in the global battle for online freedom, as authoritarian powers worldwide sought to further control their citizens both online and offline. Freedom of opinion and expression were blithely smothered by repressive governments disregarding human rights worldwide. People in more than 40 countries were detained by authorities for sharing information concerning politics, religion or society.[5] Of the global online population, 61 percent live in countries that actively censor criticism of the ruling powers.[6]

Among the worrisome trends in 2015: a crackdown on anti-censorship and privacy-enhancing technologies like Tor in Russia[7] and Belarus,[8] where it is relied upon by netizens to access unbiased news and information; increasingly advanced and adaptive malware campaigns targeting the Tibetan diaspora,[9] the development of a mobile messaging app by Iran's paramilitary militia to increase its surveillance capabilities on citizens;[10] the announcement of plans to increase social media censorship in Uganda;[11] and, notably, the launching of what might be the world's first-ever offensive censorship weapon by China, dubbed "The Great Cannon."[12]

The above is just a sampling of the numerous and novel ways censorship is expanding around the world. As repressive powers increasingly prevent the internet from being a platform for free expression, the importance of supporting technologies that protect and empower grows ever greater. Johns Hopkins University professor and cryptographer Matthew A. Green recently summarized the current landscape: "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."[13] Reviewing some of 2015's most significant censorship events lends credence to this assertion:

Censorship: A Lucrative Business

In August, Italian spyware vendor Hacking Team was itself hacked, with subsequently leaked documents revealing the ostensible 'cybersecurity' firm's sale of surveillance technology to authoritarian governments with histories of human rights abuses worldwide. Hacking Team's government clients included Ethiopia, Azerbaijan, Sudan, Uzbekistan, Nigeria, Bahrain, Saudi Arabia,[14] Morocco, and the United Arab Emirates.[15] The Hacking

---

[5] Freedom House. "Privatizing Censorship, Eroding Privacy: Freedom on the Net 2015."

[6] Ibid.

[7] Meduza. "The Russian government hired people to hack the Tor browser, but they failed and now they're quitting." Meduza. September 9, 2015. https://meduza.io/en/news/2015/09/09/the-russian-government-hired-people-hack-the-tor-browser-but-they-failed-and-now-they-re-quitting

[8] Tetyana Lokot. "Belarus Bans Tor and Other Anonymizers." Global Voices. February 25, 2015. https://globalvoices.org/2015/02/25/belarus-bans-tor-and-other-anonymizers/

[9] Katie Kleemola, Masashi Crete-Nishihata, and John Scott-Railton. "Tibetan Uprising Day Malware Attacks." Citizen Lab. March 10, 2015. https://citizenlab.org/2015/03/tibetan-uprising-day-malware-attacks/; Franceschi-Bicchierai, Lorenzo. "Hackers Target Tibetans With Malicious Google Drive Files." Motherboard. June 16, 2015. https://motherboard.vice.com/read/hackers-target-tibetans-with-malicious-google-drive-files

[10] International Campaign for Human Rights in Iran. "New Messaging App by Iran's Basij Militia Gives State Access to All Conversations." Global Voices Advocacy. May 27, 2015. https://advox.globalvoices.org/2015/05/27/new-messaging-app-by-irans-basij-militia-gives-state-access-to-all-conversations

[11] Netizen Report Team. "Netizen Report: Uganda Vows to Step Up Online Censorship." Global Voices Advocacy. October 21, 2015. https://advox.globalvoices.org/2015/10/21/netizen-report-uganda-vows-to-step-up-online-censorship/

[12] Bill Marczak (Lead), Nicholas Weaver (Lead), Jakub Dalek, Roya Ensafi, David Fifield, Sarah McKune, Arn Rey, John Scott-Railton, Ronald Deibert, Vern Paxson. "China's Great Cannon." Citizen Lab. April 10, 2015. https://citizenlab.org/2015/04/chinas-great-cannon/

[13] Groll, Elias. "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/

[14] Kopstein, Joshua. "Here Are All the Sketchy Government Agencies Buying Hacking Team's Spy Tech." Motherboard. July 6, 2015. https://motherboard.vice.com/read/here-are-all-the-sketchy-government-agencies-buying-hacking-teams-spy-tech

[15] Citizen Lab. "Hacking Team leak highlights Citizen Lab research." Citizen Lab. August 6, 2015. https://citizenlab.org/2015/08/hacking-team-leak-highlights-citizen-lab-research/

Team revelations show the many millions foreign governments are willing to spend on repressive censorship and surveillance; single iOS exploits and zero-days were sold for hundreds of thousands of dollars.[16]

Bangladesh: Murdered Bloggers and Mass Censorship

At least five bloggers and publishers were murdered in Bangladesh in 2015 for expressing their views online.[17] An increasingly violent extremist movement is openly encouraging violence against anyone who exercises their right to free speech online and endorses secular views, with a blogger "hit list" openly available online.[18] These murders are carried out in brutal fashion, as bloggers have been hacked to death with machetes.[19]

The Bangladeshi government also sought to quell public discontent via mass censorship on multiple occasions. In January 2015, the Bangladeshi government blocked the messaging apps Viber and Tango amid ongoing anti-government protests that had already seen nearly 30 people killed.[20] Months later, the government crackdown intensified, as a social media blackout saw the blockages of Facebook, Instagram, WhatsApp, and Viber for several weeks.[21] In response, Bangladeshis turned to circumvention tools including Tor, which saw a 380 percent spike in usage.[22]

China: Circumvention, Suppression, and The Great Cannon

China started 2015 by carrying out a "man-in-the-middle" attack on Microsoft Outlook users[23] before moving to block previously reliable VPN services,[24] plugging what had been a viable hole in the Great Firewall. Chinese authorities then deleted more than 60,000 online accounts as part of a "censorship sweep," conducted to remove posts that were considered to be "misleading" or "rumor mongering", according to the Cyberspace Administration of China (CAC).[25] China blocked over 50 websites for 'inciting panic' after a huge chemical explosion rocked Tianjin,[26] cut service to people using circumvention technology in Xinjiang province,[27] and moved to implant government censors inside private internet companies.[28] The government subsequently arrested more than 15,000 people in a campaign called "Cleaning the internet" and imposed numerous restrictions on online video distributors.[29]

---

[16] Zetter, Kim. "Hacking Team Leak Shows How Secretive Zero-Day Exploit Sales Work." Wired. July 24, 2015. http://www.wired.com/2015/07/hacking-team-leak-shows-secretive-zero-day-exploit-sales-work/

[17] United States Commission on International Religious Freedom. "Bangladesh: Action Needed as USCIRF Marks Anniversary of Avijit Roy's Murder." United States Commission on International Religious Freedom. February 25, 2016. http://www.uscirf.gov/news-room/press-releases/bangladesh-action-needed-uscirf-marks-anniversary-avijit-roy-s-murder

[18] ibid.

[19] Ahmed, Saeed. "Ananta Bijoy Das: Yet another Bangladeshi blogger hacked to death." CNN. May 13, 2015. http://www.cnn.com/2015/05/12/asia/bangladesh-blogger-killed/

[20] Meyer, David. "Tango down: Bangladesh blocks messaging apps amid protests." Gigaom. January 19, 2015. https://gigaom.com/2015/01/19/tango-down-bangladesh-blocks-messaging-apps-amid-protests/; Press Trust of India. "1 killed in ongoing Bangladesh protests." Business Standard. January 18, 2015. http://www.business-standard.com/article/pti-stories/1-killed-in-ongoing-bangladesh-protests-115011800289_1.html

[21] O'Neil, Patrick Howell. "Tor use skyrockets in Bangladesh after government bans social networks." The Daily Dot. November 23, 2015. http://www.dailydot.com/politics/bangladesh-social-media-ban-tor-encryption-anonymity-protests/

[22] ibid.

[23] Carsten, Paul. "After Gmail blocked in China, Microsoft's Outlook hacked, says GreatFire." Reuters. January 19, 2015. http://www.reuters.com/article/us-microsoft-china-idUSKBN0KS12520150119

[24] Qiao Long. "China Defends Blocking of Overseas VPNs That Evade Censors." Radio Free Asia. January 27, 2015. http://www.rfa.org/english/news/china/censors-block-vpns-01272015110641.html

[25] Carsten, Paul. "China censorship sweep deletes more than 60,000 internet accounts." Reuters. February 27, 2015. http://www.reuters.com/article/us-china-internet-censorship-idUSKBN0LV16S20150227

[26] Jenkins, Nash. "China Shutters 50 Websites for 'Inciting Panic' Over the Tianjin Disaster." Time. August 17, 2015. http://time.com/3999852/china-shuts-websites-tianjin-censorship

[27] Mozur, Paul. "China Cuts Mobile Service of Xinjiang Residents Evading Internet Filters." New York Times. November 23, 2015. http://www.nytimes.com/2015/11/24/business/international/china-cuts-mobile-service-of-xinjiang-residents-evading-internet-filters.html

[28] Moody, Glyn. "China to set up government censorship offices inside Internet companies." Ars Technica. August 5, 2015. http://arstechnica.co.uk/tech-policy/2015/08/china-to-set-up-government-censorship-offices-inside-internet-companies/

[29] Wee, Sui-Lee. "Chinese police arrest 15,000 for Internet crimes." Reuters. August 18, 2015. http://www.reuters.com/article/us-china-internet-idUSKCN0QN1A520150818; Lin, Lilian. "China to Tighten Limit on Foreign TV and Video Imports." Wall Street Journal. November 16, 2015. http://www.wsj.com/articles/china-to-tighten-limit-on-foreign-tv-and-video-imports-1447672849

Perhaps the most shocking development in Chinese censorship capabilities, though, came in the form of a weapon dubbed "The Great Cannon."[30] China used its Great Cannon to carry out large-scale DDoS attacks on the websites of an OTF-supported internet freedom project, GreatFire.org,[31] and a private American company, GitHub.[32] With its Great Cannon, China is able to hijack and redirect the traffic of millions of unassuming internet users (both inside and outside of China) to assail a targeted website.

The report, published by the University of Toronto's Citizen Lab, highlighted the Great Cannon's offensive, attacking nature: "The operational deployment of the Great Cannon represents a significant escalation in state-level information control: the normalization of widespread use of an attack tool to enforce censorship by weaponizing users."[33] Google noted that the attack highlights the necessity behind encrypting all web traffic.[34]

Beyond Blocking

Globally, repressive states increasingly conscripted their own people to censor and screen content, either through intimidation to encourage self-censorship or through "citizen watchdog" programs that reward people for spotting and flagging online dissent. Kenya announced legislation to require public Wi-Fi users to register their real identities with the government;[35] Russian 'troll factories' employed people solely to flood forums and comment sections with pro-Kremlin propaganda,[36] while a network of pro-government websites masqueraded as legitimate news sources;[37] and China dramatically increased conscription into its "50 Cent Army."[38]

Encryption Scrutiny

The increased scrutiny around encryption writ large reflects a need to better highlight the crucial role encryption plays in the lives of the repressed and vulnerable, let alone its function across all of modern society. Encryption not only keeps sensitive data safe and out of the hands of malicious actors, it is also the backbone technology for tools that break out of heavily censored countries such as China. For human rights activists, democracy supporters, journalists, political dissidents, and rights defenders worldwide, safety and access means strong encryption - a fact reflected by a 2015 UN report on freedom of expression which analyzed encryption and the role it plays for human rights actors.[39]

As David Kaye, the report's author and the UN Special Rapporteur on freedom of expression told the Committee to Protect Journalists,

---

[30] Marczak (Lead), Weaver (Lead), Dalek, Ensafi, Fifield, McKune, Rey, Scott-Railton, Deibert, Paxson. "China's Great Cannon."

[31] Boehler, Patrick. "Hackers Attack GreatFire.org, a Workaround for Websites Censored in China." Sinosphere (New York Times). March 20, 2015. http://sinosphere.blogs.nytimes.com/2015/03/20/hackers-attack-greatfire-org-a-workaround-for-websites-censored-in-china/

[32] Goodin, Dan. "Massive denial-of-service attack on GitHub tied to Chinese government." Ars Technica. March 31, 2015. http://arstechnica.com/security/2015/03/massive-denial-of-service-attack-on-github-tied-to-chinese-government/

[33] Marczak (Lead), Weaver (Lead), Dalek, Ensafi, Fifield, McKune, Rey, Scott-Railton, Deibert, Paxson. "China's Great Cannon."

[34] Provos, Niels. "A Javascript-based DDoS Attack as seen by Safe Browsing." Google Security Blog. April 24, 2015. https://security.googleblog.com/2015/04/a-javascript-based-ddos-attack-as-seen.html

[35] Gallagher, Sean. "Kenya to require users of public Wi-Fi to register with government." Ars Technica. July 1, 2015. http://arstechnica.com/tech-policy/2015/07/kenya-to-require-users-of-wi-fi-to-register-with-government/

[36] Bertrand, Natasha. "Russian internet trolls are trained to spread propaganda in three-person teams." Business Insider. April 1, 2015. http://www.businessinsider.com.au/russian-internet-trolls-are-trained-to-spread-propaganda-in-three-person-teams-2015-3

[37] Alexander, Lawrence. "Open-Source Information Reveals Pro-Kremlin Web Campaign." Global Voices. July 13, 2015. https://globalvoices.org/2015/07/13/open-source-information-reveals-pro-kremlin-web-campaign/

[38] Xu Yangjingjing and Simon Denyer. "Wanted: Ten million Chinese students to 'civilize' the Internet." Washington Post. April 10, 2015. https://www.washingtonpost.com/news/worldviews/wp/2015/04/10/wanted-ten-million-chinese-students-to-civilize-the-internet/; Wong, Patrick. "Chinese Nationalist 'Hawks' Form Online Volunteer Army Against 'Enemy Forces.'" Global Voices. October 19, 2015. https://globalvoices.org/2015/10/19/chinese-nationalist-hawks-form-online-volunteer-army-against-enemy-forces/.

[39] Kaye, David. "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression." Office of the United Nations High Commissioner for Human Rights (OHCHR). May 22, 2015. http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx

"...[G]overnments are using a variety of technologies and approaches either for mass surveillance or for targeted attacks on and surveillance of activists, journalists, civil society organizations, and others, and some [governments] use technology to block access to information...Individuals use tools like encryption and anonymizing platforms to protect themselves and their privacy or legitimately gain access to information...Those tools need to be protected to allow exercise of fundamental rights to opinion and expression. Restricting these tools restricts exercise of the rights."[40]

As the UN recognizes, the role of encryption in advancing access and privacy enables human rights and democracy advocates, NGOs, journalists, and at-risk activists to do their work as safely and effectively as possible under restrictive and dangerous circumstances.

Key Results from 2015

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

Expanding the Internet Freedom Community

- More than 1 billion people began regularly using OTF-supported technology to circumvent restricted internet connections, strengthen their online security, and enhance their digital privacy;

- OTF's Localization Lab enabled translations of internet freedom tools and ensured their accessibility to a global audience; The Lab now supports 49 tools with over 4,600 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 more than 100 applications for support to improve individual research, analysis, and development work that is critical to the future growth and capacity of the internet freedom community;

- The OTF Community Lab supported a wide breadth of individuals to participate in discussions and roundtables and present new information or findings, not to mention expanding the space to address the needs of affected communities. This includes the Localization Summit, Rapid Response Summit, RightsCon Manila, Reproducible Builds Summit, OONI ADINA 15, Allied Media Conference, Chaos Communication Congress and Black Hat;

- In October 2015, OTF held its fourth annual OTF Summit in Washington D.C. with more than 150 participants, including OTF-supported projects, Advisory Council members, congressional staffers, funders and experts from the greater internet freedom community to discuss challenges, innovations, strategies, and needs in the field of global internet freedom;

- Numerous circumvention tools supported by OTF integrated and built upon the "collateral freedom" approach noted in our 2014 annual report by taking advantage of widely used cloud servers to overcome internet censorship;

- Facebook extended its support for Tor users to Android devices through the OTF supported Orbot app;

[40] King, Geoffrey. "UN report promotes encryption as fundamental and protected right." Committee to Protect Journalists. June 16, 2015. https://www.cpj.org/blog/2015/06/un-report-promotes-encryption-as-fundamental-and-p.php

- OTF supported security audits of 26 internet freedom projects, identifying in total 352 privacy and security vulnerabilities; to date, OTF has supported 65 audits identifying and patching a total of 1,749 security vulnerabilities.

Organizational Efficiency

- Nearly 80 percent of OTF's program budget was used to directly support and manage well over 100 projects, initiatives, and lab support;

- The OTF Team reviewed and responded to well over 400 requests for funding totaling close to $50 million in 2015;

- OTF expanded the knowledge base and scope of expertise for proposal reviews by increasing the subject matter expert volunteers on the Advisory Council. The Council now includes leading experts in internet freedom related fields such as Digital Security Consultant Mohammed Al-Maskati, Security Technologist Bruce Schneier and Susan McGregor, Assistant Director of the Tow Center for Digital Journalism.

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 online censorship including in places such as Tibet, Iran, Thailand, Bahrain, Sudan, Vietnam and Azerbaijan;

- OTF supported numerous individuals and organizations producing ground-breaking analytical and research reports, including Baidu's and Don'ts: Privacy and Security Issues in Baidu Browser, The Crime of Speech: How Arab Governments Use the Law to Silence Expression Online, Every Rose Has Its Thorn: Censorship and Surveillance on Social Video Platforms in China, Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuing Proliferation, No Encore for Encore? Ethical Questions for Web-Based Censorship Measurement, Forgive Us our SYNs: Technical and Ethical Considerations for Measuring Internet Filtering, Politics, Rumors, and Ambiguity: Tracking Censorship on WeChat's Public Accounts Platform, Ethical Concerns for Censorship Measurement, and Understanding Internet Freedom: Tunisia's Journalists and Bloggers;

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

- OTF worked with internet freedom technologists, researchers, and policymakers while participating in key conferences, including the Internet Freedom Festival, RightsCon Manila, Hackers on Planet Earth (HOPE), Freedom Online Coalition, Mekong ICT, Privacy Enhancing Technologies Symposium (PETS), Chaos Communication Congress, Stockholm Internet Forum, Forum on Internet Freedom in East Africa, Arab Internet Governance Forum, and the DG7 internet freedom working group.

Funding Collaboration

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

- OTF raised awareness of the need for internet freedom funding around the world and helped increase globally available funding by unlocking over 100 million dollars of private funds set aside for internet freedom related efforts since 2012;

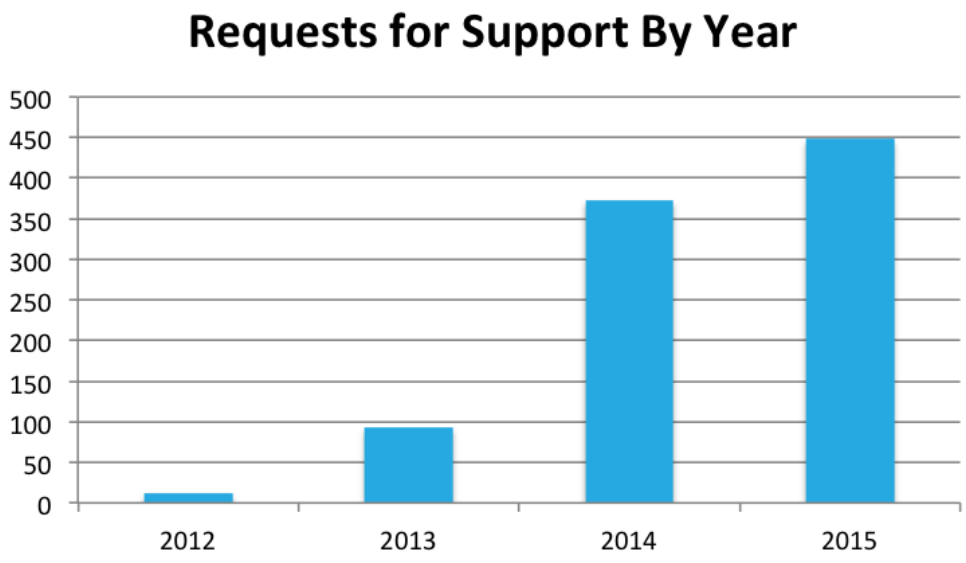
- Through active coordination with other donors, OTF more than quadrupled the impact of 4 million dollars in public funding through collaborative joint funding, expanding the amount of funds for these projects to more than 30 million dollars.

- OTF regularly participated in numerous external review panels of related technology proposals including those at 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, German Federal Foreign Office, and many others;

- OTF expanded collaboration on capacity building through fellowships hosted at premier organizations and research institutions including Princeton University, Electronic Frontier Foundation, University of California - Berkeley, Harvard University, Oxford University, Centre for Intellectual Property and Information Technology Law, Strathmore University Law School, University College London, and Simply Secure.

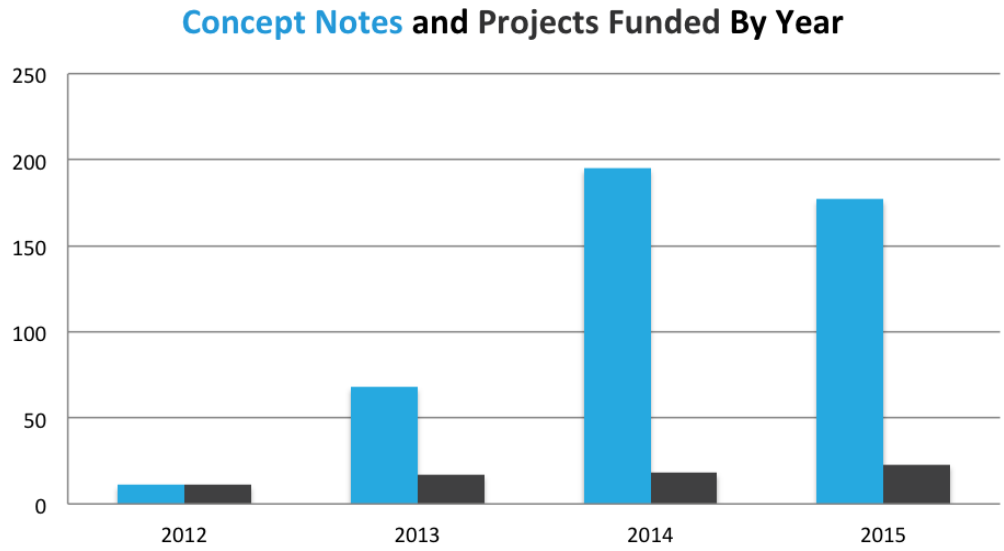
Trends from 2015

OTF saw continued growth in requests for support, once again receiving the highest number in the history of its operations. Overall, OTF received nearly 450 submissions requesting close to $50 million.



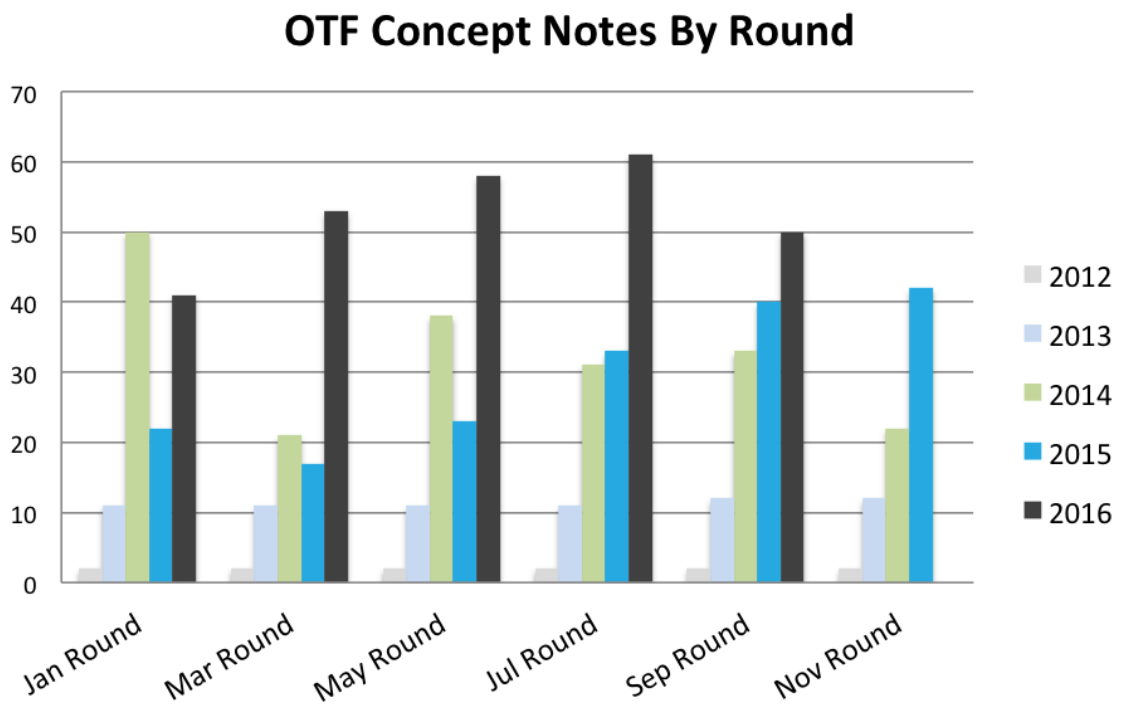
Concept Note Submissions and Increased Need

With lower fellowship expenses (see footnote 42), OTF was able to dedicate additional funds to projects applying to our Internet Freedom Fund. Nevertheless, due to budget constraints and a long funding lapse at OTF, the overwhelming majority of applicants were declined despite a wealth of creative projects. Both the quantity and quality of applicants continues to grow.



As we saw in 2014, growing levels of interest in OTF led to a high number of concept note submissions especially from new and diverse applicants. The OTF team responds to all submissions every two months. During 2014 and 2015, OTF funded approximately 10 percent of the concept note submissions received. This is substantially lower than that of the National Science Foundation which funds more than 25 percent of submissions.[41] Because OTF's overall budget has not been increasing in parallel with demand, this disparity is likely to widen given the significant growth in applications received in 2016.

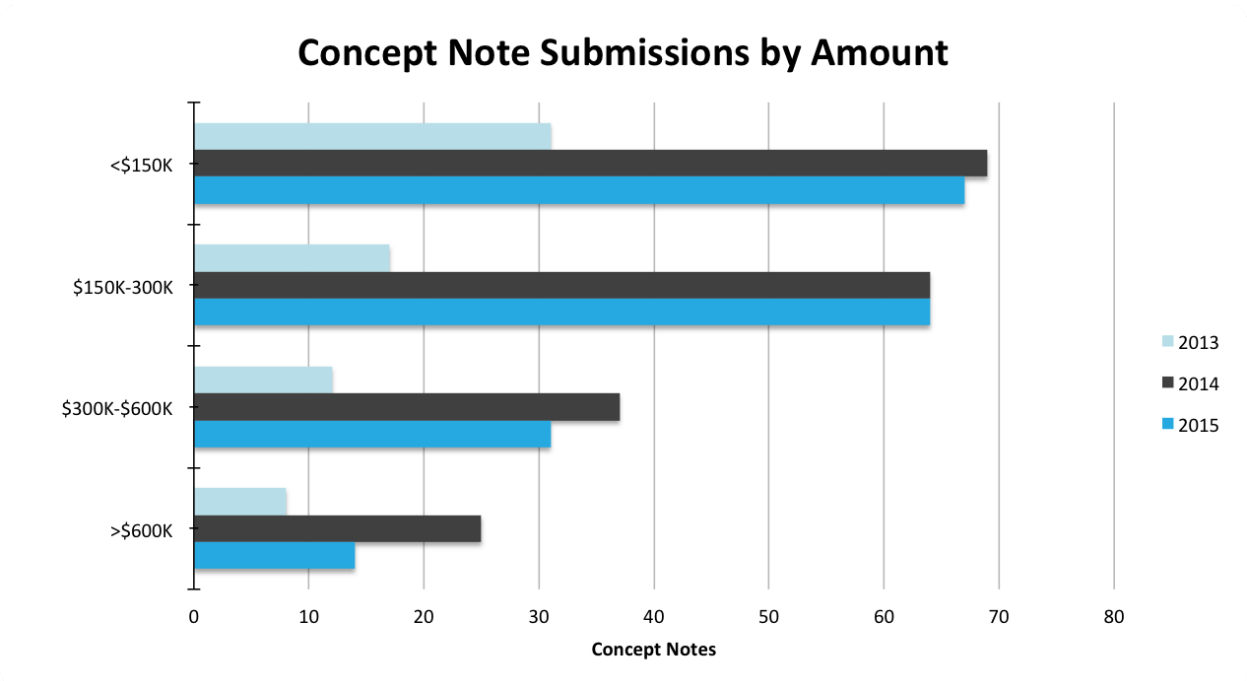
[41] "NSF receives approximately 40,000 proposals each year for research, education and training projects, of which approximately 11,000 are funded." https://www.nsf.gov/funding/aboutfunding.jsp



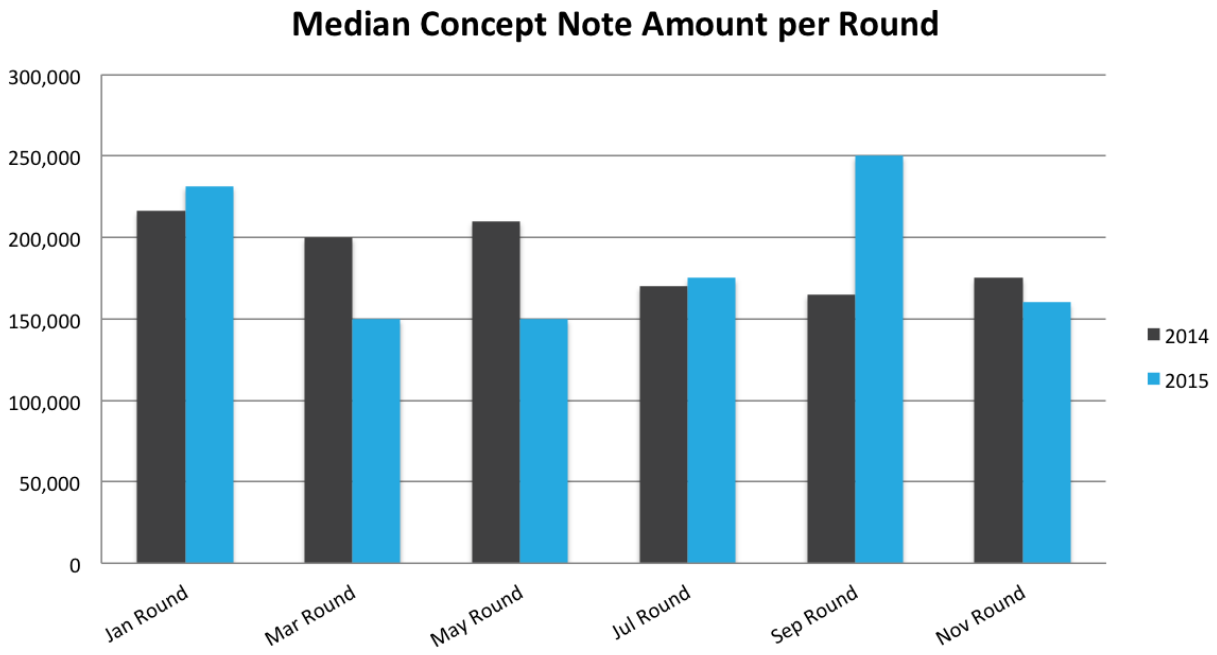
Note: OTF did not have concept note rounds in 2012 and much of 2013. Thus, the total concept notes for those years have been evenly distributed across all rounds.

Finding a Low Cost Niche

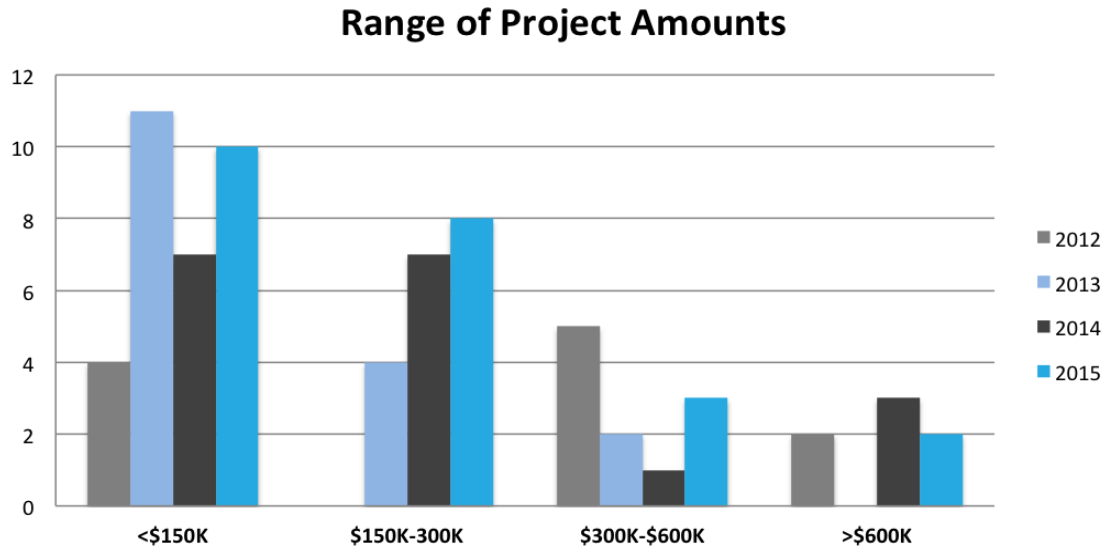
Despite the heightened level of concept note submission, this did not affect the proportion of submissions requesting less than $300,000, which is the target ceiling of OTF support contracts. In 2015, nearly 75 percent of concept notes submitted fell within this range, OTF's highest level ever.



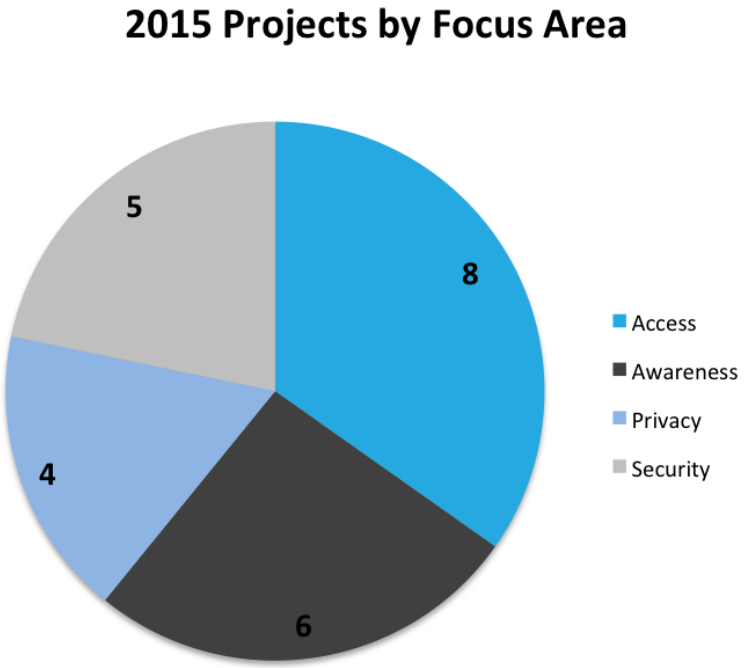
Overall, the median request level per concept note round has stayed remarkably consistent throughout OTF's past two years.



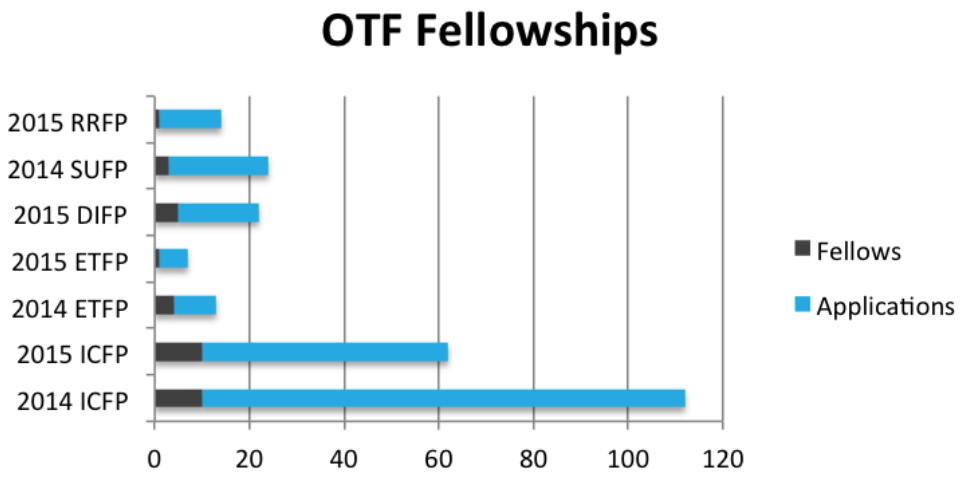
OTF prioritizes increasing the accessibility of U.S. Government internet freedom funds to emerging talent by removing unnecessary barriers to entry as well as growing capacity. These request levels are an encouraging sign that OTF is attracting projects that do not meet the minimum levels necessary to receive support from other U.S. Government internet freedom funders. Furthermore, OTF's process ensures it is open to those that would otherwise be turned away. This includes individuals, 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 act as a subcontractor to a previous recipient. As demonstrated below, OTF continued to primarily support projects in this range.



While the overall project amounts remained consistent, OTF supported a higher proportion of access and awareness projects. This reflects the increase in censorship, internet shutdowns and the growing need to ensure censored individuals understand the solutions available at no cost. Overall, projects spanned a wide range of focus areas as described in the Program Overview section below.



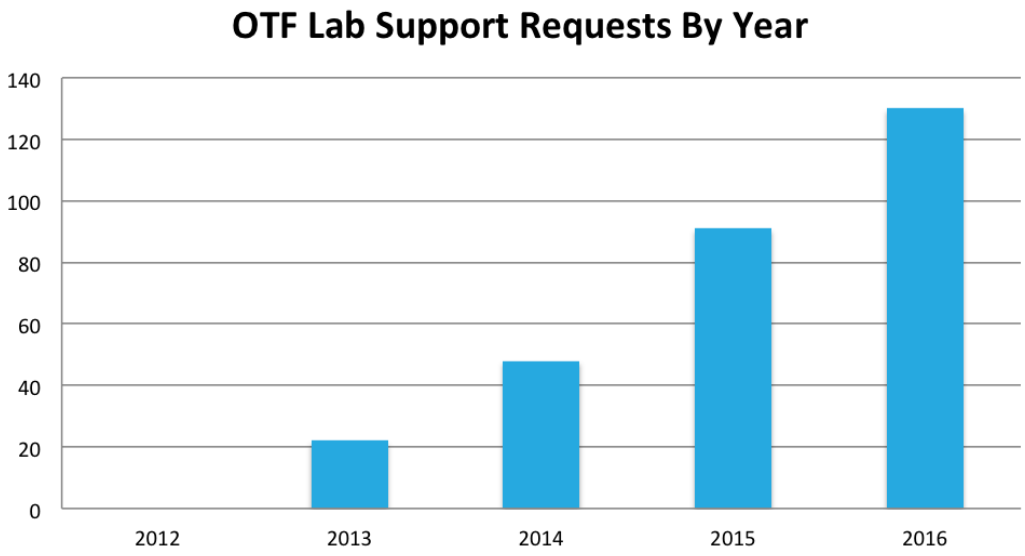
OTF's first foray into supporting fellows in 2014 was successful in both bringing in new applicants and directly supporting a multitude of talented individuals with minimal cost and maximum impact. OTF continued to operate numerous fellowship programs in 2015. They span a wide range of focus areas described in more detail in the next section.[42]



[42] The fellows in the second round of the Information Controls Fellowship Program were supported in mid-2015. These fellows were accounted for in the expenses from the previous year's budget due to the funds being set aside at the outset of the application window. This accounts for the larger costs associated with the Program in the previous annual report. The 2016 round application window opened in early February. Both the applicants and the fellows will be accounted for in OTF's 2016 annual report.

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

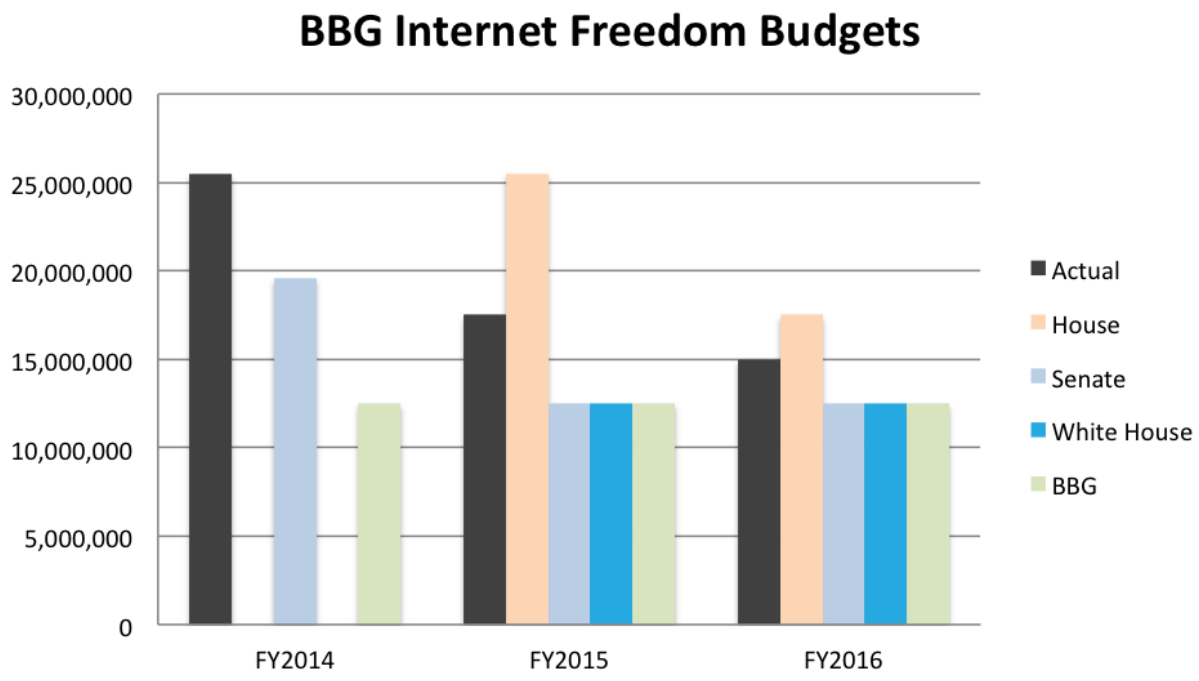
OTF's labs continue to see increasing levels of interest and utilization from OTF supported and unsupported projects alike. Each lab is supported by one or more service partners. Rather than one-off agreements between a partner and an applicant in need, OTF maintains a single service agreement with each 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. These labs have offered critical services for hundreds of internet freedom projects since 2012. In 2015 interest in these services only continued to grow, a trend that has held true in 2016.



Decreasing U.S. Government Support

After Congress increased the Broadcasting Board of Governors budget for internet freedom to its highest level ($25.5 million) in FY2014, FY2015 saw a dramatic decrease of more than 30 percent ($17.5 million).[43] OTF was able to carryover a portion of its 2014 funds providing some counterweight to this marked reduction. Still, with OTF launching a litany of new initiatives in 2014, the reduction limited the speed with which OTF could foster continued growth.

[43] OTF's budget has historically been half of the overall amount the BBG receives for internet freedom.



Note: The gaps in FY2014 are due to a specific amount not being recommended for the BBG's internet freedom appropriation by the associated entity.

While a justification for this decrease has not been provided, numerous entities sought significant reductions from the FY2014 level. For both FY2015 and FY2016, the BBG requested that Congress fund internet freedom at half of FY2014 levels ($12.5 million).[44] This lower figure was ultimately included in the White House budget and the report from the Senate Appropriations Committee.[45] The House Appropriations Committee sought a higher level of funding in both of these fiscal years with a minimum of $25.5 million being requested in FY2015 and $17.5 million in FY2016 as noted above.[46]

In both years, the final budget for internet freedom split the difference between the House of Representatives figures and those from the Senate, White House and BBG. This resulted in a minimum allocation to the BBG of $17.5 million in 2015 declining to $15 million in FY2016.[47] The latter appropriation represents a more than *40 percent reduction* over FY2014 levels. This is not only a troubling trend for the program but the combination of dramatic budget cuts and long delays in the receipt of funds have created "ongoing concern" issues with our partner funders and those supported by OTF.

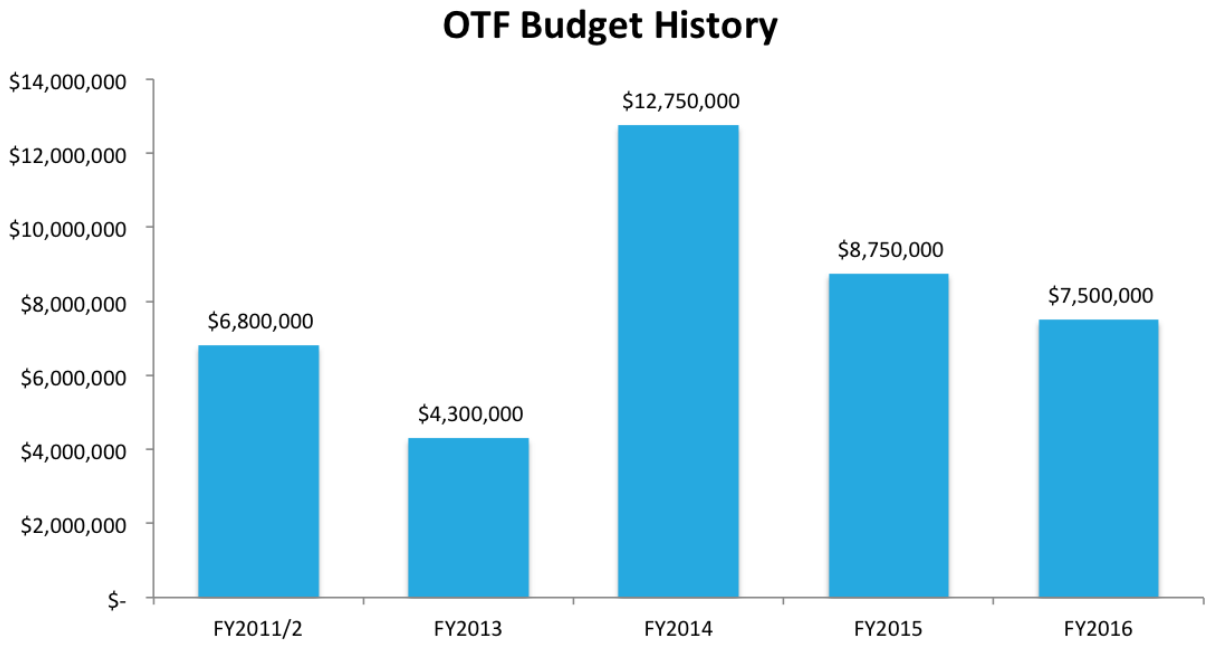
---

[44] 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.

[45] 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; 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.

[46] 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

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



FY2015 Program Overview

Types of Efforts OTF Supports

The efforts for each project or person OTF supports will have primary outcomes that fit within the following focus areas and objectives:

Focus

1. • ***Access*** to the internet, including technology to circumvent website blocks, connection blackouts, and widespread censorship;
2. • ***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 such as research and real-time monitoring of censorship behaviors;
3. • ***Privacy*** enhancement, including the ability to be free from repressive observation and the option to be anonymous when accessing the internet;
4. • ***Security*** from danger or threat when accessing the internet, including encryption tools.

Objectives

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

Programs in FY2015

The core of OTF's work consists of providing needed funding and services to projects and people: funding provides support directly to a project or a person via a contract; and services are OTF-provided goods, commodities, or other indirect services made available to 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 expression, free press and human rights, through the free flow of information online by supporting anti-censorship and secure communications technology, increasing censorship awareness, improving digital safety, and researching emerging threats to internet freedom. More than half of OTF's budget was expended on applications received through this program fund. OTF invites organizations and individuals creating or sustaining internet freedom technology and interested in potential funding to submit a concept note for their project. These projects are listed below in the following categories: Access, Awareness, Privacy and Security.

Access

Tor

FY2015, $900,000

This project builds on the baseline Tor two-year development project that ensures Tor software can continue to provide world-class anonymity and censorship circumvention solutions -- currently serving more than a million users a day -- to address two primary additional objectives: core Tor development work on resiliency to new attack techniques, and Tor Browser development work to ensure safety, integrity and usability for the packaging and user interface side of Tor.

Mudhorse

FY2014, $230,000

Mudhorse is an open-source, free, user-friendly, high-performance censorship circumvention tool with strong blocking resistance through crowdsourcing volunteers. Mudhorse has a particular emphasis on strong blocking resistance, performance and ease-of-use, rather than strong privacy protection. Mudhorse will integrate three new components: 1) A browser bundle with built in robust circumvention capabilities, designed specifically for non-technical internet users; 2) A "smart routing" browser plugin that activates circumvention channels only when a user attempts to access blocked sites; 3) a backend system that enables easy proxy creation allowing those with uncensored connections to offer an additional circumvention channel for those that are censored.

Satori

FY2014, $112,208

Satori provides tamper-resistant downloads of circumvention and security tools often blocked in repressive countries, such as Iran and China. Many other countries embed malware in these tools eradicating any increase in access or privacy the tool would otherwise provide. Previously, Satori was only available as a Google Chrome Browser App. This project introduces this critical service as both a desktop and mobile app (for Windows and Android). It also expands the diversity of circumvention channels users can employ to access these verified downloads.

Tor Bridge Distribution

FY2015, $74,944

This project improves the overall distribution, robustness, scalability, performance and maintainability of Tor Bridges. It includes the development of more secure and user-friendly mechanisms for bridge distribution. Bridges (or Bridge Relays) are entry points into the Tor network that aren't listed publicly (and therefore are not easily discoverable or known to censoring state actors). Without this work, much of the Tor Project's efforts in

the area of censorship circumvention would quickly be rendered unusable. The addition of Tor Bridges allows user resiliency in the circumvention and blocking resistance race.

Serval
FY2014, $101,573
Civil unrest, war, repressive regimes and disasters can all deny the general populace safe access to mobile telecommunications networks and the internet. The Serval Project mitigates this by enabling mobile phones to communicate directly with each other in the complete absence of cellular or other infrastructure. Given recent improvements to Apple's peer-to-peer wireless, this project will port the Serval Mesh app to the iPhone to ensure iPhone owners can communicate with each other in private without using cellular SMS or internet data and the monitoring that goes along with it.

Briar
FY2014, $150,100
Briar is an open source Android messaging app designed to provide a safe, easy, and robust way to communicate via private messaging, blogs and forums when the mobile internet connection is shut down. When the internet is down, Briar can sync via Bluetooth or Wi-Fi, keeping the information flowing during a crisis or state-imposed outage. When the internet is up, Briar can sync via the Tor network, protecting users and their relationships from surveillance. This project takes Briar from its current well-researched alpha state to a fully tested production release ready for field deployment.

Bazaar
FY2014, $468,875
Bazaar is building a complete distribution ecosystem for internet freedom tools that provides secure, streamlined tools for developers and organizations, while providing an easy "app store" experience with built-in circumvention. The second phase of the Bazaar project, aka Bazaar2, being supported here implements the entire system and user experience for the Android platform, the largest smartphone platform around the world. It will act as a secure alternative to the Google Play Store.

Clatter
FY2015, $45,000
Clatter is a suite of extremely lightweight and stand-alone libraries, which aims to create common protocols and standards for existing projects to add in secure nearby communication without having to sacrifice 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 will allow anyone to add secure device-to-device networking to their own projects.

Awareness

FreeWeChat
FY2015, $102,000
This project creates a freely available parallel website that tracks in real time what is being censored on public WeChat 'channels' including search capability. WeChat is the primary social media platform in China but exists wholly under the control of Chinese censors. This web interface functions as a WeChat mirror with functionality unavailable in static efforts to capture deleted or manipulated content.

Battle Testing Privacy Tools
FY2014, $149,705
This project explored solutions to some of the disconnects between tool developers, digital security trainers, and end-users in the internet freedom community. The project created a baseline of data and guidelines that

allows the internet freedom community to make evidence-based and cost-effective decisions about placing tools and knowledge with those in censored and surveilled environments. The two specific groups of end-users focused on were Belarusian and Turkmen activists who can travel freely in and out of their respective countries. They will test methods to determine how to achieve maximum uptake with activists from high-risk communication environments and propose evidence-based pedagogical approaches to training at-risk users.

Net Alert
FY2012, $192,570[48]
Net Alert brings together well respected researchers in the circumvention tech space to investigate recent and emerging targeted digital attacks against at-risk populations. The project focuses on the privacy issues with popular consumer-grade technologies used by at-risk populations, along with targeted malware, network side channels and man-in-the-middle attacks. Research findings are translated and rely on visualizations and other non-text based media to empower end-users to make better informed decisions about their technology usage.

Information Control Watch
FY2015, $150,950
To better understand internet censorship, shutdowns and other forms of information controls in Iran, this project uses innovative methods to document ongoing and event based information controls in Iran. The project also provides mechanisms for Iranians to push for greater online access to information.

SourcesDB
FY2015, $327,054
A growing form of internet interference focuses on co-opting the internet's open nature through sockpuppet activity. Governments are hiring hundreds to thousands of people for the sole purpose of pushing pro-government positions in online forums and message boards. This project is building an open source toolkit focused on assisting journalists and other truth seekers to quickly assess the source of information derived from social media through metadata collection by having users annotate a media source, such as a social network post or website, with confidence levels based on their online track records.

HikingGFW
FY2014, $230,000
HikingGFW is a portal that gives real-time reports on the state of censorship by the "Great Chinese Firewall" (GFW). HikingGFW monitors and publishes information on blocked domain names, keywords, and IP addresses, including both what is blocked (domain names and keywords) and how (DNS injection, IP blocking, TCP/IP RST), as well as user reports of censored websites. With OTF support, HikingGFW built a new user-friendly front-end and identified the primary blocking techniques used by the GFW.

Arab User Support
FY2015, $50,000
This pilot project provides dedicated Arabic user support for circumvention tools to improve citizens' ability to use them successfully. This project fills a critical gap by serving as a dedicated Arabic user support resource or "help desk".

Supporting Digital Security of LGBTI Communities in the MENA region
FY2015, $209,770
This project focuses on high risk users in the MENA region to analyze how they are being targeted on social networks. The project will work directly with these social platforms to address the holes, develop

[48] The funds utilized to support this project originated from a FY2012 contract. OTF and the contractor no longer found the work relevant in the present environment and agreed to terminate the contract. As such, this amount is not reflected in the Expenses Breakdown section.

methodologies to reduce the exposure and train the larger community of at-risk users on digital security and technologies in these countries.

Privacy

Signal
FY2015, $900,000
Open Whisper Systems (OWS) produces Signal, one of the leading encrypted mobile communication tools. This support enables the OWS team to implement seamless open standard for asynchronous messaging, including multi-device and broad platform support, app integration and secure voice communication.

(n+1)sec
FY2015, $133,000
This project improves the state of current standards used for multi-party encrypted instant messaging. The primary focus is building upon the current robust standard Instant Message encryption specification which supports only two users (Off-the-Record) to be a specification supporting multiple users (Multi-Party Off-the-Record). A new specification of this capability has the potential to be the solution for many other encrypted chat applications that lack multi-party support, including popular tools like Google Talk.

LEAP Encryption Access Project
FY2014, $299,887
The Bitmask Client Application is a highly secure cross-platform VPN and encrypted email application where everything is automatically configured. LEAP Encryption Access Project is partnering with two internet service providers (ISPs) to replicate and deploy the BitMask Client Application on their network. This platform provides system administrators with a cheap and easy means to deploy and manage privacy enhancing tools. Both non-profit ISP partners (Colnodo and Codigo Sur) are security-conscious and closely aligned with LEAP's goals of supporting journalists, human rights defenders and non-profit organizations to make use of internet technology. Following these successful deployments, LEAP expects to partner with an increasing number of ISPs around the globe to adopt these tools.

K-9 Mail
FY2015, $85,000
K-9 Mail is a secure email client for Android with well over 5 million installs and availability in more than 30 languages. It is a tool used by many internet freedom defenders globally. This project is adding much needed features, usability improvements and security enhancements frequently requested by users.

Security

NoScript
FY2015, $250,000
NoScript is a popular privacy and security enhancing browser extension for Mozilla Firefox and is pre-installed in the Tor Browser. The Firefox browser is transitioning to a multi-process architecture requiring a significant overhaul to maintain the critical protections NoScript provides and expand their availability to mobile platforms.

Subgraph OS
FY2014, $200,000
Subgraph OS is a desktop operating system that is designed to be both usable for non-technical users and secure against active interference and targeted attacks. It is specifically designed to protect users at risk of identification and surveillance by determined, capable, network-borne adversaries. This project supported further development of the platform, improvements to the user experience, security and usability testing, user documentation and the official launch.

Qubes
FY2015, $410,000
This project makes Qubes, a security-focused free and open source operating system, more usable and secure through the introduction of pre-configured, out-of-the-box turn-key features. This functionality allows users to control the level of access an application has to other information, protecting sensitive information both from compromise and from exfiltration.

Kitten Groomer
FY2015, $122,400
In many repressive countries USB data transfer is the most common method of transferring information but presents significant security concerns. Kitten Groomer is an independent hardware solution to sanitize documents from untrusted USB flash drives. The device automatically converts untrusted documents into a readable but unmodifiable format on a clean USB key and makes clear to the user if it was not possible. This project improves the software code, creates user documentation, performs robust security testing and disseminates the tool to key users such as journalists.

Magic Folders
FY2014, $150,000
Magic Folders is a free and open source alternative to existing cloud storage solutions that people in repressive countries can use to securely collaborate and to share their work. Unlike existing cloud storage options like Dropbox, Magic Folders protects the user's files with end-to-end cryptography, so that adversaries who compromise a server cannot spy on or alter the files. This project integrated the software with Windows and Linux platforms and improved the user interface and functionality.

Supporting People

Digital Integrity Fellowship
FY2015, $100,000
The online landscape is changing non-stop, creating an increasingly difficult challenge for small and medium sized organizations to maintain up-to-date digital security 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, human rights defenders, NGOs, activists, bloggers, 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. OTF provided initial support to five fellows working in repressive environments around the globe.

Supporting Usability and Design in Security Fellowship
FY2015, $0
The Supporting Usability and Design in Security Fellowship aims 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 program feeds into and supports existing centers of expertise by offering competitive and highly sought-after paid fellowships. Our current host organizations are Simply Secure, The Open Technology Institute, SecondMuse, and University College London.[49] OTF expects the next round of fellows to be announced in the Fall of 2016.

[49] While no funds were spent on this program in 2015, OTF expects significant support to be provided in 2016.

Information Controls Fellowship

FY2015, $41,000

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 and the technical systems that enable or undertake all of the above to the detriment of internet freedom. OTF works with nearly a dozen host organizations for the fellowship ranging from prominent academic institutions to accomplished advocacy groups. OTF's second round of ICFP resulted in ten fellows whose research spans much of this field, with selection of the third round nearly complete.[50]

Emerging Technology Fellowship

FY2015, $55,400

The Emerging Technology Fellowship Program (ETFP) focused on growing the community of internet freedom defenders and its collective expert capacity by supporting individual technologists, researchers, and advocates. Support was primarily available for individuals with novel ideas that address emerging threats to global internet freedom. Numerous applicants had difficulty differentiating this fellowship from projects supported through our Internet Freedom Fund. Given the confusion, OTF decided to lower the floor for concept notes through our Internet Freedom Fund from $50,000 to $10,000 and retired ETFP.

Rapid Response Fellowship

FY2015, $30,200

The Rapid Response Fellowship Program (RRFP) was a mechanism to directly support the global network of individuals providing digital emergency and rapid response to civil society organizations and people affected by repressed internet freedom. Numerous applicants experienced confusion about whether to apply to RRFP, DIFP or the Rapid Response Fund. As a result, OTF streamlined the process by encouraging all rapid response applications to be submitted to the Rapid Response Fund with more extended digital security assistance coming from DIFP.

Offered Services - OTF Labs

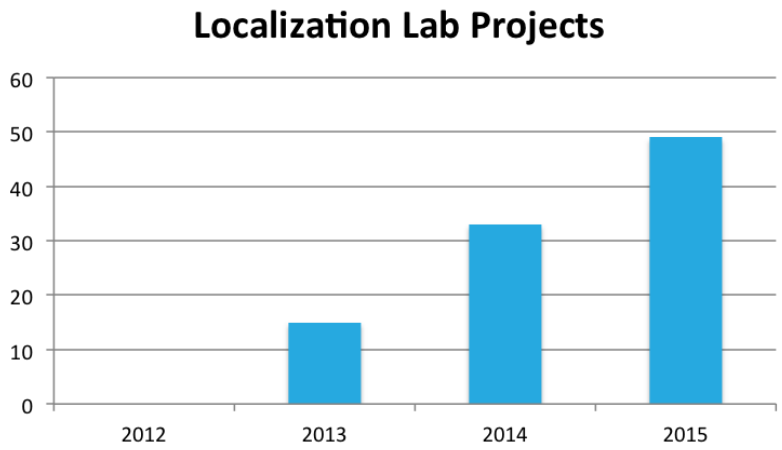
Localization Lab

$350,061

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 SecondMuse and Localization Lab.[51] By the end of 2015, the hub included 49 projects with more than 4,600 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.

[50] More information available at https://www.opentech.fund/article/otfs-newest-class-information-controls-fellows. See Footnote 42 for an explanation of how these fellows are discussed in this annual report.

[51] See https://internetfreedom.secondmuse.com/ and https://localizationlab.org/.



Engineering Lab

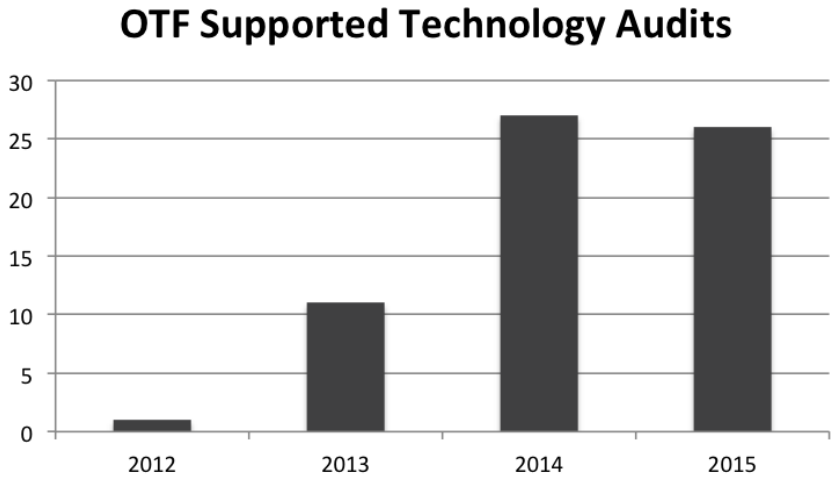
$1,023,589

The Engineering Lab includes OTF's Secure Cloud Infrastructure (now "Eclipsis"), 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. 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 2015 and dozens of others applying for other Engineering Lab services.

Red Team Lab

$318,961

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. 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.



Community Lab

$688,296

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 which must be solved with community-wide strategies bringing to bear collective vision and action, and properly working beyond cross-cultural barriers. Community Lab also 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 2015, among other things, the Community Lab supported the OTF Summit, Localization Summit, Rapid Response Summit, RightsCon Manila, Reproducible Builds Summit, OONI ADINA 15, Allied Media Conference, CCC and Black Hat. In addition, the Lab provided community management consultation to various networks.

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 these tools' adoption. More critically, these challenges sometimes lead to user misconception about tools – which in turn 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. The Usability Lab began working with I2P and the Tor Project in 2015. These projects consist of some of the oldest and most widely known circumvention tools, relied on by both developers and users. Usability experts in the Lab worked with these tools to map their priorities to identify key user challenges to their tool use, and to incorporate these design revisions into their work plans for future development cycles. OTF relied on existing FY2014 contracts to offer the Usability Lab's services in FY2015. The Lab will require additional resources in 2016.

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. Current legal clinic/pro bono partners include the Startup Legal Garage at UC Hastings, the Cyberlaw Clinic at Harvard Law School, and several US-based law firms.

Rapid Response Fund

$389,916

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 2015, OTF provided emergency support for a variety of digital emergencies experienced by high-risk internet users and organizations, such as bloggers, cyber activists, journalists, 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 website audits, forensic reports, infrastructure

improvements, VPN services, secure hosting, secure cloud access and secure mail servers. The Rapid Response Fund has been utilized by entities around the globe including those focused or residing in China, Tibet, Iran, Thailand, Yemen, Bahrain, Sudan, Azerbaijan, Myanmar, Zimbabwe and many others.

Expenses Breakdown[52]

Direct Support	**$ 6,468,982**
- *Projects*	*$ 5,852,466*
- *Access*	*$ 2,082,700*
- *Awareness*	*$ 1,219,479*
- *Privacy*	*$ 1,417,887*
- *Security*	*$ 1,132,400*
- *Fellowships*	*$ 226,600*
- *Rapid Response*	*$ 389,916*
Indirect Support (Labs)	**$ 2,380,907**
- *Red Team*	*$ 318,961*
- *Engineering*	*$ 1,023,589*
- *Community*	*$ 688,296*
- *Localization*	*$ 350,061*
Total Salaries and Benefits (10/14-5/16)	**$ 1,576,732**
OTF Administrative	**$ 156,867**
RFA Administrative	**$ 367,471**
Travel	**$ 350,619**

FY2014/2015 Total Expenditure	**$ 11,298,503**
Carryover from FY2014	**$ 2,556,781**[53]
FY2015 Budget	**$ 8,750,000**

Total Budget	**$ 11,306,781**

[52] A significant portion of FY2015 funds were spent in the first half of 2016. This is due to the incremental release of funds by Congress over a 6 month period with the bulk coming in late 2015 and early 2016 in addition to the uncertainties resulting from BBG internal processes. These extended periods with limited funding affected OTF's ability to provide consistent support throughout the year. More significant delays are particularly harmful to the Rapid Response Fund and certain Lab services. These disruptions also impact OTF's ability to leverage the resources of non-public internet freedom funders.

[53] Recognizing the need to mitigate funding gaps, Congress decided in 2014 to make internet freedom funds available as "no year funds" at the joint request of BBG IAC and OTF and significantly increase the funding allocation. These "no year" funds are available for obligation without fiscal year limitation. OTF took advantage of this by allocating a limited portion of FY2014 funds for use in FY2015. 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

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 noted above, this work has become all the more important. In 2014, OTF witnessed a noticeable uptick in interest from a variety of funders. 2015 was no different. Numerous private foundations made internet freedom related causes a primary focus[54] and other democratic governments continued to increase their support and interest.[55] Venture capitalists are also increasingly interested in fundamental technologies such as decentralization that have the potential to foster innovative new tools for at-risk communities.[56]

Leveraging Support Requests

The growing interest in receiving support from OTF has resulted in an increasing level of insight into trends within the internet freedom space. We intend to utilize this interest to assist an increasing number of internet freedom funding sources in identifying projects and individuals in need of support. While this will not offset the harm created through a reduced U.S. Government internet freedom budget, OTF will continue to explore every method to ensure critical internet freedom projects focused on helping support those in repressive environments receive adequate support. The associated activities include frequent direct outreach to non-USG internet freedom funders, capitalizing on opportunities to increase interest and engagement with new audiences and ongoing improvements to raise awareness of other funding opportunities through mailing lists and our alternative sources of support resources.[57]

U.S. Government Support

As noted above, OTF has witnessed a significant decline in support. This work has taken on greater importance given that numerous proposed budgets, including those for FY2017, continue to lower the minimum internet freedom funding amount allocated to the BBG.[58] The reductions to date have undoubtedly harmed the program's ability to support the rapidly growing community committed to addressing the increasing array of digital interference techniques proliferating 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 not only identify means to highlight the growing importance of this funding but also the tremendous disparity in financial and personnel resources invested by the USG as compared to repressive governments that continually adopt and advance information controls. The establishment of the BBG Office of Internet Freedom creates the potential to advance this effort.[59]

---

[54] See e.g. https://www.opentech.fund/article/ford-foundation-introduces-internet-freedom-program; http://www.hewlett.org/newsroom/press-release/hewlett-foundation-announces-45-million-grants-mit-stanford-uc-berkeley-establish-major-new-academic; https://responsibledata.io/forums/responsible-data-for-human-rights-funders/;

[55] See e.g. https://www.accessnow.org/the-access-grants-program-an-emerging-initiative/;

[56] See e.g. https://www.usv.com/blog/usv-thesis-20

[57] https://opentech.fund/apply/alternative-sources-support

[58] *See* Broadcasting Board of Governors, Fiscal Year 2015 Congressional Budget Request, p. 14, http://www.bbg.gov/wp-content/media/2011/12/FY-2017-Budget-Submission.pdf; The President's Budget for Fiscal Year 2017, Appendix, p. 1240, https://www.whitehouse.gov/sites/default/files/omb/budget/fy2017/assets/appendix.pdf; S.3117 - An Act Making Appropriations for the Department of State, foreign operations, and related programs, Fiscal Year 2017 114th Congress (2015-2016), Global internet freedom Sec. 7078. b)(2)(D) https://www.appropriations.senate.gov/imo/media/doc/FY2017-State-Foreign-Operations-Appropriations-Bill-S3117.pdf. The exception to these reductions has been the House of Representatives. See subsection on Decreasing U.S. Government Support above.

[59] https://www.bbg.gov/who-we-are/our-leadership/senior-management/dr-nnake-nweke/

Core Infrastructure Fund

OTF formally launched the Core Infrastructure Initiative in late 2015. It supports the core building blocks of everyday internet freedom technology. This may include efforts focused on sustaining or improving essential technologies such as PGP, SSL, SSH, Tor, OTR, pluggable transports, code libraries, and other technologies. OTF collaborates with numerous initiatives and private companies in order to identify foundational components of open source projects well suited to strengthen internet freedom. Moving forward, OTF expects to see an increasing number of requests for support focus on the large scale vulnerabilities implicated by such widely adopted technology.

Challenges Ahead

The various methods of restriction and censorship described above have already evolved and proliferated in 2016. Today we are 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 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. They have clearly and openly stated their priorities, demonstrating their dedication to further the development, sophistication, and expansion of repressive censorship mechanisms.

And again we respond, reaffirming our unremitting commitment to resist, by following those people and projects tirelessly defending internet freedom, and providing support however we can. Like them, OTF will continue to evolve, anticipate technological advancements, defend against injurious social or regulatory change, and circumvent any repressive restrictions for as long as threats against human rights, open societies, and internet freedom exist.

Appendix

The OTF Team in 2015

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.

Bernadette Mooney Burns
General Counsel and RFA Board Secretary, RFA
Ms. Burns has been RFA's General Counsel since 2006 and was elected 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.

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 including the development of annual and multiyear budgets and financial plans; contract reviews; analyzing 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.

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

Adam Lynn
OTF Research Director, RFA
Mr. Lynn joined RFA in April 2012 as OTF's inaugural program manager. He leads OTF's research initiatives including the Information Controls Fellowship program while participating in OTF's day-to-day operations and long-term planning.

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

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

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.

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, along with the Digital Integrity and Secure Usability Fellowship programs.

Esther Lim

OTF Senior Program Manager, RFA

Ms. Lim joined RFA in November 2014. As Senior Program Manager she is actively engaged in the day-to-day operations of OTF. Among her many responsibilities, she heads the Legal Lab, manages a portfolio of funded projects, and manages the emerging Accelerator program.

Denna Millet

OTF Program Manager, RFA

Ms. Millet joined RFA in October 2014 as a Program Manager with OTF. As a program manager, she is responsible for day-to-day program management, Rapid Response Initiatives, MENA focused projects and serving as a liaison to the Director General 7.

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*.

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 has the expertise of the Advisory Council. Today's council brings experience in numerous areas of research, development and disciplines. Differing from OTF's beginning, where all members served on a single panel reviewing all applications, OTF now maintains multiple panels where members review applications for specific funds and fellowships. As such OTF has significantly expanded the council.

Since 2014, the following individuals have joined the OTF Advisory Council: Mohammed Al-Maskati, Sanne Stevens, John Adams, Tanya O'Carroll, Wojtek Bogusz, Michael Geist, Chris Bronk, Bryan Nunez, Bruce Schneier, Alix Dunn, Susan McGregor, J. Ayo Akinyele, Collin Anderson, Nadia Eghbal, Stefania Milan, Emily Ratliff and Mohamad Najem. Below is the current membership:

Kevin Bankston, *Policy Director, New America Foundation's Open Technology Institute*
Gustaf Björksten, *Technology Director, Access*
Matt Braithwaite, *Google*
Cory Doctorow, *Author, Journalist, and Activist*
Peter Eckersley, *Technology Projects Director, Electronic Frontier Foundation*
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*
Andrew McLaughlin, *betaworks / Berkman Center for Internet & Society*
Haroon Meer, *Founder, Thinkst*
Kavita Philip, *Associate Professor of History at the University of California, Irvine*
Dr. M. Chris Riley, *Head of Public Policy, Mozilla*
Bruce Schneier, *Security Technologist and Author*
Ian Schuler, *CEO, Development Seed*
Joana Varon Ferraz, *Independent*
Mohammed Al- Maskati, *Digital Security Consultant, Front Line Defenders*
Sanne Stevens, *Program Officer, Hivos*
John Adams, *Independent Security Consultant*
Tanya O'Carroll, *Adviser on Technology and Human Rights, Amnesty International*
Wojtek Bogusz, *Digital Security Consultant*
Michael Geist, *Law Professor, University of Ottawa*
Chris Bronk, *Associate Director, Center for Information Security Research and Education*
Bryan Nunez, *Program Officer at Open Society Human Rights Initiative*
Bruce Schneier, *Security Technologist and Author*
Alix Dunn, *Executive Director and Co-Founder, the engine room*
Susan McGregor, Assistant Director, *Tow Center for Digital Journalism*
J. Ayo Akinyele, *Research Scientist*
Collin Anderson, *Independent Researcher*
Nadia Eghbal, *Investor, Social Researcher*
Stefania Milan, *Assistant Professor of New Media and Digital Culture, University of Amsterdam*
Emily Ratliff, *Senior Director of Infrastructure Security, Linux Foundation*
Mohamad Najem, *Advocacy and Policy Director, Social Media Exchange*