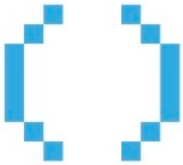
Annual Report - Fiscal Year 2013

March 2014

Open Technology Fund's (OTF) 2013 annual report provides an overview of its program, goals, and existing and future commitments to the larger Internet freedom community. It highlights important facets of OTF's work and the accomplishments and ongoing efforts of projects OTF supports around the world. This report allows the public a deep look inside OTF's internal processes. It concludes with a vision of OTF's future work in 2014 and beyond.



OPEN TECHNOLOGY FUND

The Open Technology Fund (OTF) is a program that utilizes public funds to support Internet freedom projects. We support projects that develop open and accessible technologies promoting human rights and open societies. We strive to advance inclusive and safe access to global communication networks.

Core Values

OTF supports freedom of speech and expression, freedom of the press, open exchange of ideas and information, freedom of association and unrestricted access to a free and open Internet. The OTF program works 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.

OTF supports projects and initiatives focused on increasing:

- **Access** to the Internet, including tools to circumvent website blocks, connection blackouts, and widespread censorship;
- **Awareness** of privacy and security threats and protective measures, including how-to guides and trainings for circumvention tools;
- **Privacy** enhancement, 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.

In doing so, OTF strives to:

- Advance **research into repressive Internet interference** on modern communication networks and the methodologies and technologies used to censor and to circumvent online censorship;
- Foster **development of technologies** that circumvent internet censorship, enable access with increased privacy and security from invasive online monitoring, interference and surveillance by repressive regimes; and
- Enable widespread and timely **implementation of solutions** to free people from repressive Internet interference.

Table of Contents

Executive Summary

The Internet is the global platform for information sharing, the exchange of ideas, and freedom of speech. The ability to communicate freely, collaborate, and seek information depends on a person's access to an unrestricted Internet and on the level to which one is able to exercise his or her right to freedom of expression. Internet freedom is free expression online. While the Internet is a platform for these fundamental freedoms, it is also a vehicle for violations of these same human rights every day. The Open Technology Fund (OTF) was created to support technology-based solutions to the complex challenges facing digital defenders of democracy, human rights, and fundamental freedoms around the world.

The Open Technology Fund is a Radio Free Asia (RFA) program created in early 2012 with U.S. Congressional funds and sustained through annual grants to RFA from the Broadcasting Board of Governors (BBG) to promote global Internet freedom and combat online censorship. Although RFA's mission is to support the free flow of information and press freedom to closed societies in Asia, the BBG has given OTF a global remit in order to carry out Congress' mandate to support Internet freedom in repressive societies worldwide. The BBG selected RFA to house its new global Internet freedom program because of its responsive and agile profile, nonprofit nature, and ability to a leverage private funding, among other factors.

This report covers Fiscal Year (FY) 2013 which was OTF's first full fiscal year in operation. In these twelve months, OTF has become a leader in protecting the fundamental human rights of free expression and access to information online. Every stage of OTF's work is guided by Article 19 of the United Nations Universal Declaration of Human Rights: **Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.**

In FY 2013, OTF received $4.3 million from the BBG. Nearly ninety percent of OTF's grant funds from the BBG were used in direct support of OTF's programmatic work, composed of 20 projects and initiatives aimed at promoting Internet freedom. Of this portfolio, 17 were groundbreaking anti-censorship and circumvention projects that increase unrestricted access, security and privacy for Internet users in censored environments worldwide. OTF also implemented three service-based initiatives to strengthening the Internet freedom community writ large by augmenting privacy and security standards, building localization capacity, and enabling rapid response to emerging Internet freedom challenges anywhere in the world.

Further amplifying its contribution, OTF made collaborating with public and private funders a key priority in order to maximize and leverage matching resources for Internet freedom. OTF strengthened its project selection review process' quality and capacity by increasing its Advisory Council to include additional relevant disciplines, expertise, knowledge bases and diversity. OTF's unique operating model has expanded opportunities for development and innovation across the burgeoning field of protecting human rights online. In FY 2013 OTF realized critical outcomes and strategic impact within the Internet freedom community to meet the rising demands of a repressed world. OTF's approach of supporting independent yet coordinated projects advances Internet freedom at a quicker pace, responding to the dynamic and changing nature of modern censorship and repression.

Key Results from Fiscal Year 2013

In Fiscal Year 2013, the OTF program:

- Supported the growth of censorship-resistant secure online chat and text messaging from 200,000 regular users to over 10 million globally;
- Funded the creation of the first open-source Mobile Human Rights Reporting tool capable of circumventing repressive firewalls and enabling voluminous data collection and analysis;
- Partnered with leading Internet security experts to conduct 30 technology code audits leading to the patching of 185 privacy and security vulnerabilities identified in both OTF and non-OTF-funded Internet freedom technologies currently used;
- Supported detailed security and privacy assessments of more than 100 mobile networks worldwide;
- Established and grew a localization platform of more than 1,400 people working to translate 30 tools and 1.7 million words into 180 languages and dialects including Arabic, Farsi, Korean, Tibetan, Mandarin, Spanish, Ukrainian, and Vietnamese;
- Publicly released four reports including *Collateral Freedom in China*, an exploration of Chinese circumvention technology; *How to Evaluate Technical Audits as a Funder*, a methodology for funders looking to conduct security audits; *Access and Openness: Myanmar 2012* an assessment of the telecommunication, censorship, and online safety landscape in Burma; and *Tools for Communication Security;*[1]
- Increased circumvention capacity in the Middle East and Asia by activating the first high-capacity Tor exit-node in South East Asia and establishing a Secure Cloud node in Istanbul, Turkey;
- Supported the creation of a Tunisian civil-society “hackerspace” defending Internet freedom for the region;
- Conducted eight informational training sessions for NGOs, journalists and human rights activists on anti-circumvention tools for use in regions where freedom of expression is continuously threatened;
- Pioneered increased transparency through full disclosure of OTF’s financial expenditures and programmatic operations online at www.opentechfund.org and in public reports;
- Diversified the OTF Advisory Council to expand the scope and breadth of expertise guiding OTF project decisions by tripling the Council from 6 to 18 members;
- Convened an Internet Freedom summit of OTF project teams, OTF’s Advisory Council, NGOs, and partner funders for in-depth discussion, technical collaboration, brainstorming coordinated solutions and strategic planning for the coming year;
- Received unprecedented interest from potential projects, vetting 68 concept note submissions requesting over $17 million, a fivefold increase from 2012;
- Significantly expanded OTF’s proposal and project evaluation system, making it easier to compare and monitor current and potential projects; and
- Maintained lean and agile operations, with nearly 90% of OTF’s budget - approximately $3.8 million - directly supporting programmatic work.

[1] Collateral Freedom: A Snapshot of Chinese Users Circumventing Censorship: https://www.opentechfund.org/article/collateral-freedom-snapshot-chinese-users-circumventing-censorship; How to Evaluate Technical Audits as a Funder: https://www.opentechfund.org/article/report-how-evaluate-technical-audits-funder; Access and Openness: Myanmar 2012: https://www.opentechfund.org/article/access-and-openness-myanmar-2012; Tools for Communication Security: https://www.opentechfund.org/article/tools-communication-security

Programmatic Overview

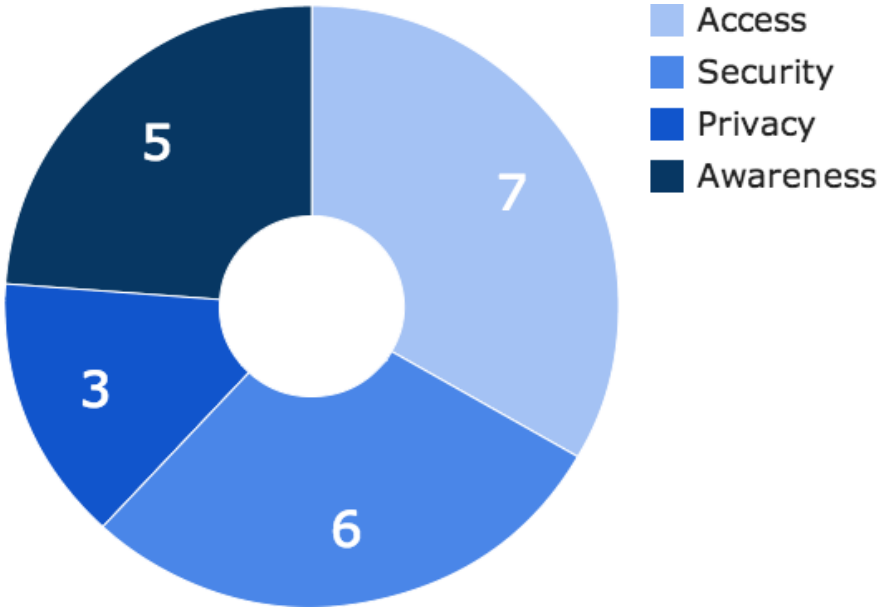
OTF's Total Operating Budget - $4,300,000[2]

Nearly 90% of OTF's operating budget - approximately $3.8 million – was expended in direct support of programmatic Internet freedom work in Fiscal Year 2013.

OTF supports projects and initiatives focused on increasing:

- **Access** to the Internet, including tools to circumvent website blocks, connection blackouts, and widespread censorship;
- **Awareness** of privacy and security threats and protective measures, including how-to guides and trainings for circumvention tools;
- **Privacy** enhancement, 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.

Figure 1: Number of Projects and Initiatives by Focus

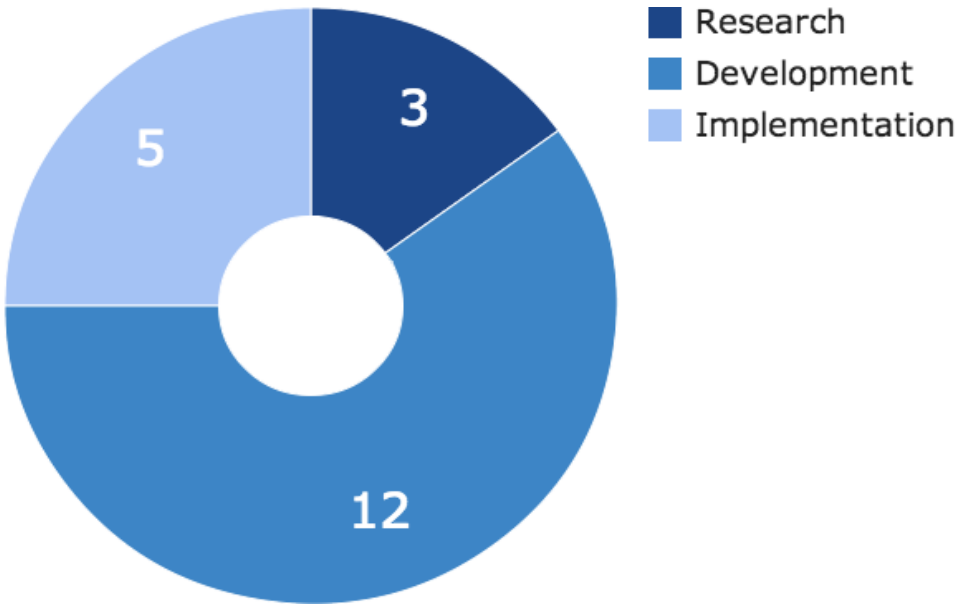


[2] The Budget Control Act of 2011 included provisions that would result in an 8.2 percent reduction in non-defense discretionary spending. These provisions were subsequently amended in The American Taxpayer Relief Act of 2012, resulting in more limited reductions for Fiscal Year 2013. As a result of these developments, OTF's original budget of $4.3 million was reduced by $150,000 to $4.15 million.

OTF supports projects and initiatives with primary activities to:

- Advance **research into repressive Internet interference** on modern communication networks and the methodologies and technologies used to censor and to circumvent online censorship;
- Foster **development of technologies** that circumvent internet censorship, enable access with increased privacy and security from invasive online monitoring, interference and surveillance by repressive regimes; and
- Enable widespread and timely **implementation of solutions** to free people from repressive Internet interference.

Figure 2: Number of Projects and Initiatives by Activity



Projects and Initiatives - By Focus

Access

Sub-total investment - $1,653,495[3]

Cupcake Bridge - $66,966

Allow any person with a Chrome or Firefox web browser to expand the Tor anti-censorship network (Development)

Tor bridges are Tor relays that are not listed in the main Tor directory. They are a step forward in the blocking resistance race. Cupcake Bridge is a Chrome browser extension that allows users to create new Tor bridges automatically, without having to install a full software suite or configure anything. ***With OTF support, more than 2,000 volunteers are already expanding the Tor network by just***

[3] For purposes of this report, OTF has slotted projects by their primary focus however many projects address multiple focus areas.

opening their browser, increasing performance and scalability of the TOR network. This year's support will expand the project to create a Cupcake Bridge extension for Firefox and plugins to work on sites like Wordpress and Drupal, significantly growing the number of global Tor bridges.

Engineering Initiative - $273,058
Global secure cloud infrastructure and tool security audits for deploy-ready projects (Development, Direct Initiative)

This initiative maintains valuable technology assets ready to be shared at any time with any individual or group who shares OTF's mission, core values, and objectives. It is a stocked garage for Internet freedom technologists, an 'engineering ideas and innovation' lab, housing crucial tools and resources with priority to help new and small efforts spin or scale up quickly. More than 10 Internet freedom projects not directly supported by OTF utilize the garage alongside 3 projects directly supported by OTF. This initiative maintains the following assets:

- Secure global cloud infrastructure. Sites include: Turkey, Cambodia, Hong Kong, South Korea, and Washington, DC;
- Collaborative independent teams that challenges a project to improve its overall technological effectiveness;
- Independent auditors that perform security and privacy audits on a projects technology; and,
- Architecture review and analysis of the project's chosen systems, conventions, and common practices.

Localization Initiative - $260,000
Localization platform to grow and manage translation resources between global Internet freedom tools (Implementation, Direct Initiative)

Transifex is an online translation platform that provides an easy means for any multi-lingual individual to contribute translations to any project using the service. This effort creates an umbrella account for Internet freedom projects within the Transifex infrastructure. ***As of this report, 1,400 translators are working with 30 projects to translate 1.7 million words into 180 languages and dialects including Arabic, Farsi, Korean, Tibetan, Mandarin, Spanish, Ukrainian, and Vietnamese.*** The platform offers translators and relevant tools a central location for their collaborative work. This project allows for rapid translations of Internet freedom tools to occur without incurring any expense to the project or OTF. The Open Internet Tools Project manages, expands and improves the OTF initiative to ensure it addresses the needs of the Internet freedom community.

Rapid Responders Initiative - $192,771
Support resources for global Internet freedom emergencies (Implementation, Direct Initiative)

OTF's Rapid Responder Initiative is an additional mechanism to provide quick support and resources to mitigate highly time-sensitive and emerging threats to Internet freedom. This initiative is designed to provide emergency support for efforts including, but not limited to:

- Establishing new Internet connections when existing connections have been cut off or are being restricted;
- Providing personal digital protection for online journalists and digital activists;

- Rapid development of tools or translations needed to respond adequately to emergencies;
- Developing decentralized, mobile Internet applications that can link computers as an independent network (mesh or delay-tolerant networks);
- Supporting digital activists with online services such as secure hosting and DDoS mitigation and providing capacity building as needed;
- Maintaining secure cloud infrastructure for Internet freedom projects; and
- Supporting emergency security and privacy audits.

StoryMaker - $98,200
Citizen journalist app for Android smartphone users (Development)

StoryMaker is a tool to help citizen journalists produce richer multimedia content. Currently, StoryMaker can publish video content securely via a custom YouTube uploader. This year's support will add at least four new distribution channels to facilitate more secure publishing of StoryMaker content. Specifically, support will be added for secure photo publishing to flickr, secure audio publishing to SoundCloud, private publishing of any media to a private server via SSH, and secure photo and video sharing to Facebook. During the development and testing phase of this tool, train-the-trainer sessions took place on the African continent. StoryMaker is being implemented in Egypt, Tunis, Iraq, and Morocco.

With OTF support, Storymaker has been downloaded and used by more than 10,000 citizen journalists

Testbed and Hyper-local Incubator - $600,000
Incubator for hyper-local circumvention tools in China and testbed for secure mobile apps (Implementation)

DETER is a testbed housed at the University of California-Berkeley that allows for real-world testing in a variety of configurable network environments. This project allows the testbed to be used for mobile-device based Internet freedom tools creating a robust resource to battle-test mobile applications for Android and iOS. The hyper-local incubation project, also at Berkeley, focuses on creating a variety of mechanisms for Chinese users to identify censorship and innovate new means of circumvention. This project fosters indigenous communities of users and developers and ensures that anti-censorship techniques are utilizing the latest means of evading censorship under a constantly evolving set of techniques. The project evaluates specific censorship events and distinguishes between different types of mechanisms utilized in real-time.

Usability Study - $162,410
A study on common usability challenges facing Internet freedom tools (Research)

This work aids in the creation and development of more effective Internet freedom tools through the application of a research framework grounded in ethnography, human-centered design, and the practice of research-based product definition. The usability framework defines motivations, needs, and usability challenges facing user communities of target tools and provide development and design milestones that are necessary to address these challenges. This work also provides selective recommendations to developers of specific tools in the form of proposed development milestones to address the findings of a pilot study.

Awareness
Sub-total investment - $461,213

Measurement Lab Browser Extension - $126,800
Develop an M-Lab browser extension to dramatically increase the real-time understanding of disruptions to Internet users (Development)

This project supports the development of new software for users to run censorship and other network interference tests on the M-Lab platform. Once deployed, this tool will enable any user to become a regular and reliable part of the M-Lab community with global access to hundreds of servers against which to run experiments. It will also give researchers and policy-makers a tool for real-time monitoring of censorship activity with a capability to zoom in on particular user communities on particular networks in particular geographic locales.

No Firewall Project - $109,115
Increasing digital security awareness and practice for South-East Asia Internet users, bloggers, and citizen journalists (Implementation)

Vietnamese netizens are among the most tech-savvy and possibly have the highest user rate of Internet freedom technology. This project provides real-time assistance to high-risk individuals by supporting the establishment of a resource center for circumvention & digital security for the average Vietnamese netizen. Also supported is the No Firewall online platform to continue to localize new manuals and guides, and promote existing Internet anti-circumvention tools. The project also establishes a help desk for bloggers, digital activists, citizen journalists and human rights defenders in need of support.

Ooni-probe - $59,134
Improving the release and deployment quality of Ooni-probe on the M-Lab infrastructure (Development)

Ooni-probe, the Open Observatory of Networking Interference, is an open source network testing framework for detecting Internet censorship in all its forms. Ooni-probe also allows for real-time analysis of censorship activities. ***With OTF support, this tool has become the go-to platform for civil-society testing of censorship in Africa, the Middle East, and Asia.*** Ooni provides the censorship detection and monitoring eco-system with a stable infrastructure as well as design and engineering improvements to facilitate broader adoption.

Security-in-a-box - $106,164
Supporting the technical upgrade of the Security-in-a-box website and publishing workflow in order to maintain the website in multiple languages and facilitate new language translations (Implementation)

Security-in-a-box drives a new paradigm of self-enabled agency in the digital realm, teaching human rights defenders how to become more efficient by adopting habits and approaches that help them to continue doing their work unimpeded and to circumvent harassment and censorship. However, before OTF's support, the Tactical Technology Collective (TTC) infrastructure was not suited to easily and dynamically support maintaining existing languages or adding new languages of the online toolkit. As the number of countries who censor the internet increases, user demand for TTC assistance has far

outstripped its capacity. This project allows TTC to update its technical infrastructure and to establish a reliable workflow to streamline the Internet freedom translation process.

Special Reports - $60,000
Reports examining key Internet freedom challenges and opportunities (Research, Direct Initiative)

Access and Openness: Myanmar 2012 and Vietnam 2013
An OTF-sponsored technology team visited Myanmar in 2012 and Vietnam in 2013. A vast amount of information was collected from a variety of sources, offering insight into each country's telecommunications landscape.

This research exposed the present critical juncture in each country: will either country continue historical trends of isolation and oppression or grasp new opportunities for technological advancement and the incubation and growth of a free expression culture?

These reports provide important, often otherwise inaccessible, information to citizens and the international human rights, democracy and Internet freedom community concerned with the country's future, along with some benchmarks against which analysis can be done. The reports are also designed to be built upon by other members of the global Internet freedom effort. While it is expected that the most interested audience is technical, the report aims to provide relevant baseline information for policy makers, civil society, and international investors.[4]

Topics investigated in each report include:

- The percentage of population with landline and wireless Internet subscriptions;
- In-country Internet penetration and mobile subscription;
- The cost of acquiring and activating an average smartphone;
- Most popular smartphone hardware and software;
- A review of network capacity and political situation of in-country telecommunication providers;
- Current privacy and security protections of voice calls and text messages; and
- Determination of in-country online censorship.

How to Evaluate Technical Audits as a Funder
OTF supports technologies that promote human rights and Internet freedom globally. To keep the quality of its investments high, OTF facilitates independent technology audits. To derive the greatest possible community-wide value from these audits, OTF sought to document its internal process by which to evaluate technical security audit reports from the perspective of a funder, not a technologist. This document provides an instructive framework for how an organization, such as a human rights funder or an NGO, can effectively and efficiently engage information security auditor and their findings, based on OTF's experience and identifiable code vulnerabilities.[5]

[4] Access and Openness: Myanmar 2012: https://www.opentechfund.org/article/access-and-openness-myanmar-2012 Access and Openness: Vietnam 2013: Expected release summer 2014
[5] How to Evaluate Technical Audits as a Funder: https://www.opentechfund.org/article/report-how-evaluate-technical-audits-funder

Privacy
Sub-total investment - $839,997

CryptoCat - $109,997
Global secure chat in the web browser (Development)

Cryptocat is an instant messaging application that offers encrypted chat within any browser. Its goal is simple: have an instant messaging platform that anyone can access and use, regardless of technical expertise. ***With OTF's support, the number of CryptoCat weekly users has grown from less than 1,000 to 105,000.*** Moreover, year two support for the CryptoCat project will improve the state of current standards used for multi-party encrypted instant messaging. The primary focus is to build upon the current robust standard Instant Message encryption specification which supports only two users (Off-the-Record) so that it develops to be a specification supporting multiple users (Multi-Party Off-the-Record). A new specification of this capability will likely be applied across the OTR spectrum of uses. Further, CryptoCat will connect to other social networks (such as Google Talk) in order to allow encrypted conversations with friends and contacts on using other social networks.

Sock puppet Detection - $130,000
Social network sock puppet detection & discovery (Research)

Armies of online drones, compromised social network accounts, and surrogate users known as "Internet sock puppets" are used to drown out the online independent voices of the voiceless. Sock puppets are increasingly used by repressive regimes to deflect or redirect conversations that are important to the maintenance of their control. The prevalence of the sock puppet false narratives threatens the benefits offered by a free Internet by abusing that same freedom. This makes for an insidious situation, because one of the fixes against sock puppet attacks would be to reduce Internet anonymity; the cure might be much worse than the problem itself. Sock puppet detection and discovery will map out these rhetorical attacks, provide for in-depth identification of commonly used techniques, and build a set of tools to be used by organizations and the public to help defend against them.

Tor Browser Bundle - $600,000
Sustaining an open network defending against network surveillance and censorship threatening personal freedom (Development)

This effort focuses on expanding security and usability of the Tor Browser Bundle (TBB). ***Tor Browser is used by millions worldwide daily and has been downloaded over 36 million times in the past 12 months with OTF support***. The project identifies and remediates current privacy and security issues in Firefox that impact TBB users; improves the usability and functionality of the Firefox extensions that are included with TBB; and finishes and extends the "reproducible build" design that allows users to gain confidence that TBB includes exactly and only the components intended to be included.

Security
Sub-total investment - $845,320

GSMMap - $200,000
Increasing mobile phone GSM security awareness and deploying mobile monitors (Research)

Research has identified attacks against mobile network users and Internet freedom technology now allows consumers to verify the safety of the mobile network being used. ***With OTF support, the number of monthly users has grown from 100 to more than 5,000***. The mobile security monitoring tool continues to be adopted by high-risk users who want to detect mobile attacks on their privacy and by security and by advocates who use the tools to contribute data to GSMMap. This tool is currently the primary evidence collection mechanism utilized by those advocating against insufficient protection of mobile networks. With OTF's ongoing support, the project will create and enhance measurement tools for additional modern GSM networks, further automate the measurement process, implement autonomous measurement hardware, and more widely communicate the necessary evolution path towards better protected networks.

Mailvelope - $140,320
Global secure email in the web browser (Development)

Although secure email is now usable for many, the majority of non-technical email users do not go through the steps to enable PGP encryption on their email clients. Mailvelope significantly increases usability and accessibility while facilitating email encryption for users of browser-based email providers. ***With OTF's support, the number of weekly users has increased from 8,000 to 42,000.*** It comes as a browser extension and allows a user to enhance existing web-mailers like Gmail™ or Yahoo™ with functionality to encrypt and decrypt mail. Mailvelope is based on the OpenPGP standard, offers key management, and is therefore compatible with existing PGP implementations.

RedPhone, SecureSync, & TextSecure - $455,000

Interoperable encrypted text messaging between Android and Apple iOS smartphone users (Development)
TextSecure is an easy-to-use encrypted text messaging application for Android. It enables secure local storage of SMS/MMS messages, as well as encrypted transmission of SMS/MMS messages to other TextSecure users and groups of users. This project introduces additional features such as group chat and increased security. It will also create an iOS app fully interoperable with the Android app. ***With OTF's support, this tool is in active use by more than 10 million users.***

Interoperable encrypted voice conversations between Android and Apple iOS smartphone users
RedPhone is an easy-to-use encrypted VoIP application for Android, which enables secure high-quality phone calls to be made anywhere in the world. ***With OTF's support, this project has enabled more than 100,000 people to conduct safe voice conversations via smartphone.*** With this year's support, the project will develop a feature-parity RedPhone client for iOS, which will provide full secure call interoperability between the supported RedPhone platforms.

Develop an app to securely backup an Android device by locally encrypting all data before sending it to the sync provider

All current Android sync providers are unencrypted, meaning that the sync service gets a plaintext copy of everything synched, leaving contact and calendar information potentially vulnerable to hostile parties. While the stock Android sync experience has no built-in confidentiality - leaking contents of contact and calendar details - Android fortunately has a mechanism for others to seamlessly provide different sync functionality. Secure sync will take advantage of this mechanism to offer Android users encrypted backup.

OTF supported the growth of censorship resistant secure online chat and TXT from 200,000 regular users to over 10 million globally

VPN and Encrypted Email - $50,000

Building VPN and encrypted email services to allow for implementation by a wide range of service providers (Development)

LEAP is a non-profit entity dedicated to giving all Internet users access to secure communication. Its focus is on adapting encryption technology to make it easy to use and widely available. For this project, LEAP is focused on the full launch of VPN and encrypted email services allowing for implementation by a wide range of service providers and building sustainability for future iterations.

Fiscal Year 2013 Expenditures

Figure 3: Expenditure of Funds by Focus

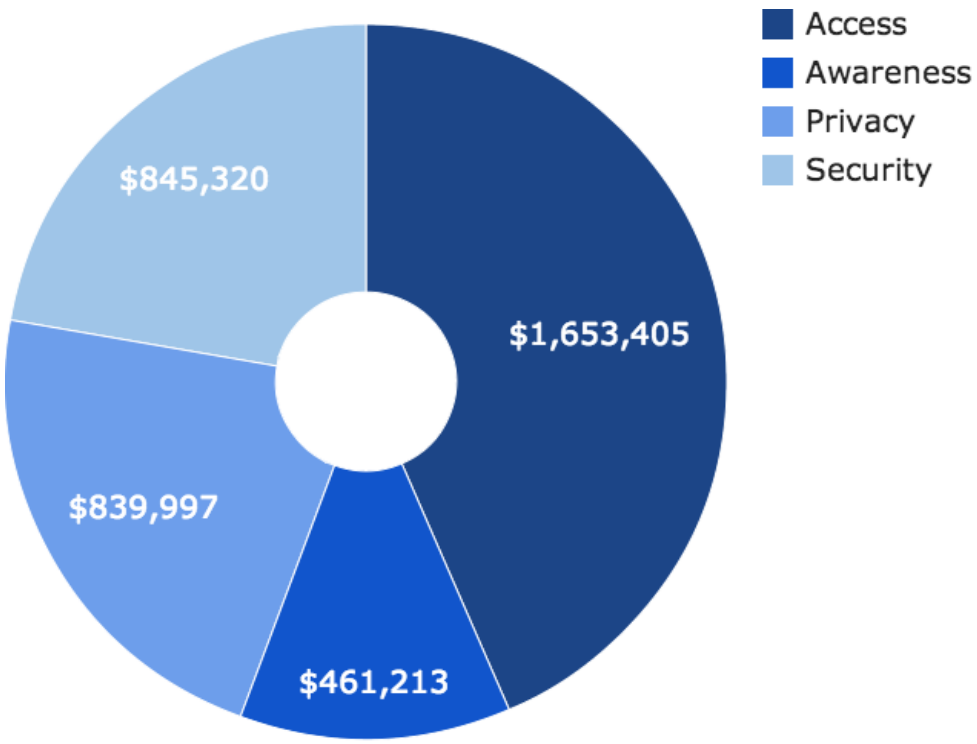


Figure 4: Expenditure of Funds by Activity

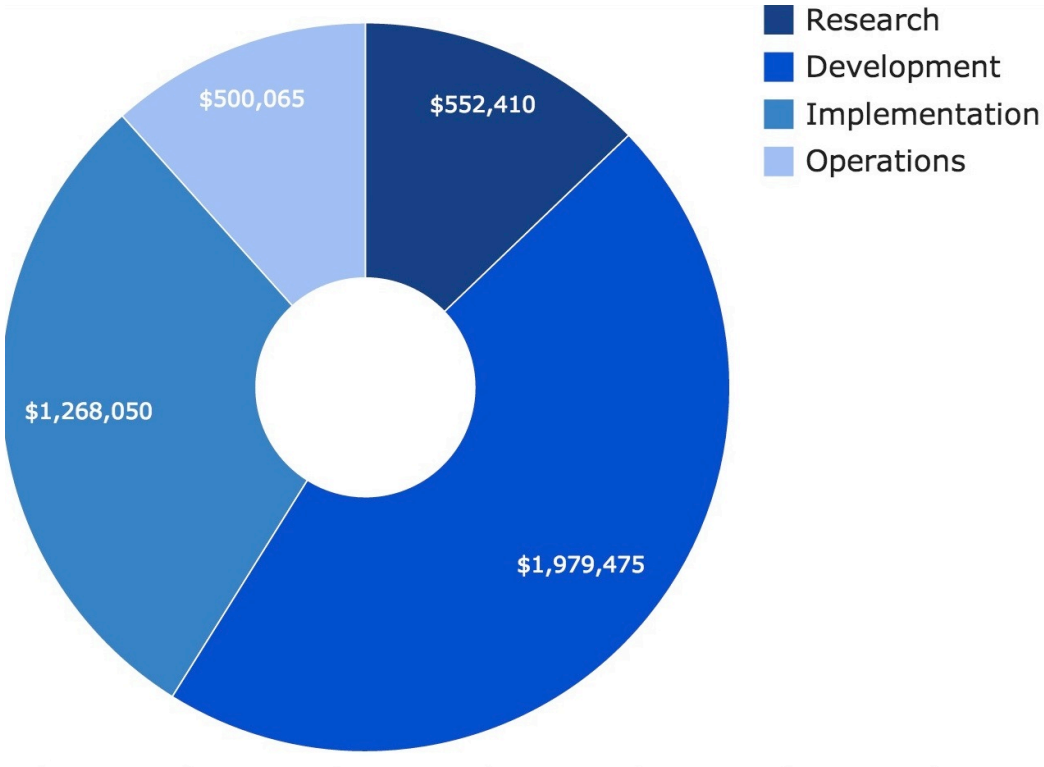


Figure 5: FY 2013 Expenditures

Entity	Project	Project Description	Amount
Access Focused			
Griffin Boyce	Cupcake Bridge	Allow any person with a Chrome or Firefox web browser to expand the Tor anti-censorship network	$66,966
OTF	Engineering Initiative	Global secure cloud infrastructure and tool security audits for deploy-ready projects	$273,058
OTF	Localization Initiative	Localization platform to grow and manage translation resources between global Internet freedom tools	$260,000
OTF	Rapid Responders Initiative	Support resources for global Rapid Responders	$192,771
Guardian Project	StoryMaker	Citizen journalist app for Android smartphone users	$98,200
Freedom2Connect Foundation / University of California Berkeley	Testbed and Incubator	Incubator for hyper-local circumvention tools in China and testbed for secure mobile apps	$600,000
SecondMuse	Usability Study	A study on common usability challenges facing Internet freedom tools	$162,410
		Access Sub-total	***$1,653,405***
Awareness Focused			
New America Foundation	Measurement Lab Browser Extension	Develop an M-Lab browser extension to dramatically increase the real-time understanding of disruptions and censorship events witnessed by Internet users	$126,800
Vietnam Action Network	No Firewall Project	Increasing digital security awareness and practice for SE Asia Internet users, bloggers, and citizen journalists	$109,115
Least Authority	Ooni-probe	Improving the release and deployment quality of Ooni-probe on the M-Lab infrastructure	$59,134
Tactical Tech Collective	Security-in-a-box	Supporting the technical upgrade of the Security-in-a-box website and publishing	$106,164

		workflow in order to maintain the website in multiple languages and facilitate new language translations	
OTF	Reports Initiative	Telecommunications landscape assessments for Burma and Vietnam, How to Evaluate Technical Audits as a Funder	$60,000
		Awareness Sub-total	***$461,213***
Privacy Focused			
eQualit.ie	CryptoCat	Global secure chat in the web browser	$109,997
Thinkst	Sock Puppet Detection	Social network sock puppet detection & discovery	$130,000
Tor Project	Tor Browser Bundle	Sustaining an open network defending against network surveillance and censorship threatening personal freedom	$600,000
		Privacy Sub-total	***$839,997***
Security Focused			
SRLabs	GSMMap	Increasing mobile phone GSM security awareness and deploying mobile monitors	$200,000
Thomas Oberndörfer	Mailvelope	Global secure e-mail in the web browser	$140,320
Open Whisper Systems	RedPhone, SecureSync, & TextSecure	Interoperable encrypted voice conversations between Android and Apple iOS smartphone users; Develop an app to securely backup an Android device by locally encrypting all data before sending it to the sync provider; and Interoperable encrypted text messaging between Android and Apple iOS smartphone users.	$455,000
LEAP Encrypted Access Project	VPN and Encrypted Email	Building VPN and encrypted email services to allow for implementation by a wide range of service providers	$50,000
		Security Sub-total	***$845,320***
OTF	Program Operations	Internal expenses required to run the OTF program	$500,065
		Total	***$4,300,000***

Fiscal Year 2013 Program Funding

Fiscal Year 2013 presented the OTF program with delays through the third quarter resulting from initial funding uncertainty tied to Congressional delays in passing a year-long federal budget. Pending the year-long budget, the mark-up legislation from both chambers of Congress contained positive references specific to the coordinated USG Internet freedom efforts.

The House Appropriations Committee's mark-up contained a continuation of "the directive to expand unrestricted access to information on the Internet through the development and use of circumvention technologies" and "commends BBG for its work in this area and requests that the operating plan … include amounts planned for Internet freedom activities in Fiscal Year 2013."[6]

The Senate Appropriations Committee's markup recommended $12.6 million for BBG Internet freedom efforts, while encouraging "continued coordination and cooperation between the Department of State, USAID and BBG" and "digital security and digital safety training".[7]

> "…the directive to expand unrestricted access to information on the Internet through the development and use of circumvention technologies…"

Congress first passed a Continuing Appropriations Act for FY 2013 funding of the government through March 27, 2013.[8] The subsequent appropriations bill for the remainder of the fiscal year became law on March 26, 2013.[9] Both Acts of Congress funded the BBG's Internet freedom effort at Fiscal Year 2012 levels - $9.1m.[10]

Full fiscal year funds were provided to the BBG more than six months into the fiscal year. Discussions determining how the BBG Internet freedom funds would be split between RFA's OTF program and the BBG's Internet Anti-Censorship (IAC) program resulted in further delays. BBG's Internet freedom funding was ultimately split at a BBG IAC meeting on March 14, 2013 between the two programs, with OTF receiving $4.3 million.[11]

Despite these funding delays, OTF funds were obligated in full by Sept. 30, 2013. The projects were promptly evaluated and processed once the funding became available, allowing for timely contract execution of approved proposals.[12] OTF's multi-disciplinary, nimble and responsive approach to evaluating proposals and contracting projects, sculpted in year one and honed further in year two, proved to be essential in these circumstances. OTF was able to both perform due diligence on project review and quickly contract support of a diverse group of meaningful fully-vetted projects working towards the advancement of global Internet freedom.

---

[6] House Report 112-494, May 25, 2012, available at http://beta.congress.gov/congressional-report/112th-congress/house-report/494/1.

[7] Senate Report 112-172, May 24, 2012, available at http://beta.congress.gov/congressional-report/112th-congress/senate-report/172/1.

[8] Public Law No. 112-175, Sept. 28, 2012, available at http://www.gpo.gov/fdsys/pkg/PLAW-112publ175/pdf/PLAW-112publ175.pdf.

[9] Public Law No. 113-6, March 26, 2013, available at http://beta.congress.gov/113/plaws/publ6/PLAW-113publ6.pdf.

[10] This is a combination of $7.5 million designated by Congress and an additional $1.6 million from the BBG's base budget. The latter has been directed towards Internet freedom for a number of years. *See e.g.* Jeff Shell, Chairman of the Broadcasting Board of Governors, "Nurturing Internet freedom in China," *Washington Post*, Dec. 9, 2013.

[11] The Budget Control Act of 2011 included provisions that would result in an 8.2 percent reduction in non-defense discretionary spending. These provisions were subsequently amended in The American Taxpayer Relief Act of 2012, resulting in more limited reductions for Fiscal Year 2013. As a result of these developments, OTF's original budget of $4.3 million was reduced by $150,000 to $4.15 million.

[12] OTF review process: https://www.opentechfund.org/submit/guide#process

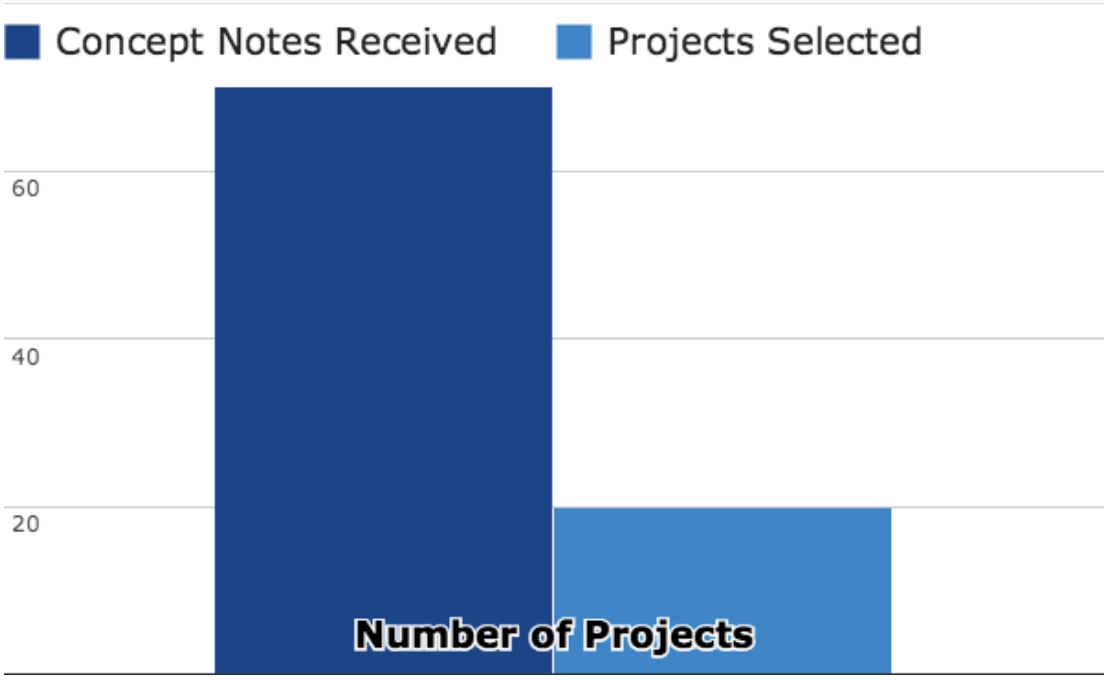
Trends in 2013

Increased need

The number of good concept notes submitted to OTF and total amount requested demonstrate a distinct asymmetry between available Internet freedom funds and the demand for funding - there are more good ideas than available support. In 2013, OTF received 68 concept note submissions requesting over $17 million from projects and organizations around the world. This is a steep increase from the 12 concept notes OTF received in FY 2012. In FY 2014, OTF has already received over 150 concept notes. This indicates a clear trend in both OTF's visibility and in the increasing interest and need for Internet freedom support.

Of the submissions received in FY 2013, OTF allocated funding to 20 projects limited only by our annual funding level. OTF was unable to fund many worthy and important projects that would have immediate positive impact on addressing current and emerging global Internet freedom needs. This trend of increased need for support is corroborated by other members of the Internet freedom community including other funders, past and presently supported projects, broader civil society and human rights technology actors, and people on-the-ground who need the tools and knowledge OTF supports to access information safely.

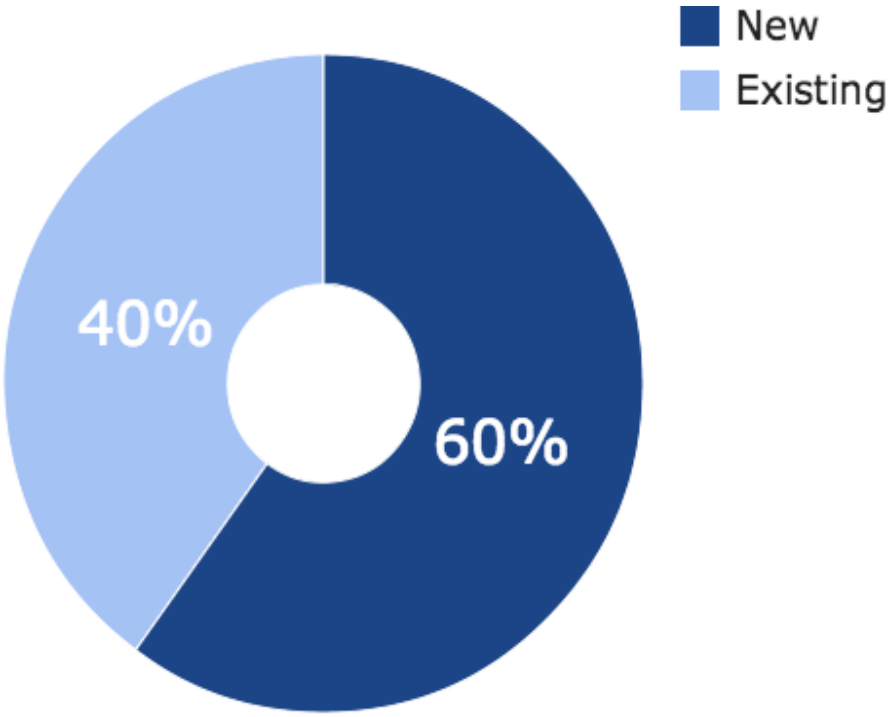
Figure 6: Submissions Received and Funded



New and diverse actors

OTF prioritizes expanding, strengthening, and diversifying the Internet freedom community through its funding. OTF is unique in that unlike other USG Internet freedom funders who have minimum proposal amounts of $500,000, organizational restrictions, or an inability to support individuals,[13] OTF can support any Internet freedom project that is approved through its rigorous proposal review and evaluation process, regardless of size, location or organizational type. As such, 60 percent of projects funded in FY 2013 had not previously received support from OTF. Based upon the breadth and ingenuity of the concept notes OTF received, a new pool technology and development talent is engaged in the pursuit of global Internet freedom.

Figure 7: New Projects in Fiscal Year 2013

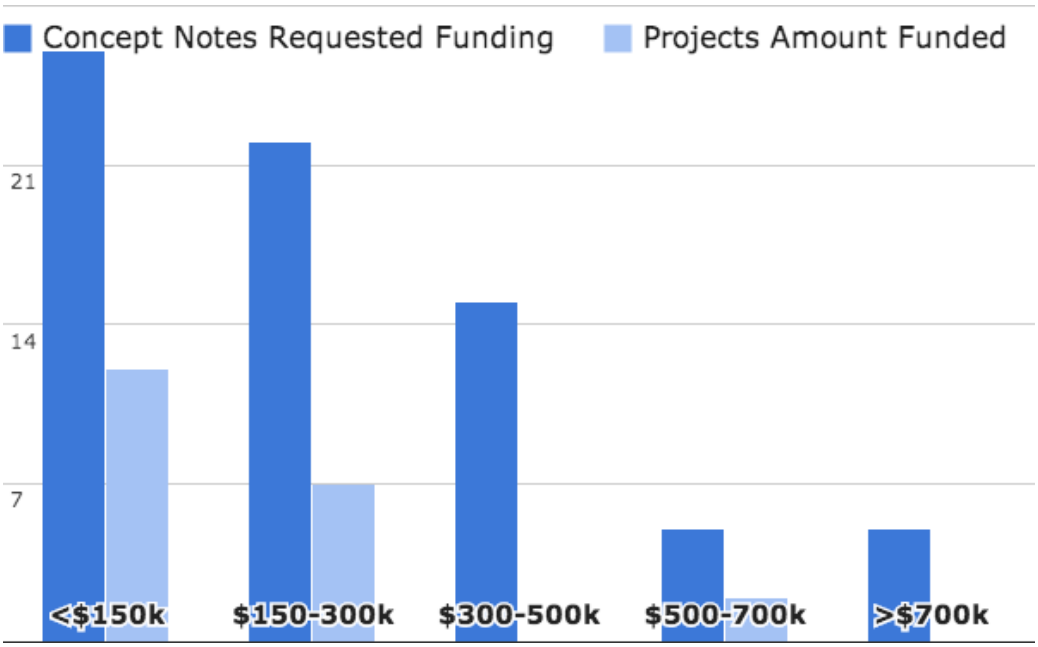


[13] DRL Internet Freedom Annual Program Statement for Internet Freedom Technology: http://www.state.gov/j/drl/p/207061.htm

Small projects

Two-thirds of the concept notes OTF received requested less than $300,000. This highlights a clear demand for small project funding and validates the need for OTF's approach to support low-cost yet high-return emerging technology projects. The large number of concept note submissions requesting less than $150,000 directly reflects OTF's portfolio priority, and as such, the majority of OTF projects (12 out of 20) are under $150,000 with an average project size of $250,000.

Figure 8: Concept Note Requests and Projects by Amount



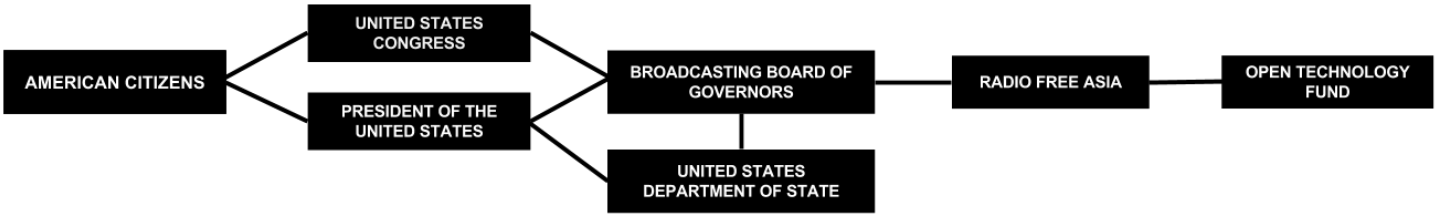
Focus on usability

OTF has seen a rising trend in the number of development concept notes it receives that address and incorporate end-user implementation as a proposal activity. 62 percent of concept notes received by OTF in FY 2013 were focused on the development of tools for non-technical end-users by simplifying existing tools or creating new tools. There has historically been a significant divide between developers creating security and privacy tools and their day-to-day usability for the target user. OTF views this as a sign of increased consideration of actual needs and collaboration with on-the-ground groups.

Organizational Overview

The Open Technology Fund was created in 2012 as a program within Radio Free Asia (RFA). RFA was founded by an act of Congress in 1994 as a private, non-federal, registered U.S. 501(c)(3) non-profit organization 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.[14] 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."[15] The BBG established OTF within RFA to support Internet freedom globally.

Figure 9: OTF Organizational Hierarchy



OTF reports to RFA's President, who in turn reports to the BBG's Board of Governors. The BBG Board, which is a bi-partisan board with nine members, eight of whom are appointed by the President of the United States and confirmed by the U.S. Senate including one designee as the Chairman of the BBG.[16] 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.[17]

The OTF Team

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 the BBG, the International Broadcasting Bureau, other associated entities, and outside stakeholders.

Bernadette Mooney Burns
General Counsel and 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.

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

Richard Smith
Treasurer/Budget Director, RFA
Mr. Smith is responsible for advising RFA and OTF on matters related to contracting and operating budgets including the development of annual and multi-year 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 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 Senior Program Analyst, RFA
Mr. Lynn joined RFA in April 2012 as a program manager. As senior program analyst, he continues to be actively engaged in OTF's day-to-day operations and long-term planning.

Liz Pruszko Steininger
OTF Senior Program Manager, RFA
Ms. 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.

OTF's Advisory Council

In FY 2013, OTF added 12 new members to the Advisory Council bringing the total number of members to 18. The Advisory Council helps OTF to gain a deeper understanding of the 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 deepen 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*
Kelly DeYoe, *Team Leader, Internet Anti-Censorship Program, Broadcasting Board of Governors*
Cory Doctorow, *Author, Journalist, and Activist*
Peter Eckersley, *Technology Projects Director, Electronic Frontier Foundation*
Gunnar Hellekson, *Chief Strategist, Red Hat*
Anthony D. Joseph, *University of California at Berkeley*
Zane Lackey, *Director of Security Engineering, Etsy*
Katherine Maher, *Director of Strategy and Engagement, Access*
Moxie Marlinspike, *Institute For Disruptive Studies*
Andrew McLaughlin, *betaworks / Berkman Center for Internet & Society*
Haroon Meer, *Founder, Thinkst*
Dr. M. Chris Riley, *Senior Policy Engineer, Mozilla*
Bruce Schneier, *Security Technologist and Author*

Ian Schuler, *CEO, Development Seed*
Jillian C. York, *Director for International Freedom of Expression, Electronic Frontier Foundation*

Funding Model

Lowering the Barrier to Entry

In FY 2013 OTF continued its role as the early investor and incubator of emerging global Internet freedom ideas. OTF prioritizes seed and project-based funding as its primary method to grow and sustain new ideas with clear contract goals, milestones, and deliverables currently not offering general operating funds or unrestricted support.

While OTF collaborates with organizations that support traditional human rights approaches, OTF-supported projects must be substantively technology-focused in order to achieve defined, real-world results in the advancement of global Internet freedom. Projects are initially assessed by three criteria: the amount requested, the project's primary objectives, and its feasibility. These criteria are analyzed against known trends in censorship and circumvention technology and techniques both by the Advisory Council, and by the OTF to assess risk and determine appropriateness.

OTF has maintained its commitment to increase the scope and impact of emerging technologies by distributing program funds to more unfunded or underfunded projects then previous years. Despite a reduction in its operating budget from $6.7 million in FY 2012 to $4.3 million in FY 2013, OTF increased the number of projects and initiatives it supported annually from 13 to 20, for a total of 33 projects over two years. Sixty-five percent of projects supported by OTF in 2013 are new Internet freedom efforts. Over these two years, OTF reduced the average project size from over $500,000 to less than $250,000 and nearly doubled the number of projects. This emphasis on smaller and more diversified projects is one key differentiator between OTF and the flagship State Department Internet freedom program, which seeks projects able to spend a minimum of $500,000 annually.[18] These distinctions with cooperation have allowed both programs to compliment each other expanding the overall breadth of public support to Internet freedom.

> Of the 20 projects OTF funded in FY 2013, 65 percent had never sought prior funding

The results have been demonstrably positive. OTF-supported projects collectively brought secure and censorship-resilient communication to more than 12 million individuals worldwide. This reflects OTF's growing role as an incubator of early-stage, low-cost, and high-return Internet freedom projects which, were previously unable to apply for public support.

Portfolio Risk and Transparency

Other Internet freedom and human rights technology funders have begun to rely on OTF's ability to support multiple projects working toward overlapping objectives. This flexibility and OTF's cooperation amongst funders allows for a multi-track approach bringing together discreet efforts aimed at solving big privacy and security challenges. OTF's approach of supporting independent yet coordinated projects advances core technologies at a quicker pace, responding to the dynamic and changing nature of digital communication.

[18] DRL Internet Freedom Annual Program Statement for Internet Freedom Technology: http://www.state.gov/j/drl/p/207061.htm

Two key tenets of OTF's work are transparency and learning from what does not work. An unsuccessful project that has publicly shared its challenges can advance the community more than a successful project, despite not achieving its goals. By openly sharing its shortcomings, the project will reduce the likelihood that future developers repeat previous mistakes, thereby contributing significantly to advancing Internet freedom. OTF strives to model transparency in its own work and to ensure a minimum level of transparency for the projects it funds, publishing the project name, amount, duration, and objectives on the OTF website.

OTF recognizes that investing in cutting-edge, early-stage technology will result in projects that both succeed and fail. It mitigates investment risk by keeping project amounts low and paying upon successful completion of milestones. In cases where larger amounts have been requested, OTF has worked with the project to decrease the scope, make it more forward-thinking and higher in return. This has allowed OTF to further diversify its program risk and to give new individuals or organizations with good ideas the opportunity to try new research, development, and implementation directions. If an existing project encounters unforeseen hurdles, OTF works with the project to adapt agreements with contract amendments that allow for new approaches.

Proposal Evaluation Process

In FY 2013, OTF institutionalized its proposal evaluation process in a formal and public structure introducing additional selection and evaluation criteria, greater transparency to the public, with increased engagement and flexibility for applicants. As stewards of public funds, this process allows OTF to maintain a high degree of accountability while simultaneously lowering the barrier of entry for nascent groups with good ideas. Increasing the accessibility of its proposal system has allowed OTF to reach new communities previously unavailable to traditional funders. The result has been a fivefold increase in concept note submissions from technical developers and civil society organizations new to the field compared to 2012.

Open Technology Fund Program Philosophy

- Open source technology allows for continuous improvement and large scale engagement in technical development
- Transparency leads to accountability
- Maximize funds spent to directly support projects and resource initiatives
- Due Diligence means evaluation and reviews are done by subject matter experts from multiple disciplines
- Collaborative development avoids duplication of efforts
- Collaborative funding increases overall return and spreads risk
- Interaction and engagement make a better product
- Vulnerabilities should not be left to the censors to discover
- Minimize risk to users through code audits and risk disclosure

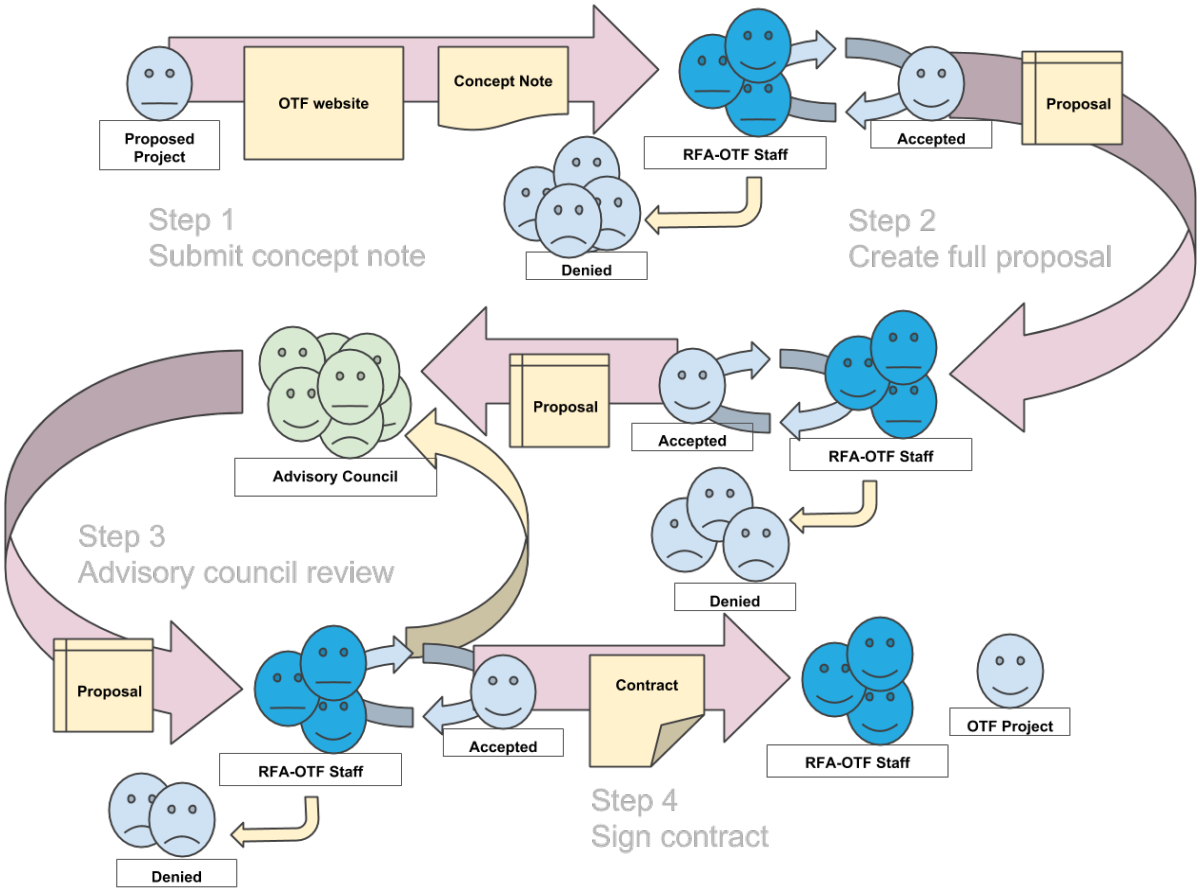
Process Overview

1) A concept note can be submitted at any time, from anyone through OTF's website;
   a. OTF performs a passive review process which includes evaluating concept notes against basic criteria;
   b. OTF performs an active review process which includes soliciting clarification on any questions regarding the criteria;
2) Preliminary proposals are requested from concept notes that successfully emerge from review;
   a. OTF evaluates full proposals against more stringent criteria;
   b. OTF provides feedback and guidance to improve the proposal quality and suitability of the proposed effort within OTF's remit;
3) Advisory Council reviews OTF's proposal recommendations;
   a. Proposals are reviewed and evaluated by the Advisory Council;
   b. Proposals with recommendations for funding from both the Advisory Council and OTF staff are reviewed by RFA's executive, legal, and financial departments before contracts are issued; and
4) Contracts are issued for final proposals determined to be a high priority, technically feasible, and legally and fiscally compliant.

OTF Proposal Review Process
1. Concept Note Received
2. Full Proposal Requested
3. Advisory Council Review
4. Contract

The diagram below illustrates OTF's process from concept note through review, assessment, and contracting:

Figure 10: OTF Evaluation Process Overview



Continuous Open Solicitation
OTF's concept note submission process consists of a short, open online form, which makes it easy for anyone to submit a proposal for a good idea at any time.[19] The few questions for applicants are tailored to solicit key information as quickly as possible, without creating unnecessary obstacles for applicants with little or no prior fundraising experience. This helps to lower the barrier to entry for applicants that may have innovative projects but limited administrative capacity.

When initially reviewing a concept note, OTF considers the following criteria:

1) Does the proposed idea contribute or have relevance to OTF's mission, core values, and objectives?
2) Does the proposed idea have technical merit?
3) Is the proposed idea sustainable and fiscally realistic?

If a concept note satisfies these initial criteria, the applicant is invited to submit a full proposal that further develops their project idea. The proposal form is also web-based, with a detailed guide walking the applicant through each step in the proposal process.

Proposal Selection and Evaluation
Once OTF has solicited and received a full proposal, OTF conducts an initial screening and determines whether to present the proposal to the Advisory Council for review. During this process, OTF will inform the applicant and, in many cases, provide feedback and suggestions for revising the proposal so that it meets OTF's standards. This assistance is invaluable for applicants who may not have experience in writing proposals, as is often the case with incipient or small organizations.

In evaluating a proposal, both OTF and its Advisory Council use the following criteria:

- Are the primary goals, objectives, and problems addressed within OTF's remit, cutting edge, and OTF priorities? e.g. blocking or filtering communications, surveillance or monitoring, intermediary liability, etc;
- Are the chosen methods and strategies appropriate for the problem they're looking to address? e.g. technology development/research/implementation, training, advocacy, testing;
- To what extent is the project technically feasible and the applicant qualified, if the proposal is primarily technology driven?
- What is the on-the-ground usability, privacy, and security standards of any technology proposed?
- What are the stated or otherwise known limitations and challenges of the proposals chosen solutions and their ability to undergo red teaming or alternative analysis?
- What is the project's current state and funding history? i.e. is it a new or a pre-existing effort?
- To what extent will the proposed effort likely sustain itself beyond the requested support?
- What potential exists for collaboration within the broader Internet freedom and human rights technology community?
- Do the costs of the proposed effort and the types of expenses outlined make the project fiscally realistic?
- Which geographic regions and/or countries that will benefit from the proposed effort?

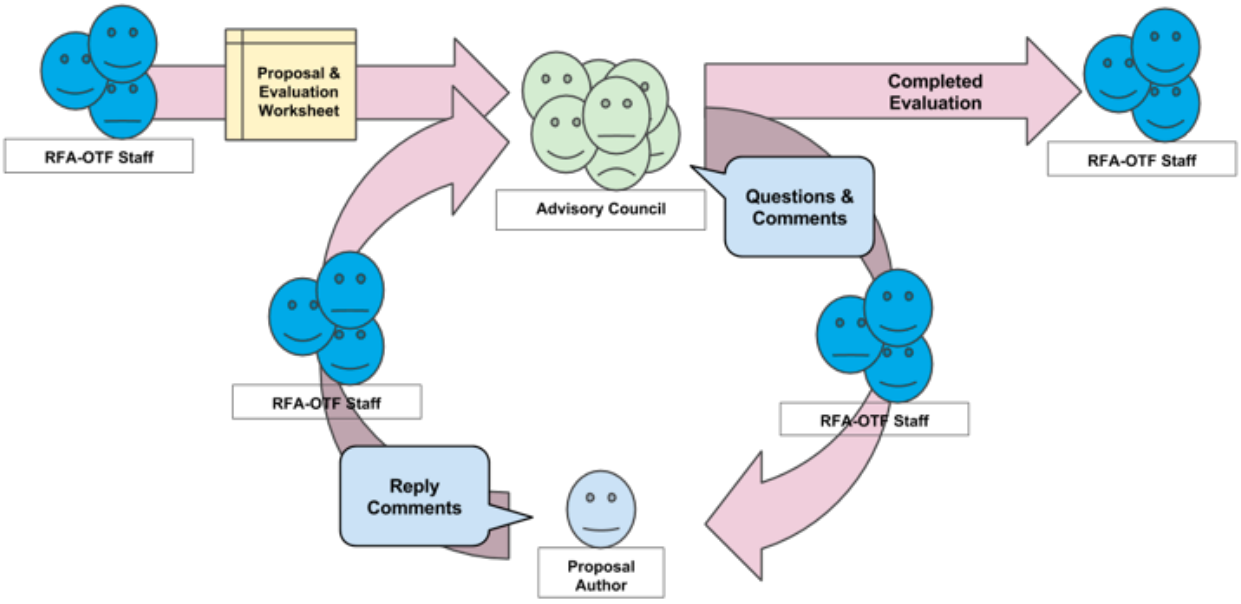
[19] Online submission page and Proposal Guide: https://www.opentechfund.org/submit and https://www.opentechfund.org/submit/guide

- Who are the target beneficiaries? e.g. youth, ethnic or religious minority, women, academia, general population, journalists, activists;
- Does the proposal clearly articulate a measurable set of evaluation criteria and milestone metrics against results?

Independent Peer Review
Proposals that pass internal review by OTF are presented to the program's Advisory Council. The Advisory Council review process greatly expands OTF's project oversight capacity, expertise, perspective, and accountability. Collectively, the Advisory Council supports OTF by providing independent verification of programmatic assessments, and identifies strategic parallels in complementary fields and draws from their knowledge of current efforts by the Internet freedom community to avoid unintentional uncoordinated duplicative of efforts.

Advisory Council Conflicts of Interest
Each member of the Advisory Council volunteers their service in their respective personal capacity, such that their contribution towards OTF is not associated with their professional affiliations. To ensure independent evaluations, protection of at-risk users and applicants' intellectual property rights, all Advisory Council members complete a Conflicts of Interests Disclosure Form and Confidentiality Agreement upon joining the Council and before reviewing any proposals. In addition, prior to reviewing individual proposals, Advisory Council members are required to reaffirm their understanding of confidentiality requirements and complete a conflicts disclosure statement specifying any potential conflicts of interests they might have related to that proposal. All conflicts disclosure statements are reviewed by RFA's legal counsel to determine if a disclosure necessitates recusal of a council member in the case of an active conflict or to verify that there is no potential conflict before Advisory Council evaluations are considered and final determinations are made by OTF.

Figure 11: OTF Advisory Council Overview



Final Proposal Determination and Contracting
If a proposal is recommended by OTF and the Advisory Council for funding, the proposal then undergoes a final RFA review. This review is performed by RFA's legal counsel and RFA's budget officer to assess the proposal is within applicable laws and regulations governing RFA, the proposal's financial risk, its compliance with RFA's grant agreement, and to construct an appropriate contractual relationship with the applicant. Once any potential issues are resolved and recommendations are approved by RFA's President, a contract is drafted reflecting the scope of work outlined in the proposal that complies with requisite contractual clauses for the use of public funds and bilaterally finalized.

If at any stage between concept note and contract OTF decides not to fund a proposal, it provides information on why funding has not been approved. While OTF's budget limits the number of projects it can support financially, OTF is committed to strengthening the field of Internet freedom to whatever extent possible, and sees this feedback loop as instrumental to this process. When OTF determines that a proposal is a priority effort valuable for global Internet freedom writ large, but finds that it falls outside of its remit or beyond its budgetary capacity, OTF will refer the individual or organization to other funding sources where appropriate. A list of alternative sources of funding is listed on the website.[20]

Project Oversight
Each OTF project is managed through contracts that include provisions for consistent and diligent oversight beyond the minimum safeguards and requirements for accountability with public funds. All projects are paid only upon an OTF determination that each contract deliverable has been satisfactorily completed.[21] Each project is required to provide monthly project reports providing detailed status updates on progress and impact, responding to OTF questions or concerns, and identifying any challenges encountered. If during the contract term unforeseen challenges to completing the deliverables arise, scope modifications are discussed and contracts can be amended to make sure the project continues to meet OTF's mission and goals, and ensure appropriate use of funds. This approach accommodates the unpredictability of supporting emerging technologies by allowing for "risk of failure" while protecting the integrity of the projects' performance and OTF's investment.

In addition, OTF retains the discretion to require an independent, third-party technology audit. This mandatory contract provision allows for a detailed, independent verification of the project's progress along with quality assurance on privacy or security claims made by the project. Not only do these external audits provide support for the strengthening and development of OTF projects, they have become a key component by which independent efforts such as the Open Integrity Index assess privacy and security properties of everyday communications tools.[22] Furthermore, OTF's emphasis on open source development allows a large community of peer reviewers to provide independent code audits and tool reviews. Accordingly, OTF actively solicits feedback from industry experts.

In 2013, OTF supported 30 technology audits of foremost Internet freedom projects, identifying in total 185 privacy and security vulnerabilities

[20] Alternate sources of funding: https://www.opentechfund.org/submit/alternative-sources-support
[21] Outside review is often available and incorporated in this determination.
[22] Open Integrity Index: https://openintegrity.org/

In an effort to actively promote open communication principles, uphold a policy of transparency, and increase project oversight, the OTF website provides the maximum level of information possible without jeopardizing the projects themselves. In doing so, OTF also encourages public scrutiny and makes every effort to respond to information requests.

Determining Portfolio Performance

Portfolio performance is one mechanism OTF utilizes each year to determine program success. In early 2013, OTF moved to integrate a portfolio performance assessment methodology developed by a then-ongoing RAND report. This report has since been finalized and become public.[23] By combining its own evaluation criteria with RAND's assessment system, OTF has created a framework that allows it to more easily relate to, collaborate with, and complement the work of other Internet freedom and human rights technology funders by situating the assessment of OTF project outcomes and impact in a comparable context. Outputs from this framework are also used within OTF's decision-making process and as a means to assess the performance of OTF projects both individually and as a portfolio, based on the cumulative performance value of individual projects.

Performance Value

For each Internet freedom project that OTF supports, a performance value is assigned for its overall contribution to the four major areas OTF identifies as impacting Internet freedom and freedom of expression:

1. **Access** to the Internet;
2. **Awareness** of privacy and security threats and protective measures;
3. **Privacy** enhancement, including the ability to be free from repressive observation and the option to be anonymous when accessing the Internet; and
4. **Security** from danger or threat when accessing the Internet.

OTF Proposals are evaluated on factors including: compatibility with OTF goals, principles and priorities; usability, security standards; problems addressed, method and strategies proposed; technical feasibility; technical qualifications; global use applicability

Risk Value

A project's direct and indirect risk to RFA, the BBG, and intended beneficiaries is used as a multiplier to a project's performance value. For each project, a risk value is assigned to three major areas:

1. **Capability:** The reliability of a project's planned approach and ability to implement;
2. **Acceptance**: Assessing a project's credibility with users and quality of the deployment plan for the product; and
3. **Sustainability**: Considering the project's planning for future activities and funding beyond OTF support.

For each of these three major areas of risk, OTF considers 5 general types of risk:

1. **Management/Performance:** Ability to effectively and efficiently deliver the stated objectives;
2. **Political:** Potential diplomatic, congressional, or media effects;
3. **Technical:** Potential to reach its stated capability thresholds;
4. **Abuse:** Potential for third-parties to use the project, or its products, for illicit or undesirable purposes; and

[23] Portfolio Assessment of Department of State Internet Freedom Program: http://www.rand.org/pubs/working_papers/WR1035.html

5. **User safety:** Exposure of a project's target users to regime retribution for their use of a project's products or services.

Cost Value
Cost is the final area to be assessed. To attain a cost value, OTF combines the project's level of funding with the potential associated indirect costs arising from OTF managing the project and its risk.

An initial assessment of potential performance, risk, and cost values is derived from proposal and evaluation forms completed by OTF and the Advisory Council.[24] Based on OTF and Advisory Council responses, each major aspect of project performance and risk is assigned a one to five value which are totaled for a final performance and risk score. After accounting for cost, a project's baseline performance score is determined.

Once a contract is fulfilled, OTF repeats this performance evaluation process. From this, the project is reassessed and a final performance score is determined. In addition, each project that completes an OTF contract is asked to participate in an exit survey to provide further insight for final evaluation and to identify areas for improvement within the OTF program framework.

Figure 12: OTF Performance Assessment

$$\text{Performance} = \frac{((\text{Access}) + (\text{Awareness}) + (\text{Privacy}) + (\text{Security})) \times (\text{Risk})}{(\text{Cost})}$$

Within the context of this methodology, OTF has seen that the highest performing projects tend to be active in more than one of the defined four major areas of Internet freedom, operating with relatively medium risk, have a low cost value, and short time frame. Specifically, projects that address both privacy and security are among the highest performers. This trend provides support for OTF's Theory of Change: The Internet freedom community has an asymmetric advantage in its response time, ability to operate at low cost, and contribution of effort driven by its dedication to the cause of free expression compared to those opposing free expression online, who, despite substantially larger budgets, are less nimble, cost efficient or innovative.

Strengthening the Internet Freedom Community

Collaboration with the BBG
In Fiscal Year 2013, OTF worked with the BBG's international broadcasters to better inform BBG journalists of digital security tools that enable them to better protect themselves and their sources. These activities included the release of a short digital guide on OTF-supported secure communication tools currently available worldwide and subsequent working sessions to engage BBG journalists in

[24] See Appendix I. These forms solicit information used to estimate the expected value and risk for each project, including background, desired outcomes, specific outputs, implementation strategy, methodology, the project's alignment with key Internet freedom attributes, cross-project synergy, tool employment, measures of performance achievement and effectiveness, and technical as well as programmatic risk, among others.

using these technologies. OTF also makes itself available to appropriately equip Governors with tools prior to overseas trips based on expected risk.[25] More, OTF initiated monthly calls with the BBG's Office of Digital & Design Innovation (ODDI) and International Broadcasting Bureau (IBB) Internet Anti-Censorship (TSI/IAC) program to identify opportunities to better leverage OTF's efforts in the BBG's digital operations. The result was better coverage and increased visibility of Internet freedom tools among international broadcasters and their audiences.

Coordination with Other Funders

In 2013, OTF substantially increased its communication, collaboration, and coordination efforts with a range of other funders. Among USG Internet freedom funders, OTF played an instrumental role in setting up recurring and open discussions to identify opportunities for complementary work and avoid duplicating efforts. OTF set up and maintains a discussion group of funders who manage public Internet freedom funds in order to build on these regular meetings. Consistent with this approach, OTF participated in multiple State Department review panels on Internet freedom funding and regularly attends other related meetings and events. OTF has extended the same opportunity to all its partner Internet freedom public funders and regularly consults with these funders to coordinate life-cycle sustainability for potential and current projects.

In addition to USG-centric efforts, OTF collaborates significantly with private foundations, NGOs, technology companies, international public funders, and start-up incubators, as well as more traditional human rights, democracy, and freedom of expression supporters. OTF strives to bridge the gap between historically siloed groups, bringing them together to discuss issues of shared relevance and coordinate efforts. This collaboration has allowed each funder to leverage their resources, maximizing their returns through a multiplier effect, resulting in increased support for global Internet freedom. In many instances, OTF seed-funded projects have gone on to receive substantial support from additional funders to continue their impact on Internet freedom, demonstrating the complementarity and synergy of this multi-stakeholder collaboration.

OTF coordinates funding decisions with the other USG funders to ensure life-cycle funding when appropriate, and preventing duplication of funds.

Security Audits

OTF is committed to establishing high-level Internet freedom technology privacy and security standards. One component of this commitment is conducting independent technology audits on all of its projects. Accordingly, OTF contracts with a range of professional information security auditors - including iSEC Partners, Cure53, Least Authority, and Veracode - who assess the privacy and security limitations of each project and suggest remedial strategies or specific changes. 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.

To maximize the impact of these audits and share information on how to replicate this process, OTF developed and published a methodology and framework for evaluating technical audit reports from the perspective of a funder.[26] Moreover, OTF offers in-kind audits to crucial Internet freedom projects including those not funded by OTF. In 2013, OTF supported technology audits of the 30 foremost

[25] Tools for Communication Security: https://www.opentechfund.org/article/tools-communication-security
BBG entities include: Voice of America, Radio Free Europe/Radio Liberty, the Middle East Broadcasting Networks (Alhurra TV and Radio Sawa), Radio Free Asia, and the Office of Cuba Broadcasting (Radio and TV Marti)
[26] https://www.opentechfund.org/article/report-how-evaluate-technical-audits-funder

Internet freedom projects, identifying in total 185 privacy and security vulnerabilities. Each one of these vulnerabilities was addressed in updated versions of audited technology, resulting in a swift and visible increase of privacy and security throughout the whole community.

Localizing Internet Freedom Tools

A major concern of the Internet freedom community has always been delays in tool-localization, e.g. adapting tools for adoption in various countries with attention to language, culture, and context. While a tool may improve a user's security, it is of limited use if it does not reach broad adoption, which is largely dependent on tool availability in a given user's native language. With OTF's global emphasis, supporting localization efforts has been key to expanding the reach of OTF-funded projects.

Prohibitive costs and limited availability of professional translation are two of the biggest hurdles to overcome when deploying Internet freedom tools globally. With continuous updates to software, recurring costs can quickly exceed a project's available resources. To address these challenges, OTF has partnered with Open Internet Tools Project (OpenITP) and Transifex to create an Internet freedom localization hub built on Transifex' online crowd-sourced translation platform.[27] Volunteers from around the world can contribute translations and ensure that a given tool is available in their native language. This localization hub has dramatically expanded the potential user base of Internet freedom tools. As this report went to press, the hub maintains more than 1,400 translators are working to translate 1.7 million words from 30 tools into 180 languages and dialects including Arabic, Farsi, Korean, Tibetan, Mandarin, Spanish, Ukrainian, and Vietnamese.

Internet Freedom Emergencies

OTF's Rapid Responder Initiative is an additional mechanism to provide quick support and resources to mitigate highly time-sensitive and urgent threats to Internet freedom. This initiative is designed to provide emergency support for efforts including, but not limited to:

- Establishing new Internet connections when existing connections have been cut off or are being restricted;
- Providing personal digital protection for online journalists and digital activists;
- Rapid development of tools or translations needed to respond adequately to emergencies;
- Developing decentralized, mobile Internet applications that can link computers as an independent network (mesh or delay-tolerant networks);
- Supporting digital activists with online services such as secure hosting and DDoS mitigation and providing capacity building as needed;
- Maintaining secure cloud infrastructure for Internet freedom projects; and
- Supporting emergency security and privacy audits.

OTF strives to assess and approve Rapid Response applications as quickly as possible. OTF typically supports Rapid Response projects for no more than $50,000 over four months or less. Support is only available through this mechanism when there is a clear time-sensitive digital emergency in which an applicant is seeking short-term and urgent support to respond. Rapid Response efforts do not support projects addressing digital security issues that are more structural in nature. All Rapid Response contracts are reviewed and approved by RFA's President, legal counsel, budget officer, and OTF to assess the project's necessity, appropriateness, risk, legality, and contractual structure.

[27] OpenITP: https://openitp.org/ Transifex: https://www.transifex.com/

Annual Summit

OTF held its second annual Summit in Washington, DC, September 4-5, 2013. All active projects were invited to send two people from their teams and OTF's Advisory Council members were invited to attend. In total, there were more than 50 participants. The summit is the one time each year that OTF gathers those running the projects and Advisory Council members in one place to facilitate project collaboration, information sharing, and brainstorming, and for OTF to get strategic feedback on the program goals for the coming year. The summit is a combination of OTF discussion topics, issues related to global strategy for Internet freedom, 19 participant-selected sessions and working groups. Session titles included: The Road Ahead and Future Problems, Inclusion and Diversity, and Secure Infrastructure. At the summit's conclusion, a dozen action items and goals for the coming year were identified and curated including: sharing of case studies, furthering of field testing, and raising of additional funds.

The Future

2014 Internet Freedom Funding

Congress passed the Consolidated Appropriations Act of 2014, commonly known as the Omnibus Act in January 2014.[28] This included appropriation decisions for 12 branches of the USG including the Department of State and the BBG - the two agencies primarily responsible for the disbursement of public Internet freedom funds.

In this 1,500 page-long Act, Congress designated "not less than" $50.5 million explicitly for Internet freedom, specifying that $25.5 million be spent by the BBG and $25 million by the Department of State. The Department of State's budget for Internet freedom has been at or near $25 million since 2011, the majority of which is spent by the Bureau of Democracy, Human Rights, and Labor (DRL) and USAID. The Consolidated Appropriations Act of 2014 increased the pool of Internet freedom funding by $16.4 million from the FY 2013 cumulative level of $34.1 million. Moreover, the BBG's one year appropriation designation was removed from the Internet freedom funding.[29]

Until 2011, the BBG's allocation for Internet freedom was $1.6 million. From FY 2011 to FY 2012, the BBG was able to increase its allocation for Internet freedom more than sevenfold to $11.6 million. Of this, OTF received $6.8 million in FY 2012. In FY 2013, the BBG's Internet freedom budget was reduced to $9.1 million, with OTF receiving $4.3 million.

In the language of the Consolidated Appropriations Act of 2014, Congress expressed its desire for government funds to be matched or leveraged by private, third-party funding. It also mandated that the bodies that manage these funds coordinate with other democracy, governance, and broadcasting programs.

At the time of publishing this report, the implications of this Act and the BBG's Internet freedom budget increase for OTF in Fiscal Year 2014 is currently undecided. A provision in the Act states that the BBG, Department of State, and USAID have 90 days after enactment to submit spending plans to the State, Foreign Operations, and Other Programs Appropriations Subcommittees within the House

[28] http://beta.congress.gov/113/bills/hr3547/BILLS-113hr3547enr.pdf
[29] Update from Congress: https://www.opentechfund.org/article/update-congress

of Representatives and Senate.[30] The decision on OTF's FY 2014 operating budget will appear as an update on OTF's website and in its the next annual report.

OTF Goals for 2014

Expanding Opportunities within the BBG

OTF intends to build on its work with the BBG and its entities in 2014. OTF will continue to identify opportunities to engage BBG journalists on secure communication strategies and to share relevant information on OTF tools. OTF will strive to make itself even more available for real-time in-country consultation for emerging censorship events and directly engages with sister entity personnel to address crisis environments worldwide. Further, OTF will build on previous collaboration with ODDI, TSI/IAC, and other BBG entities to gather feedback on secure communication gaps experienced in the field. One aspect of this assessment is to identify additional security features and platforms from OTF-incubated technologies now ready for day-to-day operations that can be integrated into the BBG's emerging digital toolkit in order to further modernize BBG entities. These efforts include, as appropriate:

- GlobaLeaks for an agency-wide platform to safely receive documents from whistleblowers around the world;[31]
- StoryMaker to help field and citizen journalists produce better video content capable of being sent directly to the BBG while protecting privacy;[32] and
- TextSecure, Mailvelope, and Cryptocat to allow staff, journalists, and sources to text message, email, or instant message securely.[33]

Increasing Capacity in the Internet Freedom Community

OTF plans to build on its contribution to the broader Internet freedom community by expanding its Direct Initiatives to create a series of Resource Labs in 2014. This will include the growth or establishment of:

- Localization Lab: translation infrastructure and community support;
- Legal Lab: connecting Internet freedom projects to law firms, clinics or individual lawyers;
- Engineering Lab: security audits, red-teaming and architecture reviews, and a global secure cloud;
- Usability Lab: making tools more usable and end-user friendly;
- Rapid Responders Fund; and
- Other labs identified over the coming year.

OTF nurtures the Internet Freedom community through quality assurance, transparency, direct initiatives, and increasing collaborative discourse within the community.

[30] House: http://appropriations.house.gov/subcommittees/subcommittee/?IssueID=34774; Senate: http://www.appropriations.senate.gov/sc-state.cfm.
[31] Globaleaks: https://globaleaks.org/
[32] Storymaker: https://storymaker.cc/
[33] Mailvelope: http://www.mailvelope.com/
Cryptocat: https://crypto.cat/

OTF Resource Labs will be a general set of mechanisms utilized by the program to offset its current inability to provide long-term funding support. The Labs are recognition that the community of Internet freedom and digital human-rights defenders require continuous sustenance rather than limited projects and constant re-application processes. The Labs are enduring capacity building efforts by OTF that reliably allow Internet freedom efforts to quickly obtain in-kind technical resources, strategic partnerships, and valuable lessons learned from others, at low cost in both time and effort.

Fostering Increased Transparency

In 2013, OTF launched a new website with the goal of being more transparent about its program, the program framework, the projects it supports, and the processes used to select projects. This commitment to increased accountability through open and accessible information has established OTF as a leader in transparency. In 2014, OTF reaffirms its commitment to transparency and accountability and will continue to add more information to the website sharing ideas, best practices, Internet freedom issues, and its means of operating.

Encouraging Collaboration

OTF will expand its current efforts and identify new opportunities to encourage collaboration amongst its partners. It will connect projects and people through in-person events such as its annual summit - a space to explore new solutions and bridge the gaps between different satellite communities. Further, OTF will continue identifying development and collaboration opportunities through its Resource Labs, through subject matter specific mini-summits. Finally, OTF online discussion groups will continue to be forums for which available funding for projects can expand.

Conclusion

OTF completed its second year of operation as an essential program supporting emerging Internet freedom technologies and as a champion of transparency and accountability in managing public funds. With 20 projects underway, more than 30 security audits conducted, 12 million more people now using secure communication, and strides towards diversifying and broadening the Internet freedom community, OTF has substantiated its role as an innovative leader in this field.

OTF's program structure and processes matured in 2013, making it more effective, efficient, and accountable. In FY 2013, OTF was able to make concrete contributions to long-standing Internet freedom resource gaps and to help bring together key funders from a range of disciplines to collaborate and coordinate efforts. By increasing partnerships within the Internet freedom community and without, OTF has created a leading program that is has been used as a model for forthcoming human rights technology and Internet freedom programs.

In FY 2014, OTF will seek to expand its ability to support solutions to evolving Internet freedom challenges throughout the world. Through OTF's commitment to transparency and knowledge-sharing within the Internet freedom community, OTF will continue to pioneer best practices that move the entire global Internet freedom movement forward. This annual report is meant to increase understanding about the OTF program and its impact as a starting place for the much-needed discussion and debates integral to the goal of global Internet freedom.

Appendix I - Peer Review Evaluation Form

A. CONFLICTS OF INTEREST AND CONFIDENTIALITY *

A conflict of interest, or an appearance of a conflict, can arise whenever a transaction, or an action, of Radio Free Asia (RFA) conflicts with the personal interests, financial or otherwise, of that of a Council Member, or an immediate family member of a Council member, or that of the Council Member's employer (collectively "your personal interests").

Please describe below any relationship, transactions or positions you hold (volunteer or otherwise), or circumstance that you believe could create a conflict of interest, now or in the future, between RFA, the proposing entity or individual, and your personal interests, financial or otherwise:

☐ I understand about confidentiality *

I have reviewed and previously agreed to the RFA Council Confidentiality and Non-disclosure Agreement and I understand that the received proposal contains "Confidential Information" that may not be publicly known and shall not be disclosed to any third party.

Do you have any conflicts of interest to report? *

- Select a value -

Conflict(s) of interest disclosure

If you checked yes, please list your conflict(s) of interest or potential conflict(s) of interest.

B. GENERAL THOUGHTS

This space is for general thoughts on the proposal. It is for comments and questions on areas not specifically addressed elsewhere in this evaluation form. Comments and questions posted here will be aggregated and returned to the Advisory Council and to the proposal authors where appropriate.

1. Things that you liked

Any general or specific aspects that got you really excited or that you like about this proposal.

2. Things that concern you

Any general or specific aspects that concern you or leave you feeling uneasy about this proposal.

3. Red Flags

Anything you think should be flagged for our attention.

C. SPECIFIC ASPECTS *

This section is asking you to score and comment on specific proposal aspects. Comments and questions posted here will be aggregated and returned to the Advisory Council and to the proposal authors where appropriate.

Scoring system: 1 is 'poor' or 'very weak' and 5 is 'excellent' or 'very strong.' 0 denotes more information needed – please specify in the space provided below each scoring section – and n/a indicates a section the reviewer prefers not to rate.

1. Project overview *

- Select a value - Show comment field

Are the project's goals clear? Are the project's goals realistically achievable by the proposed effort? Does the proposal identify and acknowledge what the challenges will be? Does the proposal state what is currently being done and the known limitations? Are project beneficiaries clear and specific? Is the project's sought after impact clear? Does the proposal cite an actual and compelling case study or user problem? Does the proposal state how much the effort will cost and how long will it take?

2. Proposal objectives *

- Select a value - Show comment field

Does the proposal state a clear and concise set of objectives and tasks for the proposed effort? Are the objectives S.M.A.R.T. (Specific, Measurable, Achievable, Relevant, Timely)? Is the project responding to a potential need or function that is currently unfilled, or will it be duplicating previous efforts or creating a solution in search of a problem?

3. Appropriate activities and strategy *

- Select a value - Show comment field

Does the project propose activities that are appropriate for its goals and objectives? Does it demonstrate effectively how it will accomplish its stated activities? Does the proposal suggest alternative or modified activities in response to changing circumstances? Are the proposed activities viable in the real world? Do the project activities disrupt the current internet freedom context? Directly or indirectly, do they increase tactical breathing space for existing challenges? Are the activity's tactics clearly identifiable as part of a wider strategy?

4. Technical feasibility (where applicable) *

- Select a value - Show comment field

Does the proposal clearly state the effort's technical objectives? Are technical objectives articulated succinctly and with appropriate language? Does the proposal explain what is novel about its approach and why it will succeed? Does the project identify any hurdles to achieving technical objectives? Does the proposal recognize potential technical byproducts, such as new or increased attack surfaces?

5. Alternative analysis – "red teaming" *

- Select a value - Show comment field

Does the project identify potential unintended consequences? Does it identify how an adversary might use the solution to further their own goals? Does the proposal consider potential illicit uses of the project? Does the proposal identify appropriate tactics for a potentially asymmetric position in relation to an adversary? Does the proposal consider sufficiently whether its approach is offensive or defensive in relation to the problem it is addressing? Does it explain why it has selected this approach (effort, cost, time, etc.)? Does the proposal explore short-, medium-, and long-term strategies from the adversary's point of view? Does the project increase or decrease known attack surfaces? Does the proposal discuss how the project could be undermined, identify its own deficiencies and limitation, or does it presume there are none?

6. Usability *

- Select a value - Show comment field

Does the proposal demonstrate clear external demand for the proposed end product? Does the project demonstrate a high degree of usability and/or accessibility? Is the project targeting a small number of high value or at-risk users, or a broader population? Is the proposed effort appropriate for the intended audience?

7. Sustainability *

- Select a value - Show comment field

Is this proposal clearly located within a larger plan for future project support, development, and implementation? Does the project have a diversified funding/support stream i.e., how dependent would the project be on OTF? Is the proposing entity able to sustain itself with the requested OTF funding in addition to other sources of direct or indirect support, such as community or other in-kind support that it already receives? Does the proposal identify any cost sharing or matching support for the proposed effort? Does the project currently receive any U.S. government or other public funding?

8. Collaboration *

- Select a value - Show comment field

Does the project support and further a collaborative and open community? Does the proposal facilitate inter-project collaboration, such as talking with like projects and identifying potential complementary aspects or points of overlap? Does the project seek to share resources or enable others to reuse the resources they develop? Do the objectives of this proposal contribute broadly to other Internet freedom projects?

9. Cost realism *

- Select a value - Show comment field

Is the budget realistic and commensurate with both the project objectives and time frame? Is this project realistically implementable within a payment-on-delivery framework, i.e. no funds up-front?

10. Qualifications *

- Select a value - Show comment field

Is the project team uniquely qualified to complete the proposed scope of work? Does the team have a history of successful work relevant to the proposed effort? Have team members worked with at-risk communities in the past? Does the proposing entity have a sufficient core team (leadership, developers, etc.) dedicated to this project? Are project team member(s) clearly identified, along with work experience, in the proposal?

11. Evaluation *

- Select a value - Show comment field

Does the project articulate a clear set of evaluation criteria and milestone metrics against activities, objectives, and deliverables? Are the criteria and metrics measurable quantitatively and/or qualitatively? How difficult will an assessment of success or failure be? Does the proposing entity have the capacity to self-evaluate and extract "lessons learned"? Is the proposed effort able to be openly peer reviewed and/or include a peer review process?

D. RATIONALE AND APPROPRIATENESS CONSIDERATION

Is the proposed project and its objectives in-line with OTF's principles and goals?

OTF mission:
OTF is a program that utilizes public funds to support Internet freedom projects. We support projects that develop open and accessible technologies promoting human rights and open societies. We strive to advance inclusive and safe access to global communication networks.

OTF guiding principles:
OTF supports freedom of speech and expression, freedom of the press, open exchange of ideas and information, open Internet, and Internet freedom. We strive to promote forward-thinking ideas and innovation, open philanthropy, alternative methodologies, new technologies, and social responsibility. We believe in collaboration, transparency, and accountability.

OTF program objectives:
- Advance research into repressive Internet interference on modern communication networks and discover the methodologies and technologies that circumvent it;
- Foster development of technologies to circumvent repressive censorship and surveillance, and increase communication access and safety;
- Enable widespread implementation of solutions that free people from repressive Internet interference.

Rationale and appropriateness rating
- None - Show comment field

E. GENERAL RECOMMENDATION *

Recommendation *
- Select a value -

Do you recommend supporting this effort based on this proposal?

OPEN TECHNOLOGY FUND

UPDATES / PROJECTS / LABS / SUBMIT / ABOUT / CONTACT NEXT DEADLINE: MAY 1

Current / Past

Projects

Cryptocat

https://crypto.cat

Cryptocat is a web application that aims to provide an open source, browser-based communication environment with security that is comparable to desktop-based encrypted chat applications. Cryptocat aims to leverage both the ease of use and accessibility afforded by web applications and the security provided by client-side public key cryptosystems.

Show / Hide Project info

Twitter
@cryptocatapp
Funding to date:

2012: $93 000 12 months
2013: $91 000 12 months

Total funding $184 000

Related articles
After initial rejection, Cryptocat finally launches on iOS
January update
OTF 2013 Projects Part 2
December update
November update

Cupcake Bridge

http://cupcakebridge.com

Tor bridges are Tor relays that aren't listed in the main Tor directory. They are a step forward in the blocking resistance race. Cupcake Bridge is a browser extension that allows users to become new Tor bridges automatically, without having to install a full software suite or configure anything. This project would bring create a Cupcake Bridge extension for Firefox and plugins to work on sites like Wordpress and Drupal significantly growing the number of global Tor bridges.

Show / Hide Project info

Twitter
@abditum
Funding to date:

2013: $66 966 12 months

Total funding $66 966

Related articles
January update
OTF 2013 Projects Part 2
November update
Tor calls for help as its supply of bridges falters