OPEN TECHNOLOGY FUND

2014 Annual Report

Open Technology Fund

Table of Contents

About Open Technology Fund

The Open Technology Fund (OTF) provides direct financial support and indirect, in-kind services to projects and people who expand and sustain global Internet Freedom, prioritizing tools for use in countries whose governments restrict freedom of expression on the Internet.

OTF supports research, development, and implementation of projects and initiatives that increase:

- **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 such as research and real-time monitoring of censorship behavior;
- **Privacy** enhancements, including the ability to be free from repressive observation and the option to be anonymous when accessing the Internet; and
- **Security** from danger or threat when accessing the Internet, including encryption tools.

As in previous years, OTF's own effort in fiscal year 2014 was supported entirely by public funds. OTF supported many technology-centric efforts that foster freedom of speech, expression, association, and the press; sustained an open exchange of ideas and information; enabled unrestricted access to content online; protected users from retaliation by enhancing their privacy and security; and promoted a globally open and accessible Internet. In doing so, OTF strived to promote forward-thinking ideas and innovation, open philanthropy, alternative methodologies, emerging technologies, new approaches, and social responsibility. We are committed to collaboration, transparency, and accountability.

Executive Summary

The Open Technology Fund completed its third year of operations in 2014. This year, OTF supported diverse efforts that significantly increased Internet Freedom globally, as measured by the number of people able to experience a more open, secure Internet, and by advancing useful technologies.

Our work continues to be focused exclusively on supporting global Internet Freedom. With increasingly restrictive regulations in a growing number of nation-states, and a sharp rise in sophisticated attacks against the people and organizations who support a more civil and democratic society, the need for OTF support is greater than ever. 2014 saw a tightening of censorship in Russia, Southern Africa, Latin America, Southeast Asia, and China, while high-profile targeted security breaches on large organizations and government agencies continued to feature prominently in the news.

The OTF program's credibility and leadership within the Internet Freedom community was further strengthened this year by word-of-mouth and technological successes like TextSecure's partnership with WhatsApp.[1] This year, the use of OTF-supported tools increased from hundreds of thousands to hundreds of millions of regular users in 2014. By leveraging social network effects, we expect to expand to a billion regular users taking advantage of OTF-supported tool and Internet Freedom technologies by 2015's end. OTF projects have also made notable technological advances that ensure a resilient open Internet, including novel methods to circumvent repressive Internet blocking, fruitful partnerships with other public and private organizations, and original research into emerging threats to Internet Freedom. For our part, the OTF team reviewed and responded to nearly 400 requests for funding totaling over $65 million in 2014 alone, and expended nearly 90 percent of our program budget on direct and indirect support for more than 80[2] projects this year.

OTF expanded our scope of support with the addition of in-kind and technical assistance programs. This year, OTF launched several fellowship programs to deepen collective knowledge and capacity and to promote the research and collaboration of individuals. These fellowships include the Information Controls Fellowship, Emerging Technology Fellowship, Rapid Response Fellowship, Secure Usability Fellowship, and the Digital Integrity Fellowship.[3]

In addition, OTF designed and implemented several in-kind labs and began developing an Incubator initiative, ranging from those aimed at strengthening the Internet Freedom Community to those making technological tools localized and more user friendly.

Finally, pursuant to our congressional mandate to leverage OTF's contribution as a major funder to the greater Internet Freedom community, our program helped open up nearly 100 million dollars of private funds to Internet Freedom efforts.[4] Our report includes information about our work with those funders and how we have enhanced the Internet Freedom funding community overall.

Details of OTF's 2014 efforts are presented below.

[1] Encryption Made More Accessible: https://www.opentechfund.org/article/encryption-made-more-accessible

[2] 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 security audits, usability audits, and localization efforts.

[3] Supporting awesome individuals, OTF's Fellowship Programs: https://www.opentechfund.org/fellowships

[4] S.1372 - Department of State, Foreign Operations, and Related Programs Appropriations Act, Fiscal Year 2014
113th Congress (2013-2014), Global Internet Freedom Sec. 7072. (a) https://www.congress.gov/bill/113th-congress/senate-bill/1372/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 2014

The Internet is integral to global society, serving both as a borderless public space and as a set of links that connect people. The Internet is widely used to access and share ideas and information, build community, and challenge repressive restrictions on our basic freedoms.

The ongoing struggle for free expression has only intensified for those online. 2014 saw an influx of attacks on people's right to global Internet Freedom, ranging from increased monitoring and censorship of communications to escalation in legislation designed to restrict and punish free expression online. As a result, journalists, activists, and whistleblowers all faced more severe retaliatory and repressive consequences when their digital security measures fell short.

The list of examples is too long for this report, but includes the following. In Turkey, Internet Freedom was further suppressed as the Turkish government expanded censorship efforts and cracked down on people using social media tools. The Turkish government passed two amendments to a pre-existing Internet Law 5651—already widely considered draconian—as a means to increase censorship controls, and increased the ability to block websites more simply and arbitrarily than before. In the period leading up to local elections, the government silenced discussion by blocking access to social media sites YouTube and Twitter. At the time, then-Turkish prime minister and current President Recep Tayyip Erdoğan vowed to "eradicate Twitter."[5] Months later, Erdoğan told the Committee to Protect Journalists that he is "[...] increasingly against the Internet every day."[6]

Russia honed its attempts to disable access to secure communications technologies. Notably, Russia made an offer of a $110,000 reward to anyone who could break the security protections offered by the Tor Network.[7] The Chinese-controlled Hong Kong government deployed both Distributed Denial of Service attacks (DDoS)—attacks making online websites or services unavailable for periods of time—and surveillance technology against citizens demanding universal suffrage.[8] During the Umbrella Revolution, the authorities blocked citizens' access to Instagram rather than let it be used by democracy-supporting protesters.[9]

Six Iranians were arrested in May 2014 for posting a YouTube dance video set to popular musician Pharrell's "Happy." The Iranian government continued to block most major social media tools (including YouTube, Facebook, and Twitter) along with tens of thousands of websites, especially those pertinent to international news, the political opposition, and human rights.

Thailand, already home to some of the most restrictive speech laws in the world, is now under junta control. The military government forbids online criticism of the army and orders ISPs to censor the Internet as the new government sees fit.[10]

[5] Turkey blocks Twitter, after Erdoğan vowed 'eradication', Hurriyet Daily News, March 20, 2014, http://www.hurriyetdailynews.com/turkey-blocks-twitter-after-erdogan-vowed-eradication.aspx?pageID=238&nID=63884&NewsCatID=338

[6] Turkey's Erdoğan Says He Is 'Increasingly Against the Internet Every Day', Newsweek, October 3, 2014, http://www.newsweek.com/turkeys-erdogan-says-he-increasingly-against-internet-every-day-275014

[7] Putin Sets $110,000 Bounty for Cracking Tor as Anonymous Internet Usage in Russia Surges, Bloomberg, July 29, 2014, http://www.bloomberg.com/news/articles/2014-07-29/putin-sets-110-000-bounty-for-cracking-tor-as-anonymous-internet-usage-in-russia-surges

[8] The Invisible Violence of Cyber War in Hong Kong's Umbrella Revolution, Global Voices Advocacy, October 6, 2014, http://advocacy.globalvoicesonline.org/2014/10/06/the-invisible-violence-of-cyber-war-in-hong-kongs-umbrella-revolution/

[9] The Revolution Will Not Be Instagrammed, Foreign Policy, September 28, 2014, http://foreignpolicy.com/2014/09/28/the-revolution-will-not-be-instagrammed/

[10] Thailand Internet Censorship: Government Orders Service Providers To Block Criticism, Take Down Content, International Business Times, December 30, 2014, http://www.ibtimes.com/thailand-internet-censorship-government-orders-service-providers-block-criticism-take-1770220

Vietnam also cracked down on netizens' rights to free speech, with at least 27 bloggers and citizen journalists currently imprisoned.[11] The Vietnamese government and government supporters also engaged in creative attacks against journalists and news outlets by using existing abuse reporting mechanisms in large social media platforms, like Facebook, to execute de facto content takedowns.[12] In South America, Venezuela responded to widespread government protests by blocking Twitter, pulling the plug on critical media outlets, and creating a new government institution with the power to "unilaterally classify and censor any information it sees as a threat to national security."[13]

North Korea was allegedly behind a major cyber attack, when the Sony Corporation became the victim of a high-profile data breach that compromised the personal information of hundreds of employees.[14] The incident underscored the necessity and importance of proper cyber security and the threat state actors can pose to ordinary netizens, regardless of borders or nationality.

No country attacked the open Internet more aggressively than China. The Chinese Communist Party further curtailed Chinese citizens' ability to circumvent the Great Firewall (GFW), moving the Internet in that country toward becoming a domestic intranet[15]. Circumvention methods commonly used to get around censors were blocked more effectively than ever, even expanding beyond public VPNs to shut down many private VPNs.[16] Even more troubling is the expansion of the GFW itself, as China's formidable censorship and surveillance methods increasingly affect Internet users abroad,[17] China now seeks to export its censorship technology to other repressive regimes (such as Iran[18]) that hope to replicate China's extensive Internet controls.

The above are just a few examples, shedding light on the stark reality that **global Internet Freedom declined significantly in 2014**. Freedom House's "Freedom on the Net 2014" report found that of 65 countries analyzed, 36 had experienced decreases in freedom.[19] Worrisome trends included data localization requirements, self-censorship by women and LGBT rights' advocates, increased retaliatory intimidation of online voices, and eroding cyber-security.

It is now more necessary than ever to maintain a free and open Internet to enable the free flow of ideas and information to anyone, anywhere, throughout the world. The freedom and empowerment of all people is the basis for a free and democratic world—and preserving the integrity of an unrestricted Internet is paramount to OTF's mission. The Open Technology Fund is committed to allowing the Internet to be what it was meant to be: safe, free and open, both of the people and for the people.

[11] Vietnam Arrests 65-Year-Old Blogger for Posting 'Bad Content,' Vice News, December 1, 2014, https://news.vice.com/article/vietnam-arrests-65-year-old-blogger-for-posting-bad-content

[12] Facebook's Report Abuse button has become a tool of global oppression, The Verge, September 2, 2014, https://www.theverge.com/2014/9/2/6083647/facebook-s-report-abuse-button-has-become-a-tool-of-global-oppression

[13] Venezuela's Internet Crackdown Escalates into Regional Blackout, Electronic Frontier Foundation, February 20, 2014, https://www.eff.org/deeplinks/2014/02/venezuelas-net-crackdown-escalates

[14] FBI Says North Korea Behind Sony Hack, The Wall Street Journal, December 19, 2014, http://www.wsj.com/articles/fbi-says-north-korea-behind-sony-hack-1419008924

[15] China Clamps Down on Web, Pinching Companies Like Google, The New York Times, September 21, 2014, http://www.nytimes.com/2014/09/22/business/international/china-clamps-down-on-web-pinching-companies-like-google.html

[16] China's Great Firewall Is Rising, Foreign Policy, February 3, 2015, http://foreignpolicy.com/2015/02/03/china-great-firewall-is-rising-censorship-internet/

[17] Why Internet users all around the world should be worried about China's Great Firewall, The Washington Post, February 2, 2015, https://www.washingtonpost.com/blogs/worldviews/wp/2015/02/02/why-internet-users-all-around-the-world-should-be-worried-about-chinas-great-firewall/

[18] China's Newest Export: Internet Censorship, U.S. News & World Report, January 30, 2014, http://www.usnews.com/opinion/blogs/world-report/2014/01/30/china-is-exporting-internet-censorship-to-iran

[19] Freedom on the Net 2014, Freedom House, December 2, 2014, https://freedomhouse.org/report/freedom-net/freedom-net-2014#.VaAx9flViko

Key Results from Fiscal Year 2014

Growth in Programmatic Effectiveness and Impact

OTF expanded its programmatic capacity and effectiveness in 2014 by increasing the number of people benefiting from OTF-supported technologies, while making Internet more open overall. 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 700 million people regularly use OTF-supported technology to circumvent restricted Internet connections, strengthen their online security, and enhance their digital privacy;
- OTF supported security audits of 28 Internet Freedom projects, identifying in total 1,170 privacy and security vulnerabilities;
- OTF's Localization Lab, in partnership with Transifex, enabled translations of Internet Freedom tools and ensured their accessibility to a global audience; the Localization Lab now supports 32 projects with 2,557 participating individuals contributing to the submission and verification of over 29,600 translated texts in 212 languages and dialects;
- OTF collaborated with the Vietnamese netizen community to create a rapid response procedure with popular social networking platforms to unblock and protect online accounts of activists under immediate threat of censorship and surveillance;
- To meet the expanding need for individuals to work on Internet Freedom technology, OTF launched a number of collaborative fellowship programs, including the Information Controls Fellowship Program (ICFP), Emerging Technology Fellowship Program (ETFP), and the Secure Usability Fellowship Program (SUFP), receiving over 140 applications for support to perform individual research, analysis, and development work that are critical to the growth of future efforts and capacity of the Internet Freedom community;
- In September 2014, OTF held its third annual Summit in Washington D.C. with more than 70 participants, including OTF-funded project team members, Advisory Council members, congressional staffers, and experts from the greater Internet Freedom community to discuss challenges, innovations, strategies, and needs in the the field of global Internet Freedom;
- The OTF Legal Lab expanded to include new law school and law clinic partners providing legal resources for OTF projects needing pro bono legal advice on issues ranging from OPEC waivers to incorporation;
- OTF launched the Community Lab in 2014 to advance the knowledge and expand the capacity of the community through collaborative work sessions on subspecialties such as mobile encryption, on emerging practice areas, and on strategic coordination of significant community events.

Organizational Efficiency

- Nearly 90 percent of OTF's program budget was used to directly support more than 80[20] projects, initiatives, and lab support through 2014;
- The OTF Team reviewed and responded to nearly 400 requests[21] for funding totaling over $65 million in 2014 alone;

[20] 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 security audits, usability audits, and localization efforts.

[21] This number includes the various types of funding and support that OTF makes available publicly, including applications for various funds, fellowships, rapid response, and labs.

- 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, Kavita Philip (University of California Irvine), Nadia Heninger (University of Pennsylvania), Joana Varon Ferraz (Coding Rights), and Ben Laurie (Google);
- OTF internally reviewed our own processes and procedures to streamline our workflow and to ensure consistency and compliance with applicable rules and regulations.

Civil Society and Governmental Outreach

- The OTF team engaged in direct support of citizen journalists by meeting and working directly with Vietnamese and Venezuelan bloggers and journalists, among others, to demonstrate and train in OTF-supported Internet Freedom technologies;
- OTF supported numerous analytical and research reports, including *Internet Access and Openness in Vietnam,* a comprehensive report on the ICT landscape in Vietnam, and three reports published by SecondMuse: *A Needfinding Framework for Internet Freedom, Understanding Internet Freedom: Vietnam's Digital Activists; and Understanding Internet Freedom: The Tibetan Exile Community*;
- OTF held regular meetings to increase collaboration and coordination with other Internet Freedom and Human Rights Technology funders;
- OTF and its project leaders participated in multiple informational briefings for congressional staff and other stakeholders concerned with foreign affairs, human rights, and Internet Freedom;
- OTF worked with Internet Freedom technologists, researchers, and policymakers while participating in key conferences, including the Stockholm Internet Forum, RightsCon Conference, Personal Democracy Forum, the Symposium on Usable Privacy and Security (SOUPS), Open Knowledge Festival (OKFest), Hackers on Planet Earth (HOPE), the International Human Rights Funders Conference, 31st Chaos Communication Congress Conference, Free and Open Communications on the Internet (FOCI), and USENIX Symposium on Networked Systems Design and Implementation.

Unlocking Additional Funding

- OTF further 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 global Internet Freedom funding and helped increase globally available funding by unlocking over 50 million dollars of private funds for use in Internet Freedom efforts in 2014 alone—and nearly 100 million dollars since 2012;
- Through active coordination with other donors, OTF more than quadrupled the impact of 2 million in public dollars by collaborative joint funding, expanding the total for these projects to over 8 million dollars.

Working Together for Greater Internet Freedom

Actively engaging other funders and experts to expand an open Internet.

Funders

As a leader in the human rights and Internet Freedom technology space, OTF advises, lends expertise to, and helps develop capacity for a variety of other funders' human rights technology investments. In FY 2014, we worked with several funders in the field, including BBG's Internet Anti-Censorship, The U.S. Department of State/DRL, USAID, BBC & DFID (U.K.), Deutsche Welle (Germany), SIDA (Sweden), and Hivos (Netherlands).

On the privately supported funding side, we shared our experience and expertise with the Ford Foundation, Open Society Foundations, Access, Google, and the Linux Foundation. OTF is on the Advisory Council of the Linux Foundation's Core Infrastructure Initiative with private companies, whose participants include Verizon, Samsung, Amazon, Google, IBM, Cisco, Intel, HP, and many others. Similarly, subject matter experts from the Ford Foundation, Open Society Foundations, and Google volunteer on OTF's Advisory Council. OTF also continued to expand and cultivate a primary Human Rights Technology (HRT) community through mailing lists and other mechanisms. As a result, OTF's transparent and open processes have become a model used by private funders, including the requirement that all technology projects receive a third-party security audit.

Distribution and Collaboration

OTF projects leveraged large-scale free distribution through corporate partnerships. Through our partnerships with private companies WhatsApp and Cyanogenmod, more than 600 million users are now able to use TextSecure daily.

On the research side, OTF partnered with the Citizen Lab at the University of Toronto to support practical research hosted at premier research institutions: Georgia Tech, Stony Brook, Ranking Digital Rights, Rice University, the University of Washington, and Oxford Internet Institute. In 2014, OTF and Citizen Lab launched the Information Controls Fellowship Program to cultivate research, outputs, and creative collaboration in the area of repressive Internet censorship and surveillance.

And because young Internet Freedom projects are predominantly entrepreneurs, they need lawyers too. OTF partnered with several U.S. and EU law schools, including Harvard Law School and UC Hastings, to generate public service legal resources tailored to entrepreneurial technology developers (examples include export control regulations, intellectual property law, privacy laws, corporate law, and nondisclosure agreements).

Empowering OTF Projects

OTF provided new and underresourced ICT funder partners in the human rights and Internet Freedom space with crucial services and non-OTF projects with in-kind resources: code security audits, usable security audits, access to secure servers, localization/translation services resulting in nearly 30,000 translated texts into over 200 languages, and rapid response funding and access to community support in times of emergency. These additional support mechanisms holistically support the ICT community and the sustainable life-cycle of the project, ensuring the effectiveness of OTF-contracted deliverables, and advance digital protections globally for frontline practitioners who do not have direct relationships with OTF.

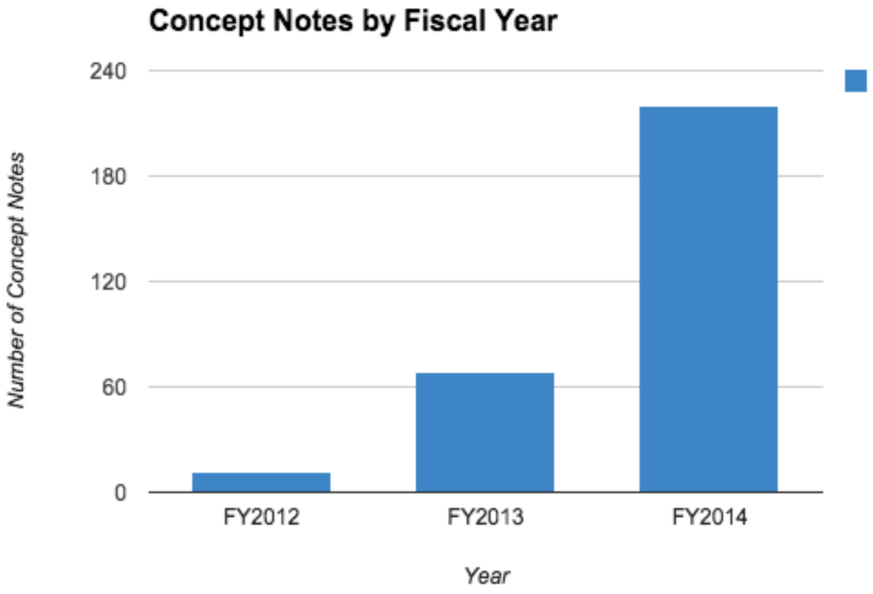
OTF has built strategic guidance into its core with an external Advisory Council of leading experts who review funding proposals. These experts include Red Hat's Chief Strategist, EFF's Director for International Freedom of Expression, and key people from Google, Mozilla, Etsy, Harvard's Berkman Center, and UC Berkeley.

Trends from FY2014

In 2014, OTF received the largest number of requests for support in the history of its operations. Overall, OTF received more than 345 applications for direct support of some kind (Concept Notes, Fellowships, Rapid Response). The total number of requests for OTF support in 2014 exceeds 450 when including in-kind service requests, such as applications for security audits, access to localization services, or community building support.

Concept Note Submissions and Increased Need

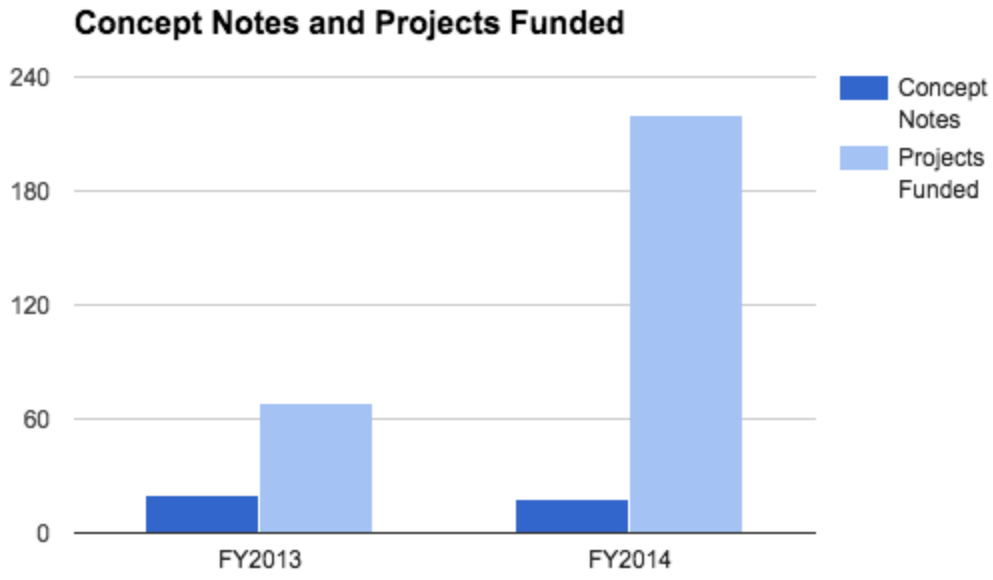
The political, censorship, and technological climate of 2014 resulted in a growing need for assistance around the globe. OTF saw a dramatic increase in requests for support as a result of the significant increase in restrictive regulations, sophisticated censorship tactics, and targeted attacks. These requests were submitted by many new and diverse applicants, signaling increased awareness of OTF within the Internet Freedom community. In numbers, OTF received 220 project concept notes requesting more than $60 million. In comparison, we received 68 concept notes requesting $17 million in 2013, and only 12 concept notes in 2012.



While we funded less than 30 percent of the concept notes received last year,[22] in 2014 we contracted only 18, or 8.1 percent, of the 220 requests due to budgetary constraints.[23] Unfortunately, the vast majority of the requests OTF declined represented viable efforts that would have advanced Internet Freedom. Given that OTF continues to spend the vast majority of its programmatic budget on supporting people and projects, OTF's ability to positively increase Internet Freedom is currently limited only by budgetary constraints.

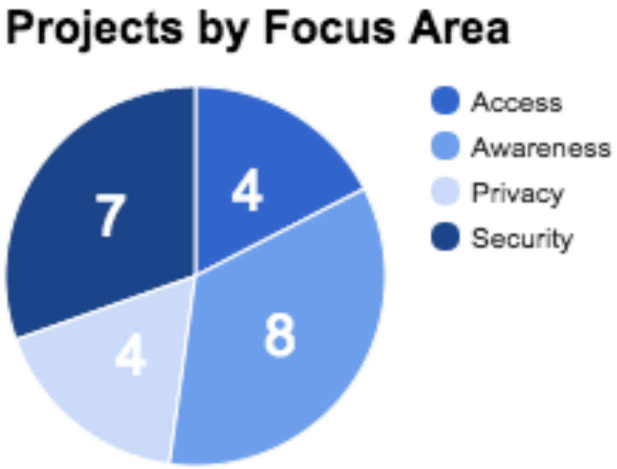
[22] In 2013, OTF funded 20 out of the 68 concept notes we received.

[23] Requests include types of support other than concept notes.



Concept Notes Breakdown

In 2014, the OTF team actively managed 23 projects[24] in total, excluding Labs and Fellowships. Of these, four were Access projects, eight were Awareness, four were Privacy, and seven were Security. This variety of support areas complies with legislative guidance which includes “research of key threats to Internet Freedom,” “enhanc[ing] digital security training and capacity building for democracy activists,” and “continued development of technologies that provide or enhance access to the Internet.”[25]

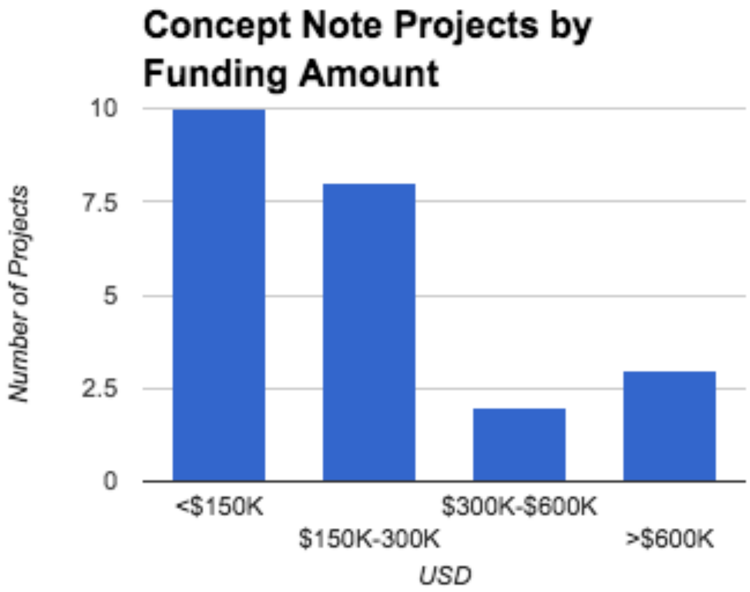


[24] This number includes 18 projects newly contracted in 2014, and five projects from previous years that completed in 2014.

[25] Consolidated Appropriations Act, 2014, Section 7080(b)(4) and (5). http://docs.house.gov/billsthisweek/20140113/CPRT-113-HPRT-RU00-h3547-hamdt2samdt_xml.pdf

Innovative Lower-cost Efforts

This year OTF continued to support smaller, innovative, emerging technologies with high impact potential. In 2014, the majority of the OTF projects came under $300,000, and almost half of the projects required less than $150,000. This reflects the need for a continuous and dynamic set of Internet Freedom tools that address the myriad of challenges faced by people in target areas.

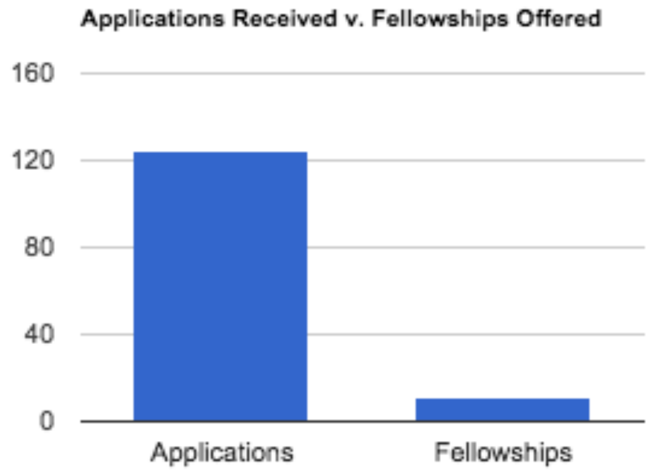


Innovative Support for People and Projects

OTF is committed to diversifying and strengthening the Internet Freedom ecosystem through responsive and effective funding mechanisms. To that end, OTF introduced several new methods of direct and indirect support to the greater Internet Freedom community and independent researchers, developers, and experts.

First, we began awarding fellowships directly to individuals to pursue research and development in the area of counter-censorship and counter-surveillance within repressive environments. During FY2014, OTF launched five different fellowship programs: Information Controls, Secure Usability, Digital Integrity, Emerging Technology, and Rapid Response. These fellowship programs are complementary to each other and to our concept note processes, and are positioned to address the broadening spectrum of challenges to Internet Freedom. The fellows are selected via a competitive, open application process, modeled after our concept note submissions in procedure, but oriented to better support individuals.

OTF received 125 fellowship applications for the Information Controls and Secure Usability fellowships in 2014. Of these applications, OTF funded 11 fellowships after a rigorous review process which included significant due diligence reviews of host organizations that could support each fellow.



Second, OTF further expanded the scope of our labs and introduced the idea of an OTF Incubator. The Incubator combined existing in-kind services to formulate a structured program for projects who need strategic guidance rather than direct funding. These efforts—security audits, usability assessment, localizations, etc.—enable OTF to support positive growth for many more Internet Freedom projects by helping them become more reliable, secure, user-friendly, and accessible. Labs strengthen the technological and organizational structure of OTF-supported projects. And this, in turn, increases the safety and security of the people who use these tools to communicate.

Details about OTF Fellowships and the OTF Incubator can be found in the Program Overview section of this Annual Report.

FY 2014 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

- ***Access*** to the Internet, including technology 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 such as research and real-time monitoring of censorship behaviors;
- ***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 threat 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, enabling relevant development;
- 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.

Programs

The core of OTF's work consists of providing needed funding and services to projects and people: *Funding* provides funds directly to a project or a person via a contract. *Services* are OTF-provided goods, commodities, or other in-kind services delivered to a project. Listed below are programs OTF supported in 2014:

How we supported projects in 2014

General Internet Freedom Fund

Projects and funding amounts are listed below:

The General Internet Freedom Fund continued to be the primary open call for OTF-supported projects that promote free expression, fundamental freedom, human rights, and 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. OTF expects approximately 70 percent of its annual funds to be 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: Access, Awareness, Privacy, Security.

Access Projects

OpenNet Africa

FY2014, $173,715

The Internet is becoming less free in East Africa, but knowledge about and skills to counteract these threats are severely lacking. This project aimed to close that gap in three steps: (1) work with local ICT for Development (ICT4D) Innovation hubs and human rights defenders to test and, where relevant, localize tools, particularly those developed through OTF support; (2) conduct skills building and awareness raising on Internet Freedom, privacy, and security online; and (3) research and document the nature of threats to access, privacy, and security online in East Africa.

Revolico, Offline Internet Content Generator
FY2014, $50,000
The main purpose of this effort is to provide a way for the Cuban people to access Internet content in an offline, collaborative, and uncensored manner. Currently, a robust organic network of offline content consumers exists on the Island. To that end, Open Cuba worked on a desktop application that will be able to display, import, share, and distribute packages of offline Internet content. The content is meant to be consumed both within the app and to be adapted to the most popular devices such as DVD players. Furthermore, both the app and the exported package of content will be designed to be easily sharable using USB drives or any other data-storage devices.

Lantern
FY2014, $791,506
Lantern focuses on ease of use, speed, and unrestricted access to the Internet. Unlike other access tools, Lantern utilizes peer connections as a source of Internet connectivity when servers are unavailable, and is particularly useful in repressive environments like Iran, China, and parts of Latin America. Lantern Mobile and the Lantern Anti-Censorship Platform build on Lantern Desktop's success to bring their platform to Android mobile users.

Awareness Projects

GreatFire
FY2014, $114,000
Greatfire.org implements the concept of "collateral freedom" on the Internet by creating mirrors of websites that are hosted on cloud servers, mainly Amazon Web Services (AWS). AWS uses HTTPS, which means that governments cannot selectively block URLs being hosted there. The strategy has resulted in the successful hosting of mirror sites for Reuters China, China Digital Times, and FreeWeibo. This success resulted in China recently, and unsuccessfully, deploying the "Great Cannon" in an effort to shut down GreatFire. This project enhances the features and security of the Android and iOS apps, provides an open-source version of the collateral freedom platform and associated documentation for third party replication, and enables censorship-resistant sharing of mirror sites on social networks and email.

GlobaLeaks
FY2014, $235,440
GlobaLeaks is the first open-source data, evidence, and anonymous sourcing framework. It empowers anyone to easily set up and maintain a platform. GlobaLeaks can help many different types of users: media organizations, activist groups, corporations, and public agencies. The current project integrates a variety of new and requested features primarily focused on expanding the capabilities and security of the platform while simultaneously increasing usability. An evergrowing list of GlobaLeaks's successful implementations, including Tunisia, Venezuela, Nigeria, Zimbabwe, and Zambia, are listed here.[26]

SR Labs/GSMMap
FY2014, $364,000
Gsmmap.org is a popular web site that provides detailed assessments of more than one hundred cellular network operators as well as tools that users can use to check on the security of their mobile network. This project aims to create tools to detect and—where possible—prevent abuse of mobile network and SIM card vulnerabilities, and to spread the tools to end users as widely as possible. These tools are meant to help phone users avoid insecure communications and demand better protection from technology providers.

[26] https://en.wikipedia.org/wiki/GlobaLeaks#Implementations

Transparency Toolkit

FY2014, $68,002

Transparency Toolkit is an open-source software that lets journalists, activists, and human rights workers bundle together tools to collect, combine, visualize, and analyze documents and data. This project aims to improve the usability of Transparency Toolkit among journalists and human rights groups and make the Toolkit useful enough to be utilized in investigations by outside organizations. Transparency Toolkit also plans an integration with GlobaLeaks to make it easier for users to analyze the documents that they receive through the system.

SecondMuse Web-Based Internet Freedom Needfinding Framework

FY2014, $74,974

With OTF support, SecondMuse has developed and implemented a framework for understanding user needs in the context of Internet Freedom. This framework guides development of Internet Freedom tools for use in at-risk communities living under repressive regimes, while respecting people's cultural diversity, security, and privacy. This particular project supports a needfinding engagement utilizing this framework. It also increases the impact of the framework through a dynamic and engaging online[27] version of the framework that can be easily updated and modified.

SecondMuse-Vietnam Needs Finding

FY2014, $42,030

SecondMuse conducted a needs assessment and training with high-risk bloggers traveling from Vietnam to understand their digital security needs via a human-centered design approach to identify communication priorities, security behavior and habits, threat models, cultural and contextual usability needs, and what tools they are using or not using, and why?

SecondMuse-Middle East/North Africa Needs Finding

FY2014, $43,850

SecondMuse conducted a needs assessment and training with digital activists throughout the MENA region to understand their digital security needs via a human-centered design approach to identify communication priorities, security behavior and habits, threat models, cultural and contextual usability needs, and what tools they are using or not using, and why.

Privacy Projects

Tor Browser Bundle

FY2014, $900,000

For the past ten years, the Tor Project has been providing the world with technology and research essential to protecting privacy and freedom of speech online. Tor's community of over a million daily users and almost 10,000 relay and bridge operators has played an influential role in conflicts around the world, including in Egypt, Tunisia, Iran, and elsewhere. With OTF support, Tor is working on a two-year development project to make sure the Tor software continues to provide world-class anonymity and censorship circumvention solutions. This combined effort describes two primary objectives: core Tor development work to make sure the underlying technology remains strong, and Tor Browser development work to ensure safety and usability for the packaging and interface side of Tor.

Open Whisper Systems

FY2014, $900,000

Open Whisper Systems (OWS) produces some of the leading encrypted mobile communication tools such as TextSecure, RedPhone, and Signal. OWS intends to turn TextSecure, the leading encrypted text message tool, protocol, and infrastructure into a seamless open standard for asynchronous messaging. The protocol is being made adaptable for other implementers such as WhatsApp. Over the next year, Open Whisper Systems

[27] http://internetfreedom.secondmuse.com/needfinding/

will escalate their efforts and make a concerted push to focus on multidevice and broad platform support, make integrating the TextSecure protocol into existing apps (including email clients) simple, and integrate secure voice into a single offering.

Security Projects

Proxy Looking Glass
FY2014, $63,000
Proxy Looking Glass (PLG) aims to build a safe, feasible alternative for technical data collection for forensic analysis of attacks, intrusions, interference, or censorship events inside countries with repressive regimes. PLG aims to analyze the limitations of existing tools and technologies, describe the mechanisms, tools, and methods that will allow normal readers to conduct coordinated experiments from their Internet connections, and increase awareness of Internet tampering in selected countries.

Security First/Umbrella App
FY2014, $150,031
Umbrella is a mobile application that provides all the information needed for a human rights defender to operate safely. It will provide users with how-to guides, risk assessments, and checklists, ultimately allowing users to securely and anonymously save their settings and track their progress. Umbrella has completed its first round of user testing and content feedback, and is currently undergoing further development. Given their focus on Human Rights, Security First is working closely with Amnesty International and UNICEF, among others.

Martus
FY2014, $235,000
The Martus Secure App Generator is built around the long-standing secure information collection tool known as Martus. The Secure App Generator will be an open-source tool that creates custom versions of Martus. This mechanism will meet the demand of many organizations which collect sensitive data on human rights violations to have secure, easy-to-use data collection tools and for users to collect and secure information from at-risk sources in the field. The application will be easy to use and equipped with capable back-end tools for presenting and analyzing the securely collected information.

PushSecure
FY2014, $266,520
PushSecure is a decentralized push service that allows app developers to provide interoperable push messaging in a way that eliminates the service’s knowledge of message content and minimizes any identifiable metadata. By doing so, PushSecure protects users in repressive countries that employ sophisticated and surveillance tactics that rely on the collection of metadata. This specification ultimately gives end-users much more control over their communications and metadata trail, without sacrificing modern usability expectations for asynchronous push messaging. This project completes the client integration on both iOS and Android, test servers, ensure device compatibility, and deploy the service to production.

Qubes (Operating System tool)
FY2014, $160,000
Qubes is a security-focused free and open-source operating system that tries to secure typical workflows through controlled interaction, and that minimize the attack surface for adversaries—i.e repressive host governments—as much as possible through compartmentalization. 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. This project seeks to make the system more usable and secure through the introduction of preconfigured, out-of-the-box ready features.

Tails (Zwiebelfreunde)
FY2014, $208,000
Tails is a live operating system that can be started on almost any computer from a DVD, USB stick, or SD card. Tails provides a platform to solve many digital threats by “doing the right thing” out of the box by default, protecting even less tech-savvy users from the most likely and highest-impact risks. This project will

make a variety of needed technical improvements to Tails including scaling infrastructure, updating underlying software, upgrading the mail client, and improving the quality assurance process.

How we supported people in 2014

Information Controls Fellowship

FY2014, $945,360

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 selected eleven inaugural fellows this fall. The ICFP is jointly administered with Citizen Lab at the Munk School of Global Affairs at the University of Toronto. Our current host organizations include: Citizen Lab, Munk School of Global Affairs at University of Toronto; University of New Mexico, Department of Computer Science; Stony Brook University, Department of Computer Science; Ranking Digital Rights, New America Foundation; NOISE Lab, Princeton University; Security and Privacy Lab, Princeton University; University of Washington; Berkman Center for Internet & Society, Harvard University; Centre for Intellectual Property and Information Technology Law, Strathmore University Law School; Program on Liberation Technology, Stanford University; Computer Security Lab, Rice University; International Computer Science Institute, University of California, Berkeley; and Electronic Frontier Foundation.

Emerging Technology Fellowship

FY2014, $188,880

The Emerging Technology Fellowship Program (ETFP) grows the community of Internet Freedom defenders and its collective expert capacity by supporting individual technologists, researchers, and advocates. Support is primarily available for individuals with novel ideas that address emerging threats to global Internet Freedom. It is also available for individuals working to increase the effectiveness or awareness of privacy enhancing, digital security, anti-censorship, and circumvention technologies that may not be new or novel but are widely considered crucial to defending Internet Freedom globally.

Secure Usability Fellowship

FY2014, $221,600

The Secure Usability 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.

Digital Integrity Fellowship (Launched)[28]

FY2014, $0

The online landscape frequently changes, making it very challenging for organizations to keep their safety and security strategy and policies up-to-date (if they have them in place at all). Meanwhile online security is a key priority for their target group—human rights defenders, who might be imprisoned or killed when their online or real identities become known. Many organizations do not have the skills, capacity, or funds for strategy, protocol creation, digital safety, and/or security trainings. Many other organizations might not even know the risks they pose to human rights defenders, or the need for organizational change around digital strategies. The aim of the Digital Integrity Fellowship Program is twofold, to keep human rights defenders safe and secure while they access their right to freedom of expression online by (1) scaling-up organizations that

[28] We received applications for this fellowship, but due to funding issues we plan to support them in 2015.

provide platforms to human rights defenders on their digital safety and security strategy and policies, and (2) providing space through fellowships to digital safety and security experts working within organizations that provide platforms to human rights defenders.

Rapid Response Fellowship (Launched)[29]

FY2014, $0

The Rapid Response fellowship program is 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. This fellowship is open to all individuals providing support and resources to mitigate highly time-sensitive and urgent digital threats to Internet Freedom and human rights. Collectively, OTF considers this network of individuals, host organizations, and service partners a set of federated nodes sustaining a global Internet Freedom Emergency Response Team. This fellowship provides support for technology-centric individuals who carry out emergency assistance to at-risk journalists, human rights defenders, NGOs, activists, and bloggers around the world who face digital threats to their free expression and speech resulting from rapid escalation in censorship and surveillance.

How we provide support through in-kind resources and services in 2014

Localization Lab

FY2014, $467,000

OTF's Localization Lab made Internet Freedom tools relevant to local conditions and usable to local users. Prohibitive costs and the limited availability of professional translators can prevent global deployment of Internet Freedom tools. To address these challenges, OTF has partnered with SecondMuse and Transifex to create an Internet Freedom localization hub built on Transifex' online crowd-sourced translation platform. We currently work with a number of partners, including Transifex and SecondMuse.

Community Lab[30]

FY2014, $588,660

Community Lab seeks to bring together and strengthen the Internet Freedom community through initiatives that cultivate deeper trust relationships, improve knowledge sharing, create synergies, and increase diversity. As the Internet Freedom community grows, so do the needs and challenges which must be solved by community strategies that bring forth collective vision and action, and properly navigate cross-cultural barriers. In addition, specifically for OTF, an increase in the number of funded projects implies greater need for community harmonization so that individuals can better share tools, API's, protocols, and technological expertise.

In the future, Community Lab will also generate intelligence about the state of various segments of the field, enabling OTF to better understand the ecosystem while gaining insight into where and how to target further investments. As well, the Community Lab will: generate research and insights to inform investments, design and host targeted research and development convenings intended to strengthen relationships, design and facilitate the annual OTF Projects Summit, provide OTF projects and community stakeholders with on-demand project advising, increase capacity building writ large, and strengthen community ties and increase collaboration between OTF and non-OTF communities.

Engineering Lab

FY2014, $575,453

The Engineering Lab included OTF's Secure Cloud Infrastructure, Amazon Cloud credits, Google Apps credits, and other engineering resources frequently needed by projects. Working with partners on the ground,

[29] We received applications for this fellowship, but due to funding issues we plan to support them in 2015.

[30] Service providers include Aspiration Technology.

OTF deploys high-capacity cloud infrastructure 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. We work with several partners including Greenhost, Powernetix LTD, and Santek Bilgisayar. The Engineering Lab currently supports 20 projects, with daily requests for access.

Usability Lab[31]

FY2014, $50,000

There are many open--source software projects that aim to help people — activists, journalists, and ordinary citizens — around the world communicate in privacy and security. Unfortunately, few of these software-development teams have the research expertise or design support to make tools that are truly usable. The resultant usability challenges hamper these tools' adoption. More critically, these challenges also lead to users developing inaccurate mental models about how the tools work – which in turn can give users a false sense of security and expose them to greater risk. As a response, OTF has 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 of Internet Freedom and human rights technology.

Red Team Lab

FY2014, $1,058,500

The Red Team reflects OTF's commitment to establishing a high standard for privacy and security in Internet Freedom technology. One component of this commitment is conducting independent technology audits on all of its technology-centric projects. These audits mitigate the risk inherent in funding cutting-edge technologies and strengthen the technical capacity of the project as well as the broader human rights and Internet Freedom technology community. OTF developed and published a methodology and framework in 2013 for evaluating technical audit reports from the perspective of a funder. Continuing this work, OTF currently offers in-kind audits to crucial Internet Freedom and human rights technology projects including those not funded by OTF. Partners include Cure53, iSEC Partners, Veracode, HackerOne.com, and Trevor Perrin.

Legal Lab

FY2014, $0

Legal Lab anticipated, assisted with, and responded to various legal issues unique to Internet Freedom projects at all stages. During the life of a project, a variety of legal questions can arise related to incorporation, IP issues, export laws, regional policy restrictions, mobile app Terms and Conditions, etc. We connected our projects with legal professionals and provided general information common to all Internet Freedom projects. Current legal clinic/pro bono partners include the Startup Legal Garage at UC Hastings, the Cyberlaw Clinic at Harvard Law School, Sidley Austin DC, and Covington SF.

How we addressed emergencies in 2014

Rapid Response Fund

FY2014, $155,634

The Rapid Response Fund is part of 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 2014, OTF provided emergency support to news outlets and human rights activists who experienced serious attacks against their websites and platforms. Going forward, OTF will offer financial support and technical services from trusted partners to resolve digital emergencies experienced by high-risk Internet users and organizations, such as bloggers, cyber activists, journalists, and human rights defenders. Applicants will also receive technological services from trusted service partners, and/or direct financial support from OTF.

[31] Service providers include Simply Secure.

Expenses Overview

Direct Support	**$ 6,351,542**
- *Projects*	*$ 4,840,068*
- *Access*	*$ 1,015,221*
- *Awareness*	*$ 942,296*
- *Privacy*	*$ 1,800,000*
- *Security*	*$ 1,082,551*
- *Fellowships*	*$ 1,355,840*
- *Rapid Response*	*$ 155,634*
Indirect Support (Labs)	**$ 2,739,613**
Total Salaries and Benefits	**$ 595,122**
Administrative	**$ 167,499**
GOE	**$ 80,530**
Travel	**$ 204,958**
Technical/Equipment	**$ 53,955**
Carryover to FY 2015	**$ 2,556,781**[32]

FY 2014 Total Expenditure	**$ 12,750,000**

[32] The nature of the public appropriations process creates a period of budget variability between fiscal years, the time utilized by congressional lawmakers, appropriators, and government agencies to determine and allocate the public budget. Following congressional allocation and appropriation, funds are distributed to OTF through the BBG. When there is a "continuing resolution" delaying the final appropriation, the BBG process can begin as late as the second quarter of the fiscal year. The BBG internal process varies by fiscal year and can sometimes further delay the distribution of funds to OTF and, therefore, by OTF.

There are periods in which this delay has slowed OTF’s ability to provide consistent support. Recognizing the need to bridge gaps caused by this variability and the importance of continuing Internet Freedom programs, Congress decided in 2014 to make Internet Freedom funds available as “no year funds” at the joint request of BBG IAC and OTF. These “no year” funds are available for obligation without fiscal year limitation. However, OTF strives to fully utilize each year's BBG allocation of appropriated Internet Freedom funds within the intended year to maximize the impact of our work. To allow for steady, uninterrupted support during this period, OTF allocated a small portion of FY 2014 funds for use in FY 2015.

Looking to the Future

Harnessing the power of individuals

OTF has repeatedly seen that individuals can create a huge impact in the field of Internet Freedom in ways that institutional and organizational actors cannot. As part of our ongoing effort to maximize the output potential of individuals working to promote Internet Freedom and strengthen that community of experts, OTF will offer three, six, and twelve-month fellowships focusing on Internet censorship and surveillance, secure usability of tools, rapid response, emerging technology, and digital integrity. In 2014, OTF supported 12 fellows, and in 2015 OTF plans to support at least 40 individuals through those five different fellowship programs. OTF has created partnerships with a number of international organizations to support these fellowships and, in 2015, plans to develop greater relationships with local organizations and individuals in different regions to enhance the capacity of local communities.

Diversifying Funding Pool

For the last three years, OTF has relied solely on public funds allocated by Congress. While that source of funding has been central and primary to our work, the nature of the congressional appropriations process requires OTF to work within the remit provided by Congress each year. In 2015, OTF will prioritize diversifying our funding pool in order to increase the quantity and expand the scope of support.

At the same time, OTF wants to encourage other organizations to get involved in the broader Internet Freedom work. We have successfully engaged and partnered with funders and corporations, as described in previous sections. However there is untapped growth potential in this area. OTF will continue to communicate and strategize with other funders to identify gaps in Internet Freedom space, and to appropriately respond to historically and technologically marginalized groups.

Greater Community Development

While OTF continues to be positively regarded within the Internet Freedom community, our priority is to increase use in at-risk communities. Our work is meaningless without direct, positive effects on the journalists, human rights activists, and everyday people working on the frontlines within repressive countries. OTF is increasing our public awareness through social media, outreach, open communication, and other available means. We want the people affected by the lack of Internet Freedom and those who support them to know that we are available to address, through our projects, the access, awareness, privacy, and security issues most relevant to them. This will require close collaboration with other nonprofit organizations, private funders, and advocacy organizations, and a sustained development of successful relationships with diverse communities. We understand that this kind of relationship-building necessitates a sustained effort from OTF, and we understand the importance of staying close to those living in restrictive Internet environments.

Empowering Internet Freedom Organizations: Incubator

Late in 2014, we leveraged the collective resources of all the OTF Labs — Red Team, Engineering, Localization, Legal, Communication, Community, Usability — to express our commitment to creating an Internet Freedom Incubator initiative. The Incubator is designed to grow the technological and institutional capacity of the people and organizations behind new and exciting Internet Freedom projects. We now want to push our existing efforts even further, making the Incubator a place where early-stage projects evolve into highly competent Internet Freedom developers. To do this in 2015, we will offer two different channels of Incubator support: a comprehensive boot camp that provides a strong knowledge base and lab support and an a la carte support service that provides specific support as needs arise. In 2015, we will continue to bolster and formalize processes for a more comprehensive initiative, while strengthening existing relationships with our partners in order to provide seamless assistance in each of the subject areas.

Challenges Ahead

In addition to the various restrictions we listed as examples in previous section, more severe repressive tactics have already been introduced in 2015 in the form of harsher penalties for information sharing, increased sophistication in government surveillance and cyber attacks, public-private data sharing agreements, aggressive censorship and access to information, and big data mining. We want to better anticipate both the technological advancements and changing regulatory environment to identify and fund tools that will best counteract those restrictions. That will not be easy. The Internet is by nature evolving and complex, and each success will spur new, distinct types of restrictions.

Conclusion

In 2014, OTF significantly expanded its scope, impact and ability to meet current and future online freedom challenges. While we are very proud of the accomplishments and impact of our team, the projects we support, and the greater Internet Freedom community this year, we are ever cognizant of the the hard work ahead. Sustainable unrestricted global Internet requires constant vigilance, creativity, and effort because the issues and challenges that affect its openness are complex and powerful. We hope, and believe, that our work in 2014 helped keep the doors open for all.

Appendix

Program Operation

Organizational Overview

The Open Technology Fund was created in 2012 as a program within Radio Free Asia (RFA). RFA is a private nonprofit grantee corporation created pursuant to an act of Congress in 1994, based in Washington, D.C. It is funded by an annual grant from the Broadcasting Board of Governors (BBG), an independent agency of the U.S. government.[33] On July 13, 2010, a bill was signed into law permanently authorizing RFA for federal funding and including a Sense of the Senate that RFA should receive additional funding for "Internet censorship circumvention."[34] The BBG established OTF within RFA to support Internet Freedom globally.

OTF reports to RFA's president, who in turn reports to the Radio Free Asia Board of Directors. The Broadcasting Board of Governors (BBG) is appropriated funds from which it provides a grant to RFA for legislatively mandated activities and provides oversight over the grant. The BBG is a bipartisan board with nine members, eight of whom are nominated by the President of the United States and confirmed by the U.S. Senate, including one designee as the Chairman of the BBG.[35] The ninth member *ex officio* is the U.S. Secretary of State. By law, no more than four members shall be from the same political party.[36]

The OTF Team in 2014

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.

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.

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 ensuring compliance with applicable laws and regulations.

Dan Meredith
OTF Director, RFA
Mr. Meredith joined RFA in January 2012 as OTF's inaugural director. He is responsible for OTF's day-to-day

[33] Public Law No. 103-236, April 30, 1994, available at http://uscode.house.gov/statutes/1994/1994-103-0236.pdf
[34] Public Law No. 111-202, July 13, 2010, available at http://www.gpo.gov/fdsys/pkg/PLAW-111publ202/pdf/PLAW-111publ202.pdf
[35] Current Broadcasting Board of Governors: http://www.bbg.gov/about-the-agency/board
[36] Establishment of the Broadcasting Board of Governors: http://www.bbg.gov/about-the-agency/history/legislation/#q304

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[37]
OTF Senior Program Manager, RFA
Mr. Lynn joined RFA in April 2012 as OTF's inaugural program manager. He leads OTF's research initiatives while participating in OTF's day-to-day operations and long-term planning.

Liz Pruszko Steininger
OTF Senior Program Manager, RFA
Ms. Pruszko Steininger joined RFA in April 2013. As senior program manager, she is actively engaged in OTF's day-to-day operations and long-term planning. She launched the Information Controls Fellowship and helped grow various OTF initiatives.

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.

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 several directly funded projects, OTF's Localization Lab and Communications Lab, and the Digital Integrity Fellowship 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, leading Emerging Tech fellowships, and serving as a liaison to the Director General 7.

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 co-manages Rapid Response Initiatives with Ms. Millet.

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*.

[37] Mr. Lynn took a sabbatical in August 2014 and returned April 2015.

OTF’s Advisory Council

In FY 2014, OTF expanded the Advisory Council to include 21 members. Since 2013, Kelly DeYoe exited the AC and Kavita Philip, Nadia Heninger, Joana Varon Ferraz, and Ben Laurie newly joined. The Advisory Council helps OTF gain a deeper understanding of current Internet Freedom challenges and opportunities, reviews project proposals, and helps shape the collaborative and collective work of the OTF program. OTF’s volunteer Advisory Council members assist with OTF’s unique highly technical and due-diligence needs to ensure a comprehensive and holistic proposal evaluation process.

Kevin Bankston, *Policy Director, New America Foundation’s Open Technology Institute*

Gustaf Björksten, *Technology Director, Access*

Matt Braithwaite, *Google*

Michael Brennan, *SecondMuse*

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, *Director of Security Engineering, Etsy*

Ben Laurie, *Software Engineer and Cryptoplumber, Google*

Katherine Maher, *Chief Communications Officer, 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, *Senior Policy Engineer, Mozilla*

Bruce Schneier, *Security Technologist and Author*

Ian Schuler, *CEO, Development Seed*

Joana Varon Ferraz, *Independent*

Jillian C. York, *Director for International Freedom of Expression, Electronic Frontier Foundation*