OPEN TECHNOLOGY FUND

FY 2018 Annual Report

Open Technology Fund

Table of Contents

About this Report

This report covers the activities supported by OTF with FY2018 funds. Therefore, with a small number of exceptions for highly sensitive projects, the report covers all projects, fellows, and labs that OTF funded from roughly July 2018 through September 2019. More information is available at opentech.fund.

About OTF

Our Mission

The Open Technology Fund (OTF) works to advance internet freedom in repressive environments by supporting the research, development, implementation, and maintenance of technologies that provide secure and uncensored access to the U.S. Agency for Global Media's (USAGM) content as well as the broader internet. This critical support helps to counter attempts by authoritarian governments to restrict freedom online.

Originally established in 2012 as a program within Radio Free Asia a private non-profit corporation funded through a grant from USAGM, OTF was incorporated as a new independent organization in September 2019. Over the last seven years, OTF has supported pioneering research, development, and implementation of cutting-edge internet freedom technologies to respond to rapidly evolving censorship threats around the world. Today, over two billion people use OTF-supported technology on a daily basis, and more than two-thirds of all mobile users have OTF-incubated technology on their device.

OTF supports projects in an effort to:

- **Provide unrestricted access to the internet** to individuals living in information-restrictive countries to help ensure they are able to safely access USAGM content and other essential news and information otherwise censored by their governments. This includes supporting the development and deployment of an array of circumvention technologies to counter increasingly sophisticated censorship techniques, as well as funding applied research and awareness-raising to help circumvention tool developers and users stay ahead of the censors.

- **Protect journalists, sources, and audiences from repressive surveillance and digital attacks** to help ensure they are able to safely create and engage with USAGM content. This includes support for secure communication tools, targeted digital security interventions, and other forms of privacy and security technology.

Our Approach

OTF provides resources through a variety of implementation mechanisms to provide tailored and comprehensive assistance to internet freedom projects. Because internet censorship technology and tactics are constantly evolving and adapting, OTF receives, reviews, and contracts projects on an ongoing basis via open calls.

OTF solicits project ideas through a fully open, competitive, and rolling application process on its website. The process is designed to reduce barriers to entry in an effort to make funding more accessible to qualified individuals and organizations around the world. These efforts help

attract innovative applications from groups that traditionally are not able to apply for federal funds, including expert technologists, frontline journalists, human rights defenders, cutting-edge researchers, and digital security specialists. OTF's commitment to lowering barriers to entry results in a vast number of applications, requiring the organization to be extremely efficient in its review and ultimate funding of operations.

In order to ensure a high degree of due diligence, OTF implements a rigorous multi-stage application review process throughout which successful applications are ultimately improved and refined. All proposals are reviewed by OTF's specialized staff of subject matter experts as well as OTF's Advisory Council—a group of nearly 40 technical, regional, and specialized experts from a wide range of relevant disciplines—to provide feedback and guidance. In addition to ensuring that the most competitive and impactful projects are funded, this multistage review process also achieves maximum efficiency, collaboration, and economies of scale resulting in substantial savings of public funds.

During the time period covered by OTF's Fiscal Year 2018 appropriations,[1] OTF implemented four funds, six labs, and two fellowship programs.

- **Funds**: OTF provided direct funding to support the research, development, and implementation of technologies that enable censorship circumvention and enhance online user security and privacy. During the FY18 period, support was provided primarily through four funds:

    - Internet Freedom Fund (IFF) is the primary mechanism through which OTF provides funding for innovative global internet freedom projects. Projects receiving IFF support are primarily focused on technology development, and also include research and digital security projects. OTF solicits IFF project proposals year-round through an open and transparent application process. Submissions are reviewed every two months.

    - Core Infrastructure Fund (CIF) supports the essential "building block" technologies that help power everyday digital security and circumvention tools. This infrastructure (which includes PGP, SSL,[2] SSH, Tor, TLS, pluggable transports, and code libraries) is utilized by people throughout the world to increase their online access, privacy, and security. Yet despite the widespread adoption of these foundational technologies across the private sector, the

[1] This report covers programmatic spending for OTF's FY2018 funding, which occurred over a period roughly spanning from July 2018 through September 2019

[2] A fundamental weakness in HTTPS encryption allows powerful third parties, such as the Chinese and Iranian governments, to use TLS certificates to perform man-in the-middle attacks. An OTF-supported project identified techniques to protect against these attacks. The techniques have since been adopted by Cloudflare (which hosts more than 20 million websites) and Let's Encrypt (which has provided SSL certificates for nearly 190 million active domains). *See, e.g.*, Emma Woollacott, "Oracle confirms China Telecom BGP hijacking claims," *The Daily Swig*, November 9, 2018, <https://portswigger.net/daily-swig/oracle-confirms-china-telecom-bgp-hijacking-claims> and Charlie Osborne, "BGP attacks hijack Telegram traffic in Iran," *ZDNet*, November 6, 2018, <https://www.zdnet.com/article/persian-stalker-grayware-targets-telegram-instagram-users/>.

ongoing development needed to keep them viable tends to fall on the shoulders of volunteers. CIF's support of these efforts is therefore essential to help ensure the efficacy and security of critical circumvention and security tools, as well as the safety of the people using them.

    - Community Prototype Fund (CPF) supports the rapid development of new, cutting-edge internet freedom technology prototypes that serve the needs of independent journalists and human rights defenders. Through the CPF, technologists and activists receive micro-investments to bring new, creative ideas to proof-of-concept, particularly in areas of the ecosystem where gaps exist.

    - Rapid Response Fund provides emergency support to independent media outlets, journalists, and human rights defenders facing imminent digital attacks and acute censorship events. These efforts help them stay safe, get back online, and mitigate future attacks.

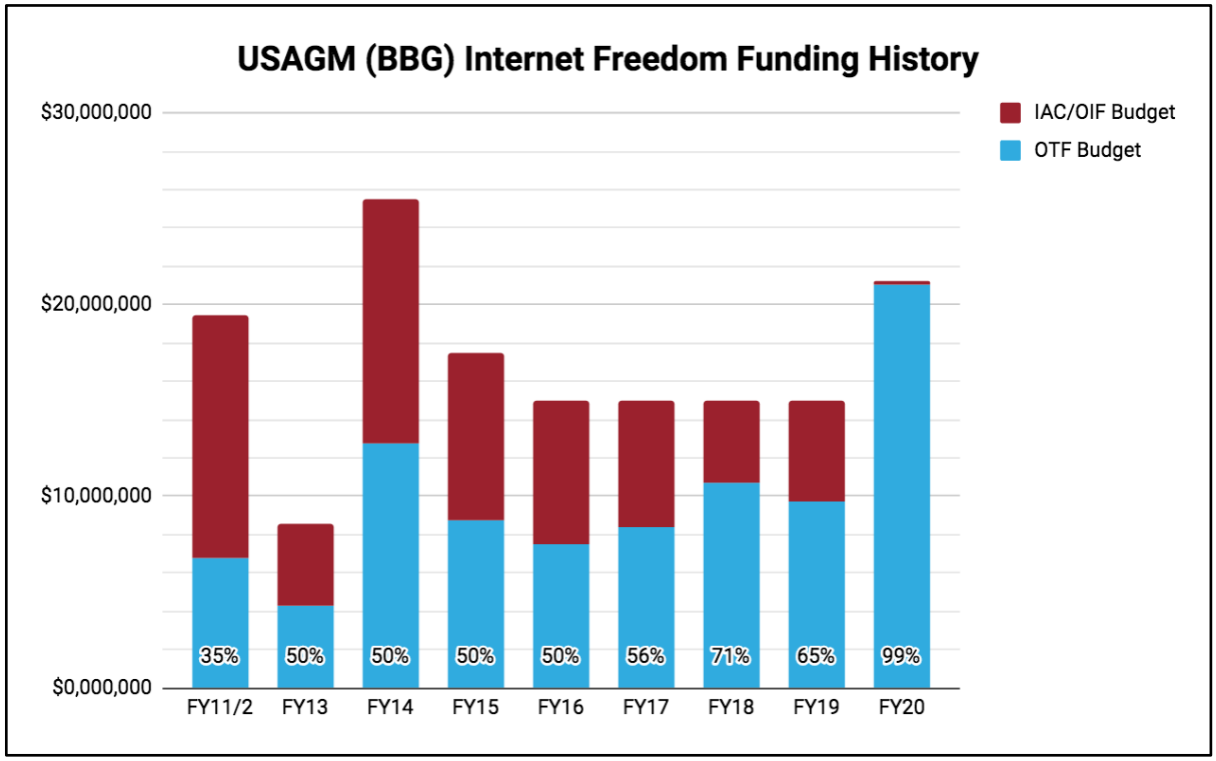
- **Fellowships**: OTF also supported two fellowship programs - the Information Controls Fellowship Program (ICFP) and the Digital Integrity Fellowship Program (DIFP). The ICFP helps individuals conduct critical applied research projects to examine the means by which authoritarian states restrict the free flow of information and to help devise ways for citizens to overcome those tactics. This real-time research feeds directly into the implementation of technical solutions to emerging threats, creating a dynamic feedback loop between research and development. The DIFP enables digital security experts to provide hands-on, comprehensive internal support to organizations and communities most affected by internet freedom violations (such as journalists, human rights defenders, NGOs, activists, and bloggers) . OTF fellowships also help to cultivate the next generation of internet freedom experts by creating a viable career track for those who have the skills and passion for internet freedom.

- **Labs**: In addition to direct funding, OTF provided a number of vital expert service offerings through its Labs, including security audits, usability assessments, engineering support, tool translation, writing and graphic design support, and secure cloud storage. These services were provided through six separate Labs: the Engineering Lab, the Red Team Lab, the Usability Lab, the Community Lab, the Localization Lab, and the Learning Lab.

  Lab services help ensure the technologies incubated and supported by OTF are as effective, secure, and usable as possible. By coordinating the provision of these services through Labs, OTF is able to achieve large economies of scale and bring down the overall cost of providing expert support to internet freedom projects. These services are available to both OTF-funded projects, as well as other important internet freedom efforts, through applications associated with each Lab.

OTF Funding

OTF's FY2018 budget allocation totaled $9.5 million in programmatic funds and $1.2 million in salaries and benefits. This budget comes from part of the Internet Freedom (IF) funds allocated by Congress to USAGM (formerly the Broadcasting Board of Governors). To date, IF funds have been divided between OTF and USAGM's Office of Internet Freedom (OIF), as approved by the USAGM CEO and Board. The total amount of IF funds allocated to USAGM have remained stable for several years at $15 million. This trend continued into FY2019, for which OTF was allocated approximately $8.5 million in programmatic funding and $1.2 million to Radio Free Asia for OTF salaries and benefits (with the balance of USAGM's overall $15 million IF allocation going to OIF). As the final section will explain, however, OTF was given approval to spin off and form its own independent organization under the USAGM umbrella as a grantee corporation in the FY2020 congressional appropriations. At the same time, the USAGM's programmatic annual IF allocation increased to $20 million, with the vast majority (save for a small portion which USAGM retains for oversight) going to OTF.



Unfortunately, the resources available to repressive regimes attempting to censor and surveil the internet far exceed those available to the internet freedom community. It is therefore paramount that every available dollar of internet freedom funding be well-coordinated and well-spent. As part of OTF's role as a U.S. internet freedom funder, OTF coordinates closely with other U.S. government funding sources such as the State Department and USAID, as well as a host of private foundations, in order to ensure that the overall internet freedom funding landscape is calibrated to the needs of the internet freedom community such that impactful projects are able to find appropriate funding sources. Notably, over its operating history, OTF

has raised awareness of the need for greater internet freedom funding and unlocked new sources, helping to bring the total amount of private funds set aside for internet-freedom-related efforts to more than $100 million since 2012.

Accordingly, OTF continues to raise awareness of other funding opportunities for those in the internet freedom community by sending out regular “Alternative Sources of Funding” updates, encouraging those with good ideas to investigate the full range of government and non-government funding sources, and referring competitive projects to other funders.

To ensure well-calibrated donor coordination including de-duplication of funding, OTF actively participates in numerous external review panels of related technology proposals and provides consultation upon request to other funders, including the State Department’s Internet Freedom Program, USAGM Office of Internet Freedom, Access Now, Media Democracy Fund, Ford Foundation, Open Society Foundations, MacArthur Foundation, Knight Foundation, Mozilla Foundation, British Broadcasting Corporation, Deutsche Welle, Swedish International Development Agency, and the German Federal Foreign Office.

Threats to Internet Freedom

During the time period covered by OTF's Fiscal Year 2018 appropriations,[3] authoritarian actors around the world took increasingly aggressive and expansive steps to consolidate their control over what citizens could read, write, or share online. Many governments viewed an open, global, and secure internet as a threat to their power and control over their citizens. Online free expression and even basic connectivity were therefore routinely targeted and suppressed, especially during key political times such as elections and protests. This section provides an overview of these critical developments and addresses relevant threat trends from a high-level perspective.

Censorship and Shutdowns

Around the world, numerous governments sought to block their citizens' internet connectivity, whether in part (site-specific) or in whole (network-level). For example, in January 2019 the Cyberspace Administration of China announced that it had "cleaned up" more than 9,000 apps and shut down more than 700 websites over their hosting of "harmful" content.[4] Throughout the year, the ruling Chinese Communist Party started blocking previously accessible media sites such as The Washington Post, The Guardian, The Intercept, and NBC News,[5] as well as all language versions of Wikipedia.[6] This intense censorship environment was bolstered by so-called "censorship factories," where thousands of employees work diligently to help companies comply with vague and ever-shifting rules on acceptable content.[7] Through a multifaceted information controls strategy, the Chinese government also expanded its reach beyond the country's territorial borders. The regime made its presence felt abroad by increasing its international media presence, censoring Chinese platforms like WeChat (even for users abroad), and intimidating critical exile voices.[8]

While China has long been recognized as a world-leader when it comes to sophisticated censorship, repressive governments elsewhere are working to catch-up. In Venezuela, the Nicolas Maduro regime instituted highly targeted, short-term censorship of key social platforms to coincide with speeches made by political opposition figures.[9] And in July 2019, the

[3] This report covers programmatic spending for OTF's FY2018 funding, which occurred over a period roughly spanning July 2018 through September 2019

[4] BBC News, "Chinese censor calls Tencent news app 'vulgar,'" *BBC News*, January 23, 2019, <https://www.bbc.com/news/technology-46978924>.

[5] Ryan Gallagher, "China Bans The Intercept and Other News Sites in 'Censorship Black Friday,'" *The Intercept*, June 7, 2019, <https://theintercept.com/2019/06/07/china-bans-the-intercept-and-other-news-sites-in-censorship-black-friday/>.

[6] Sukhbir Singh, Arturo Filastò, and Maria Xynou, "China is now blocking all language editions of Wikipedia," *OONI*, May 4, 2019, <https://ooni.org/post/2019-china-wikipedia-blocking/>.

[7] Li Yuan, "Learning China's Forbidden History So They Can Censor It," *The New York Times*, January 2, 2019, <https://www.nytimes.com/2019/01/02/business/china-internet-censor.html>.

[8] Reporters Without Borders, "RSF Report: 'China's Pursuit of a New World Media Order,'" *Reporters Without Borders*, October 22, 2019, <https://rsf.org/en/reports/rsf-report-chinas-pursuit-new-world-media-order>.

[9] Elias Groll, "Playing Cat and Mouse With Venezuela's Internet Censors," *Foreign Policy*, May 3, 2019, <https://foreignpolicy.com/2019/05/03/playing-cat-and-mouse-with-venezuelas-internet-censors/>.

Kazakhstan government attempted to intercept all HTTPS traffic inside its borders by compelling local ISPs to force users to install "a government-issued certificate on all devices, and in every browser."[10] This plan would have allowed the government to decrypt and analyze a user's internet traffic. Following widespread criticism, however, the government walked back the proposed system and called it just a "test."[11] Nonetheless, Apple, Google, and Mozilla made adjustments to block the certificate from working if it were to be reintroduced at a later date.[12] Meanwhile, the Egyptian government "collaterally blocked" thousands of websites while attempting to block the website of the Batel ("Void") opposition political campaign.[13] According to a report by OTF-supported OONI, the websites of the U.S.-funded Alhurra news network and BBC were also blocked in Egypt following anti-government protests.[14]

Beyond the targeted blocking of specific sites and apps, the growing prevalence of internet shutdown events around the world represents an alarming and increasing authoritarian trend. Shutdowns often coincided with events like elections (such as in Bangladesh,[15] Benin,[16] and the Democratic Republic of Congo,[17] to name but a few) or protests (as happened in Iran,[18] Sudan,[19] Zimbabwe,[20] Algeria,[21] and

"We can't move anywhere and now we can't communicate with anyone … We are in total darkness."

Rohingya resident in Maungdaw Township, Myanmar, experiencing an internet shutdown, as told to Fortify Rights.

[10] Catalin Cimpanu, "Kazakhstan government is now intercepting all HTTPS traffic," *ZDNet*, July 18, 2019, <https://www.zdnet.com/article/kazakhstan-government-is-now-intercepting-all-https-traffic/>.
[11] Olzhas Auyezov, "Kazakhstan halts introduction of internet surveillance system," *Reuters*, August 7, 2019, <https://www.reuters.com/article/us-kazakhstan-internet-surveillance/kazakhstan-halts-introduction-of-internet-surveillance-system-idUSKCN1UX0VD>.
[12] Zack Whittaker, "Apple Google and Mozilla block Kazakhstan's browser spying tactics," *TechCrunch*, August 21, 2019, <https://techcrunch.com/2019/08/21/google-mozilla-kazakhstans-browser-spying/>.
[13] Mohammad El-Taher, "Thousands of Websites are collaterally blocked in Egypt," *AFTE*, May 22, 2019, <https://afteegypt.org/en/digital_freedoms-2/publications_digital_freedoms-digital_freedoms-en/2019/05/19/17500-afteegypt.html>.
[14] Ramy Raoof, Mohamed El-Taher, Mohamed Tita, Arturo Filastò, and Maria Xynou, "Egypt blocks BBC and Alhurra: Expanding media censorship amid political unrest," *OONI*, September 26, 2019, <https://ooni.org/post/2019-egypt-blocks-bbc-and-alhurra/>.
[15] Aljazeera, "Bangladesh shuts down mobile internet in lead up to election day," *Aljazeera*, December 29, 2018, <https://www.aljazeera.com/news/2018/12/bangladesh-shuts-mobile-internet-lead-election-day-181229111353218.html>.
[16] Salem Solomon, "Benin Internet Shutdown Repeats Pattern of Government Censorship Across Africa," *Voice of America*, April 30, 2019, <https://www.voanews.com/africa/benin-internet-shutdown-repeats-pattern-government-censorship-across-africa>.
[17] Raidió Teilifís Éireann, "DR Congo govt cuts internet to avert 'popular uprising,'" *Raidió Teilifís Éireann*, January 1, 2019, <https://www.rte.ie/news/world/2019/0101/1019866-dr-congo-internet/>.
[18] Michelle Quinn, "Iranians Struggle Without the Internet," *Voice of America*, November 20, 2019, <https://www.voanews.com/middle-east/iranians-struggle-without-internet>.
[19] Abdi Latif Dahir, "Sudan's anti-government protests face a total power outage and social media shutdown," *Quartz Africa*, April 8, 2019, <https://qz.com/africa/1589356/sudan-protests-cuts-off-electricity-social-media-shutdown/>.
[20] Maria Xynou, Arturo Filastò, Tawanda Mugari, and Natasha Msonza, "Zimbabwe protests: Social media blocking and internet blackouts," *OONI*, January 23, 2019, <https://ooni.org/post/zimbabwe-protests-social-media-blocking-2019/>.
[21] Abdi Latif Dahir, "Algeria has blocked the internet days before its ailing president files to run for a fifth term," *Quartz Africa*, March 2, 2019, <https://qz.com/africa/1563958/algeria-shuts-internet-amid-anti-bouteflika-election-protests/>.

Russia[22]). Elsewhere, authorities severed connectivity in conflict areas where reporting and documentation of human rights abuses were most needed, such as in Myanmar (Rakhine and Chin States)[23] and India (Kashmir).[24] And the Republic of Chad oversaw a 16-month block on social media sites like Facebook, WhatsApp, Twitter, Instagram, and YouTube in what is considered to be the longest recorded shutdown event of all-time.[25] Globally, more than 200 documented internet shutdown events occurred in 2019 in 33 different countries (up from 25 countries in 2018).[26] These shutdowns cost the global economy more than $8 billion in 2019.[27]

Surveillance and Spyware

Journalists, activists, and other members of civil society continued to face threats to their work and personal safety due to targeted surveillance by sophisticated state actors. Many individuals and specific groups found themselves under attack. For example, Tibetans working for the office of the Dalai Lama, the Central Tibetan Administration, and the Tibetan parliament were targeted through phishing campaigns intended to install spyware on their iOS or Android devices.[28] In 2017 covert surveillance technology was used by authorities in Myanmar to access the phones of Reuters journalists Wa Lone and Kyaw Soe Oo to build prosecutorial cases against them for reporting on human rights abuses in the country.[29] And an Amnesty International report uncovered a targeting phishing campaign attacking Egyptian human rights defenders, likely instigated by Egyptian authorities.[30] Amnesty itself was even the target of a state-sponsored online attack in April 2019 when its Hong Kong chapter was attacked by "hostile groups linked to the Chinese government." [31]

---

[22] Meduza, "'BBC Russian Service' reportedly finds letter confirming that Moscow police ordered cell signal shutdown during August 3 protest," *Meduza*, August 7, 2019, <https://meduza.io/en/news/2019/08/07/bbc-russian-service-reportedly-finds-letter-confirming-that-moscow-police-ordered-cell-signal-shutdown-during-august-3-protest>.
[23] James Griffiths, "Myanmar shuts down internet in conflict areas as UN expert warns of potential abuses during blackout," *CNN*, June 25, 2019, <https://www.cnn.com/2019/06/25/asia/myanmar-internet-shutdown-intl-hnk/index.html>.
[24] C.K. Hickey, "India is the World's Leader in Internet Shutdowns," *Foreign Policy*, August 5, 2019, <https://foreignpolicy.com/2019/08/05/india-is-the-worlds-leader-in-internet-shutdowns/>.
[25] Abdi Latif Dahir, "After a record 16-month ban, this president has unblocked social media access," *Quartz Africa*, July 16, 2019, <https://qz.com/africa/1667263/chads-idriss-deby-unblocks-social-media-after-record-shutdown/>.
[26] Access Now, "Targeted, Cut Off, And Left In The Dark: The #KeepItOn report on internet shutdowns in 2019," *Access Now*, 2020, <https://www.accessnow.org/cms/assets/uploads/2020/02/KeepItOn-2019-report-1.pdf>.
[27] Chloe Taylor, "Government-led internet shutdowns cost the global economy $8 billion in 2019, research says," *CNBC*, January 8, 2020, <https://www.cnbc.com/2020/01/08/government-led-internet-shutdowns-cost-8-billion-in-2019-study-says.html>.
[28] Bill Marczak, Adam Hulcoop, Etienne Maynier, Bahr Abdul Razzak, Masashi Crete-Nishihata, John Scott-Railton, and Ron Deibert, "Missing Link: Tibetan Groups Targeted with 1-Click Mobile Exploits," *The Citizen Lab*, September 24, 2019, <https://citizenlab.ca/2019/09/poison-carp-tibetan-groups-targeted-with-1-click-mobile-exploits/>.
[29] Timothy McLaughlin, "Security-tech companies once flocked to Myanmar. One firm's tools were used against two journalists," *The Washington Post*, May 4, 2019, <https://www.washingtonpost.com/world/asia_pacific/security-tech-companies-once-flocked-to-myanmar-one-firms-tools-were-used-against-two-journalists-/2019/05/04/d4e9f7f0-5b5d-11e9-b8e3-b03311fbbbfe_story.html>.
[30] Amnesty International, "Egypt: Activists, government critics hit by wave of digital attacks," *Amnesty International*, March 6, 2019, <https://www.amnesty.org/en/latest/news/2019/03/egyptactivists-government-critics-hit-by-wave-of-digital-attacks/>.
[31] Amnesty International, "State-sponsored hackers target Amnesty International Hong Kong with sophisticated cyber attack," *Amnesty International*, April 25, 2019, <https://www.amnesty.org/en/latest/news/2019/04/state-sponsored-cyber-attack-hong-kong/>.

In addition to targeting specific individuals or groups, state actors also became increasingly adept at large-scale monitoring. For example, perhaps unprecedented in pervasiveness and scale, the Uyghur community in China's Xinjiang Uyghur Autonomous Region experienced constant monitoring in the form of facial recognition-equipped cameras, mandatory use of surveillance software, police checkpoints, and informants.[32] Police in Xinjiang use an app called IJOP to collect "massive amounts of personal information," which the app then uses to flag activities considered to be suspicious.[33] The use of these tactics and others like them resulted in the mass imprisonment of as many as a million mostly ethnic Uyghur and Kazakh people.[34]

The Chinese government's crackdown on Uyghurs extended beyond the country's borders, as telecom networks in Central and Southeast Asia were reportedly hacked in order to spy on Uyghur travelers abroad.[35] Research revealed nearly a dozen websites popular with Uyghurs were compromised, becoming "watering holes" for unsuspecting visitors who had spyware installed on their devices after visiting the sites.[36] Surveillance techniques like this, once used sparingly and only to target select individuals, can now be applied to target larger population swaths.[37]

> **"If you are targeting one activist, it might cost one million dollars for the necessary zero day exploit, but if you are able to monitor thousands of activists or an entire ethnic population with a single exploit suddenly the cost per person drops down to a much more affordable price."**
>
> Cooper Quintin, "Watering Holes and Million Dollar Dissidents: The Changing Economics of Digital Surveillance," EFF.

[32] *See, e.g.*, Chris Buckley, Paul Mozur, and Austin Ramzy, "How China Turned a City into a Prison," *The New York Times*, April 4, 2019, <https://www.nytimes.com/interactive/2019/04/04/world/asia/xinjiang-china-surveillance-prison.html>.
[33] Maya Wang, "China's Algorithms of Repression: Reverse Engineering a Xinjiang Police Mass Surveillance App," *Human Rights Watch*, May 1, 2019, <https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass-surveillance>.
[34] Austin Ramzy and Chris Buckley, "'Absolutely No Mercy': Leaked Files Expose How China Organized Mass Detentions of Muslims," *The New York Times*, November 16, 2019, <https://www.nytimes.com/interactive/2019/11/16/world/asia/china-xinjiang-documents.html>.
[35] Jack Stubbs, "China hacked Asian telcos to spy on Uighur travelers: sources," *Reuters*, September 5, 2019, <https://www.reuters.com/article/us-china-cyber-uighurs/china-hacked-asian-telcos-to-spy-on-uighur-travelers-sources-idUSKCN1VQ1A5>.
[36] Kevin Collier, "China hacked iPhones and Android devices to target Uyghur Mulisms," *CNN*, September 4, 2019, <https://www.cnn.com/2019/09/04/politics/china-uyghur-hack/index.html>.
[37] Cooper Quintin, "Watering Holes and Million Dollar Dissidents: The Changing Economics of Digital Surveillance," *Electronic Frontier Foundation*, September 9, 2019, <https://www.eff.org/deeplinks/2019/09/watering-holes-and-million-dollar-dissidents-changing-economics-digital>.

Exporting Authoritarianism

No longer the sole provenance of only the most well-resourced states, advanced surveillance and censorship tools are increasingly cropping up in repressive contexts around the world. The Chinese telecom company ZTE, for example, is helping Venezuela to develop a smart ID card that many fear will be used by the government as a powerful surveillance tool.[38] And, in the face of mounting opposition protests, the Serbian government also turned to a Chinese telecom company, acquiring a 1,000-camera-strong surveillance system from Huawei.[39] Huawei has built over 70% of the 4G networks on the African continent, raising concerns around surveillance and user privacy.[40] Validating these fears, the Wall Street Journal in August 2019 revealed that Huawei technicians had helped the governments of Uganda and Zambia spy on political dissidents.[41]

A global review shows just how far these technologies, techniques, and tactics have spread. A September 2019 report authored by OTF Information Controls fellow Valentin Weber examined the diffusion of these types of surveillance technologies and found that 110 different countries had purchased, imitated, or received training on information controls from China or Russia.[42] There are also indications that the Russian government is attempting to mimic China's Great Firewall.[43] And although the results have so far been mixed (see for example Russia's failed attempted Telegram block in 2018), it is clear that authoritarian states like Russia are seeking more and more online control.

> **"Beijing's experience using digital tools for domestic censorship and surveillance has made it the supplier of choice for illiberal regimes looking to deploy their own surveillance systems[.] "**
>
> Alina Polyakova and Chris Meserole,
> "Exporting digital authoritarianism: The Russian and Chinese models," Brookings Institute.

[38] Angus Berwick, "How ZTE helps Venezuela create China-style social control," *Reuters*, November 14, 2018, <https://www.reuters.com/investigates/special-report/venezuela-zte/>.
[39] Bojan Stojkovski, "Big Brother Comes to Belgrade," *Foreign Policy*, June 18, 2019, <https://foreignpolicy.com/2019/06/18/big-brother-comes-to-belgrade-huawei-china-facial-recognition-vucic/>.
[40] Amy Mackinnon, "For Africa, Chinese-Built Internet Is Better Than No Internet At All," *Foreign Policy*, March 19, 2019, <https://foreignpolicy.com/2019/03/19/for-africa-chinese-built-internet-is-better-than-no-internet-at-all/>.
[41] Joe Parkinson, Nicholas Bariyo, and Josh Chin, "Huawei Technicians Helped African Governments Spy on Political Opponents," *The Wall Street Journal*, August 15, 2019, <https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017?mod=e2tw>.
[42] Open Technology Fund, "Examining the Expanding Web of Chinese and Russian Information Controls," *Open Technology Fund*, September 17, 2019, <https://www.opentech.fund/news/examining-expanding-web-chinese-and-russian-information-controls/>.
[43] Reuters, "Chinese, Russian cyber watchdogs meet in Moscow," *Reuters*, July 17, 2019, <https://www.reuters.com/article/russia-china-internet/chinese-russian-cyber-watchdogs-meet-in-moscow-idUSL8N24I4RF>.

From 5G to BGP: Infrastructure and Network-Level Security

Concerns surround who will build and maintain the fundamental network infrastructure of the future. The creation of 5G (or fifth generation mobile network) is intended to usher in a new era of connectivity speed, performance, and interoperability between devices. Yet alongside the promise of new possibilities come critical internet freedom questions. How will human rights protections be incorporated from the earliest stages of 5G's implementation? How will internet freedom technologies adapt to a new network and new security concerns? And looming over it all, what type of surveillance capabilities will a 5G network operator such as Huawei gain?

Fundamental security issues related to the way the internet functions from a high-level perspective also exist. For example, the Border Gateway Protocol (BGP) acts as the internet's global routing system and plays an integral role in making sure online data arrives at its intended destination. But because the BGP was developed during the early days of the internet, fundamental weaknesses in the system exist, such as susceptibility to hijack attacks and reliance on trust. Unfortunately, these weaknesses can be exploited. In November 2018, for instance, researchers found evidence of BGP hijacking campaigns being waged against Iranian users of Telegram and Instagram.[44] And in June 2019, "a large chunk" of European mobile traffic was rerouted through Chinese ISP China Telecom for two hours, reportedly due to a BGP routing leak.[45] To address this issue, internet standards bodies have started developing the Resource Public Key Infrastructure (RPKI). Though RPKI will improve trust and authentication in the routing process, and better prevent route hijacking or spying, it remains a work in progress.

Network-level security issues persist as well. Over the past year, several governments have made progress building national intranets in which online traffic is limited to networks and websites operated in-country. In May 2019, Iran announced its national information network was 80%

> **"With Russia and Iran spearheading a new level of internet fragmentation, they're not just threatening the global network architecture (cables, servers) or working to allow the government to greatly control information flows and crack down on freedoms; their actions could also inspire others to follow suit and create geopolitical implications extending far beyond those two countries' borders."**
>
> Justin Sherman, "Russia and Iran Plan to Fundamentally Isolate the Internet," Wired.

[44] Danny Adamatis, Warren Mercer, Paul Rascagneres, Vitor Ventura, and Eric Kuhla, "Persian Stalker pillages Iranian users of Instagram and Telegram," *Talos Intelligence*, November 5, 2018, <https://blog.talosintelligence.com/2018/11/persian-stalker.html>.
[45] Catalin Cimpanu, "For two hours, a large chunk of European mobile traffic was rerouted through China," *ZDNet*, June 7, 2019, <https://www.zdnet.com/article/for-two-hours-a-large-chunk-of-european-mobile-traffic-was-rerouted-through-china/>.

complete.[46] To increase use of the new domestic network, the Iranian government has developed copycat versions of popular foreign apps and sites and made them available at lower cost than the authentic versions.[47] Similarly, the Russian government approved regulations for its own domestic-only intranet, which it plans to test through an intentional country-wide internet shutdown.[48] These troubling trends pose obvious obstacles to internet freedom around the world.

Controlling the Narrative, Rigging the Rules: Disinformation Campaigns and Policy Trends

Repressive regimes engaging in censorship have increasingly supplied their citizens with state-backed disinformation. By clearing out the presence of critical voices, such governments create information vacuums that they can then fill with a desired narrative. These insidious actions continued over the past year, with authoritarian governments using social media to spread disinformation and counteract critical reporting. The Myanmar government, for instance, used Facebook to push a false narrative around violence against the country's minority Rohingya Muslims.[49] Similarly, Citizen Lab identified an Iran-aligned network of social media accounts and websites designed to look like legitimate accounts which were being used to spread false information critical of the US and Israel.[50] And the Chinese government used Twitter and Facebook to spread disinformation prior to elections (in Taiwan) and amid large scale anti-government protests (in Hong Kong), all the while continuing to block both platforms inside China's mainland borders.[51]

In addition to these attempts to control the information landscape, many authoritarian states continued to rely on legal frameworks to legitimize their invasive censorship and surveillance practices. Specific laws and policies were used to pressure private sector companies to comply with government censorship demands ("content takedowns") and to compel them to store user data in-country ("data localization"). In 2019, Vietnam passed a new cybersecurity law criminalizing criticism of the government and requiring companies to not only store Vietnamese

[46] Radio Farda "Iran says its Intranet is almost ready to shield country from 'harmful' internet," *Radio Farda*, May 20, 2019, <https://en.radiofarda.com/a/iran-says-its-intranet-almost-ready-to-shield-country-from-harmful-internet/29952836.html>
[47] Center for Human Rights in Iran, "Speed and Bandwidth," *Center for Human Rights in Iran*, January 9, 2018, <https://www.iranhumanrights.org/2018/01/ir2017-speed-and-bandwidth/>.
[48] Nathan Hodge and Mary Ilyushina, "Putin signs law to create an independent Russian internet," *CNN*, May 1, 2019, <https://edition.cnn.com/2019/05/01/europe/vladimir-putin-russian-independent-internet-intl/index.html>.
[49] Kayleigh Long, "The war for truth in Myanmar's cyberspace," *Coda Story*, June 4, 2019, <https://codastory.com/authoritarian-tech/myanmar-facebook-conflict-rakhine/>.
[50] Gabrielle Lim, Etienne Maynier, John Scott-Railton, Alberto Fittarelli, Ned Moran, and Ron Deibert, "Burned After Reading: Endless Mayfly's Ephemeral Disinformation Campaign," *The Citizen Lab*, May 14, 2019, <https://citizenlab.ca/2019/05/burned-after-reading-endless-mayflys-ephemeral-disinformation-campaign/>.
[51] Paul Huang, "Chinese Cyber-Operatives Boosted Taiwan's Insurgent Candidate," *Foreign Policy*, June 26, 2019, <https://foreignpolicy.com/2019/06/26/chinese-cyber-operatives-boosted-taiwans-insurgent-candidate/>; Marie C. Baca and Tony Romm, "Twitter and Facebook take first actions against China for using fake accounts to sow discord in Hong Kong," *The Washington Post*, August 19, 2019, <https://beta.washingtonpost.com/technology/2019/08/19/twitter-suspends-accounts-it-accuses-china-coordinating-against-hong-kong-protesters/>.

user data in-country but also remove content at the government's request.[52] Similarly, the Turkish government gave the country's Radio and Television Supreme Council control over all online content, including news outlets and streaming services.[53] In Russia, measures were established so that those who show "blatant disrespect" for the government online can now face fines or jail time.[54] Thailand also passed a cybersecurity law granting sweeping and ill-defined powers to monitor internet traffic, access user data, and seize devices.[55] And in China, Google banned ads for VPNs targeting users in China.[56] Together, these collective actions pose an existential and immediate threat to internet freedom writ large.

[52] Euan McKirdy, "'Stalinist' Vietnamese cybersecurity law takes effect, worry rights groups and online campaigners," *CNN*, January 2, 2019, <https://www.cnn.com/2019/01/02/asia/vietnam-cybersecurity-bill-intl/index.html>.
[53] Ece Toksabay and Tuvan Gumrukcu, "Turkey moves to oversee all online content, raises concerns over censorship," *Reuters*, August 1, 2019, <https://www.reuters.com/article/us-turkey-internet-censorship/turkey-moves-to-oversee-all-online-content-raises-concerns-over-censorship-idUSKCN1UR539>.
[54] Tom Balmforth, "Russia's Putin signs law banning fake news, insulting the state online," *Reuters*, March 18, 2019, <https://www.reuters.com/article/us-russia-politics-fakenews/russias-putin-signs-law-banning-fake-news-insulting-the-state-online-idUSKCN1QZ1TZ>.
[55] Patpicha Tanakasempipat, "Thailand passes internet security law decried as 'cyber martial law,'" *Reuters*, February 28, 2019, <https://www.reuters.com/article/us-thailand-cyber/thailand-passes-internet-security-law-decried-as-cyber-martial-law-idUSKCN1QH1OB?il=0>.
[56] Catalin Cimpanu, "Google bans VPN ads in China," *ZDNet*, March 20, 2019, <https://www.zdnet.com/article/google-bans-vpn-ads-in-china/>.

Project Highlights

During the period covered by FY2018 funding, OTF funded over **32 innovative projects** to combat censorship and repressive surveillance, **18 fellowships** to support cutting-edge research and digital security interventions, **6 labs** to improve the security, usability, resiliency and interoperability of key Internet freedom technologies, and **22 rapid response interventions** to address digital emergencies.

A full list of all supported projects is included at the end of this report. This section provides an overview of key project highlights.

Supporting Innovative Technologies

- **Advanced Circumvention Technology**: Virtual Private Networks (VPNs) have become one of the most popular methods for circumventing government-imposed censorship and, as a result, have become the target of repressive governments. Unfortunately, many popular, proprietary VPNs rely on underlying protocols that have numerous, widely known vulnerabilities, massive codebases, and significant performance issues. In order to meet the demand for more secure, resilient, easy-to-use VPNs, OTF has invested in better documenting the vulnerabilities in widely used VPN protocols and the privacy practices of commercial VPNs and has supported several emerging circumvention solutions to address these issues, such as Wireguard and MassBrowser. Wireguard, a new VPN protocol, features a lightweight codebase, extensive security review, and integration of many important security features lacking in previous VPN protocols such as a "fail-closed" feature, which forces a more secure connection by default. MassBrowser is a novel peer-to-peer system that allows volunteers in “uncensored” locations to help users in censored contexts access the Internet. This joins a number of emerging peer-to-peer circumvention approaches OTF is funding that could constitute a new generation of blocking resistant content delivery methods.

- **Secure Document Sharing and Storage**: As part of their daily operations, journalists, media networks, and human rights organizations frequently collect, store, and share sensitive information. This information often contains multiple layers of sensitivity and requires varying forms of protection from governments that seek to surveil and censor their citizens. In order to address this threat and to protect information at rest and shared within an organization, OTF has supported the development of several open source, secure file storage and file-sharing system designed for journalists and human rights organizations, including Globaleaks, Tahoe-LAFS, OpenArchive, and OpenAppStack.

- **More Secure Messaging**: The use of secure messaging platforms has skyrocketed over the last several years, with over 2 billion users worldwide. While many secure messaging platforms include important security features, such as end-to-end encryption, many still put users at risk by relying on and exposing users' phone numbers. This has become a growing threat to journalists, human rights defenders, and civil society organizations working in repressive environments, whose communication networks are frequently surveilled. In response, OTF has supported the development of Delta Chat, a new messaging application that provides enhanced user privacy and security with end-to-end encryption without requiring a phone number or a central server. These features create a resilience to surveillance that is vital for users in repressive contexts.

- **Encrypted SNI**: Blocking websites through the unencrypted SNI field is an increasingly pervasive censorship tactic. This method of censorship is being used extensively in China as well as in Venezuela, which OTF-supported researchers discovered last year. Simply encrypting the SNI field would prevent censors from using this form of blocking. However, in order to encrypt SNI, browsers and website hosting providers must adopt this approach, which many have not because of a lack of standardization and difficulties related to implementation. Over the last year, OTF has supported a central actor in the IETF working group to finalize the encrypted SNI standard and create the template code to minimize any challenges associated with implementation. This will dramatically increase adoption of encrypted SNI and remove a primary blocking strategy employed by censorship regimes.

- **Mobile Surveillance Detection**: An international mobile subscriber identity-catcher (IMSI-catcher) is a surveillance device used to intercept mobile phone traffic and track mobile phone users. Over the last several years, repressive regimes have increasingly deployed IMSI-catchers during political protests to identify, track, and intercept the communications of protestors, journalists, and opposition groups in order to target, censor, and/or arrest them. In order to protect citizens from this repressive surveillance, OTF has supported the development of tools to detect the use of IMSI-catchers based on research conducted by the University of Washington and has piloted this technology in three Latin American cities.

Combatting Internet Shutdowns

Over the last year, governments around the world have shut down the Internet over 200 times. In order to ensure that citizens can continue to access and share digital content in the face of Internet shutdowns, OTF has invested in unique peer-to-peer technologies that enable content-sharing and communication without an Internet or cellular connection, including:

- Briar, an open- source, decentralized, encrypted messaging system that is designed for journalists, human rights defenders, and anyone who needs a safe and easy way to communicate when Internet connectivity is uncertain.
- Ouinet, a free, open source technology that allows web content to be served with the help of an entire network of cooperating nodes using peer-to-peer routing and distributed caching of responses.
- NewNode, a software development kit for content delivery through secure peer-to-peer distribution that works even if access to the source of the material is blocked.
- Qaul.net, a communication tool created by and for people in repressive internet environments designed to make information exchange possible by creating a decentralized peer-to-peer local communication network capable of operating in inconsistent connectivity situations.
- Ayanda, an open source library that offers tools for offline network communication based on sending data through BlueTooth, WiFi, and ultrasonic-sound technology.

Timely, Accurate Censorship Detection

Growing levels of Internet censorship have heightened the need for robust censorship detection and analysis tools. Without knowledge of what is being blocked where, and the underlying technical means through which something is blocked, it is very difficult for circumvention tool developers to understand their adversaries' capabilities and to create effective tools to respond. Recognizing this, OTF has invested in the development and implementation of leading censorship detection tools, including the Open Observatory of Network Interference (OONI) and the Internet Outage Detection and Analysis (IODA) project. OONI is an open-source networking testing framework and testing network for detecting network interference including outright censorship. IODA is a system that monitors the Internet in near-real time to identify macroscopic Internet outages affecting the edge of the network. Collectively, these projects measure and document Internet censorship nearly every minute in more than 210 countries.

Exposing Repressive PRC Surveillance

OTF has also played a key role in investigating and exposing PRC-affiliated apps used for repressive surveillance, including tools used by the government to target religious minority Uyghur Muslims in Xinjiang province as well as the widely used PRC-affiliated app, Study the Great Nation. In addition to exposing the increasingly sophisticated tactics that the Chinese government is using to surveil and control their own citizens, this research has also helped to shine a light on the types of technologies and tactics that the Chinese government is exporting to like-minded regimes around the world.

OTF conducted an audit of the "BXAQ" app that is used by Chinese police in the Xinjiang province to scan tourists' mobile phones. The audit found that the app not only scans phones but also captures users' data and sends that information insecurely to a local file server for analysis. In conjunction with Human Rights Watch, OTF also supported technical

researchers to analyze a data collection and analysis system, called the Integrated Joint Operations Platform (IJOP), that is used by police in the Xinjiang region to track residents. Researchers found that the system tracks the location data of phones, ID cards, and vehicles as well as the use of electricity and gas stations by all residents in the region. When the IJOP system detects irregularities or deviations from the norm, the system flags these abnormalities to authorities as suspicious, which prompts an investigation. In addition, OTF supported research on the mobile application, known as Jingwang, that all residents of Xinjiang have been forced to install on their mobile phones. Researchers found that the app collects personally identifiable information, scans the device for "dangerous" files, and sends a list of all files to an unknown entity for monitoring. Research supported by OTF also tracked the export of Chinese censorship and surveillance technologies and tactics to 102 countries around the world.

Responding to Digital Emergencies Around the World

Over the last year, OTF supported rapid response interventions across the globe to help journalists and human rights defenders respond to digital attacks and other forms of online censorship, including in places such as Venezuela, Hong Kong, Iran, Egypt, Gambia, DRC, Tibet, Thailand, Bahrain, Sudan, Ethiopia, Pakistan, Vietnam and Azerbaijan.

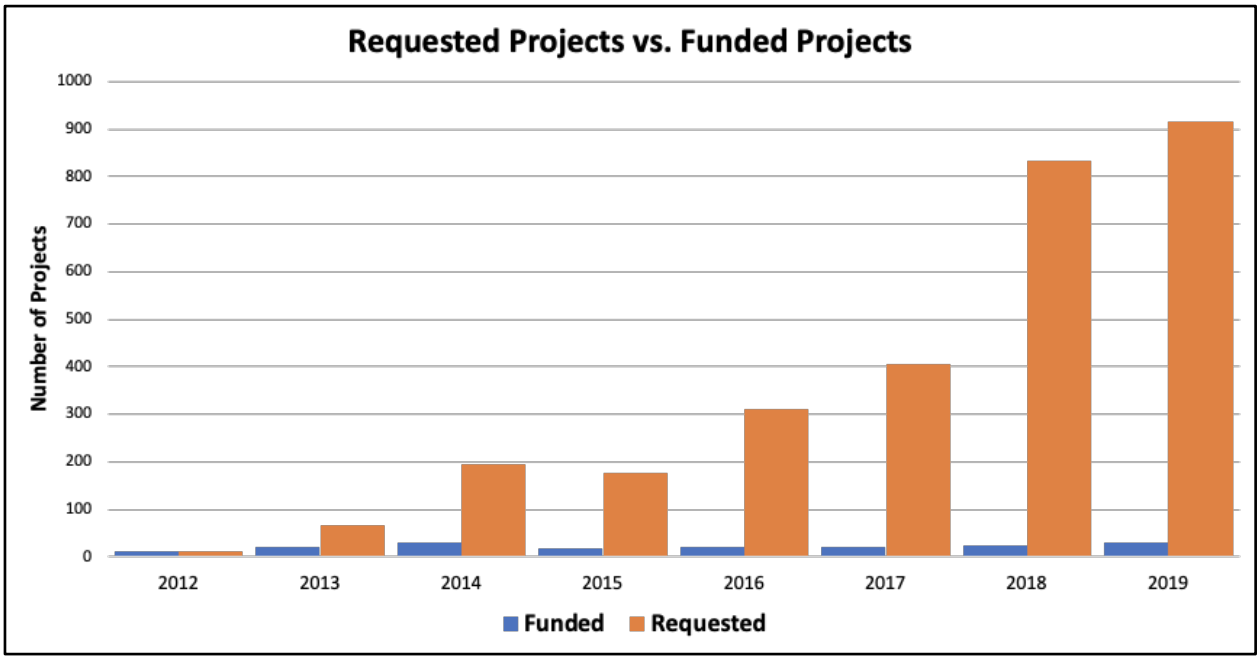
- **Venezuela**: After Venezuela's contested 2018 presidential election, the Maduro regime drastically ramped up its Internet censorship and online attacks against journalists and activists. These attacks escalated further in 2019 with authorities regularly implementing "just-in-time" censorship tactics to block media content and popular social platforms. In response to this worsening censorship environment, OTF quickly activated its networks to detect and monitor new censorship events, provide rapid response digital security assistance to journalists and activists on the ground, and deploy anti-censorship and secure communication tools for tens of thousands of citizens. OTF also provided rapid response assistance to a leading Venezuelan human rights organization and a network of Venezuelan journalists that were the targets of government-sponsored hacking attempts. These combined efforts ensured that activists and journalists were able to continue safely communicating and reporting on the situation.

- **Hong Kong**: In late 2019, protests erupted in Hong Kong in opposition to a proposed extradition law that would essentially subject its citizens to the Chinese legal system. Shortly after the protests began, Hong Kong-based journalists and human rights organizations reached out to OTF for digital security support and assistance. In response, OTF supported the creation of a tailored Chinese/English digital security guide for journalists and protesters, quickly deployed anti-censorship and secure communications tools to over 100,000 citizens, and supported the integration of OTF-incubated New Node into the popular Telegram app to improve the security and resiliency of communications.

Increasing Need

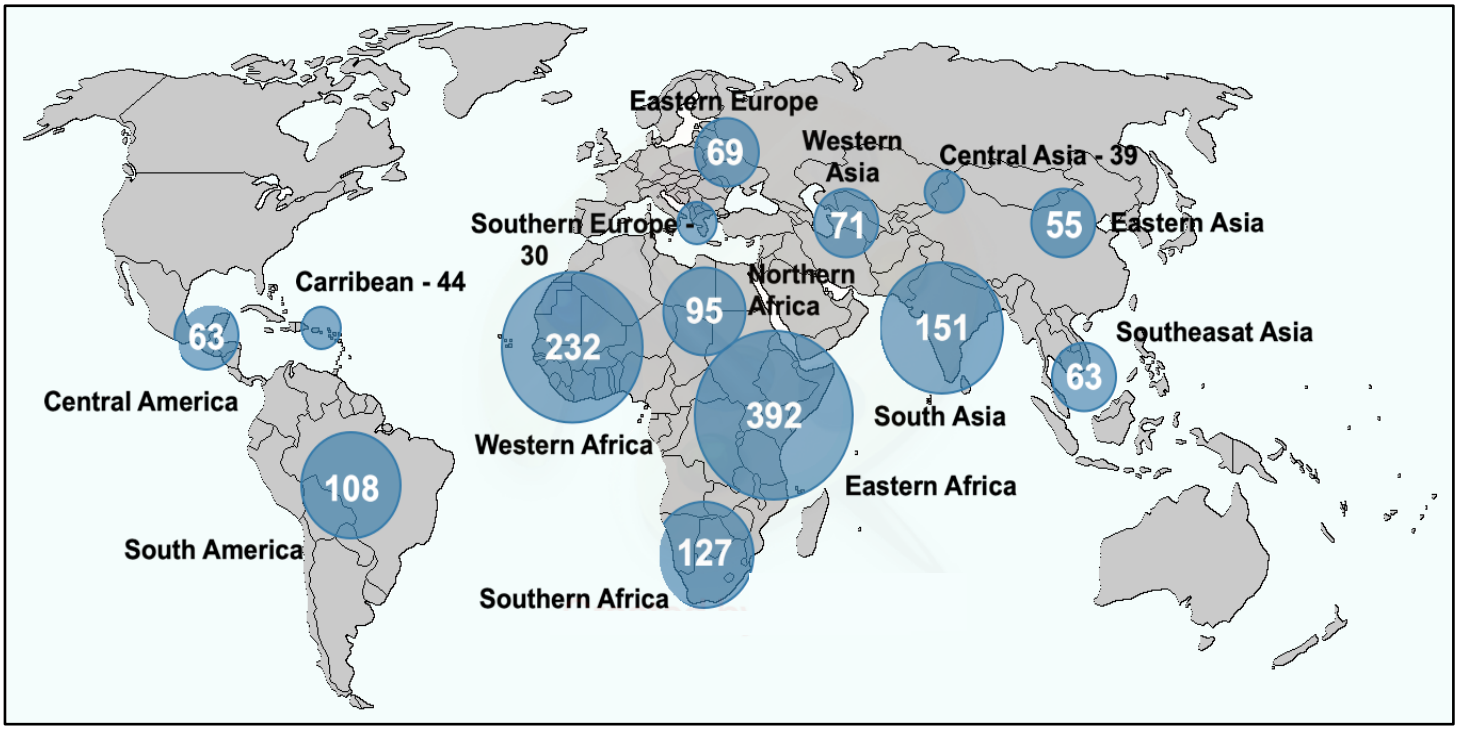
During the period covered by FY2018 funding, OTF received over 1,500 concept notes through the Internet Freedom and Core Infrastructure Funds, in addition to hundreds of Fellowship, Lab, and Rapid Response requests. This is the most applications for funding that OTF has ever received and is clear evidence of the growing need for OTF's services.

As a result of this increasing demand for support, OTF's funding continues to become more competitive. As the chart below demonstrates, the percentage of funded projects to applications received continues to decline as applications grow. In calendar year 2019, for instance, OTF was able to fund just 3% of applications submitted to the Internet Freedom and Core Infrastructure Funds.



As demonstrated in the maps below, OTF received increased concept note submissions from throughout the Global South in 2018 and 2019. These applications are a reflection, in part, of the concerted effort made by OTF to foster relationships with internet freedom communities designing solutions on the frontlines of censorship and surveillance, as well as increasing threats to internet freedom in these regions.

Concept Note Submissions by Region in Calendar Year 2018 and 2019



Looking to the Future

In September 2019, OTF was incorporated as an independent organization and became a new USAGM grantee solely focused on internet freedom for citizens in repressive environments around the world. This new structure will enable OTF to take USAGM's internet freedom efforts to the next level by creating the flexibility, speed, and oversight needed to empower innovation and compete against far more aggressive and well-resourced adversaries to a free and open internet. As an independent entity, OTF will be able to increase long-term support for core internet freedom tools while expanding funding for innovative, next generation solutions to stay ahead of evolving censorship threats. With a growing percentage of USAGM's audiences relying on the internet to access news and information, this new approach will ensure USAGM journalists and audiences have the tools they need to safely report on sensitive issues and retain access to otherwise censored content.

Historically, OTF has supported the research, development, and implementation of cutting-edge internet freedom technologies. As a newly independent organization, however, OTF's mission will expand to support an even broader range of technologies in order to respond to increasingly aggressive and sophisticated censorship and surveillance threats, and to provide more comprehensive and tailored support to USAGM networks. OTF will continue to work to advance internet freedom around the world by supporting the research, development, and implementation of innovative internet freedom technologies. But the organization will now also support the long-term maintenance and advancement of core internet freedom tools. Doing so will enable OTF to provide tailored support throughout the entire technology development lifecycle: from proof-of-concept, to on-the-ground deployments, to multi-year efforts. The longer timelines of this new approach will enable OTF to better support technology development at both speed and scale.

In addition, OTF will provide direct internet freedom assistance to USAGM's news networks to help improve the digital security of USAGM entities and journalists. These efforts will include making USAGM websites and applications more secure and resistant to censorship, providing customized and secure tip lines for sources, and deploying leading internet freedom technologies to ensure that audiences can access USAGM content even in the face of increased censorship.

Independence and increased funding will also allow OTF to begin to more substantively fight the internet freedom battles of tomorrow. The technologies funded by OTF over the last year played a critical role in advancing the state of anti-censorship and secure communication technologies around the globe. Despite this, threats to internet freedom continue to grow at an exponential rate as repressive regimes work to deploy increasingly bold and sophisticated censorship and surveillance tactics and technology.

Indeed, over the past year, regimes started to deploy artificial intelligence and machine learning to enable faster, more targeted, and more aggressive online censorship and surveillance. These

new technologies significantly decrease the overall cost of mass censorship and surveillance, making such tactics and techniques more accessible to repressive regimes around the world. In addition, many repressive regimes have also begun to deploy new and nefarious technologies to create and propagate disinformation. By combining advanced censorship and surveillance technology with disinformation tactics, repressive regimes are now able to control and manipulate the online information landscape in a way they never have before. Existing internet freedom solutions will need to evolve quickly to meet these challenges and to proactively engage innovations before they become active threats. Thanks to its new structure, OTF is ready to lead the way.

Direct Support with FY2018 Funds

OTF provides critical funding and service offerings to projects and individuals pursuant to its core mission of increasing unrestricted, secure access to the internet for those living in repressive societies. While OTF strives to innovate better tailored and more impactful funding processes, OTF is ultimately defined by the projects, fellows, and Labs its funding and service offerings help make possible. The various efforts supported by OTF's FY2018 allocation are detailed below, organized by fund, fellowship program, and Lab.

Funds

Internet Freedom Fund

The Internet Freedom Fund (IFF) is the primary mechanism through which OTF provides funding for innovative global internet freedom projects. IFF projects are primarily focused on technology development and implementation, but also include applied research and digital security projects. OTF continuously solicits IFF project proposals via an open and transparent process. Submissions are reviewed every two months.

WireGuard

$250,000

The WireGuard project helps address critical issues related to Virtual Private Network (VPN) security. VPNs are used around the world as both an internet access and privacy tool, enabling the circumvention of state-imposed blocks and helping individuals protect their personal information online. Unfortunately, most VPNs rely on underlying protocols that have numerous, widely known vulnerabilities which are increasingly being exploited by repressive governments attempting to prevent users from overcoming censorship. WireGuard's underlying encryption, which is used to help combat these repressive efforts, relies on the OTF-supported noise encryption protocol. Although WireGuard's protocol is relatively new, it has been adopted by numerous commercial VPNs (such as Mullvad, AzireVPN, and StrongVPN) and integrated into the Linux kernel. OTF's support helped advance WireGuard's efforts to strengthen VPNs by advancing kernel development, improving project code maintenance and bug tracking, and developing client software for users. The project was also able to conduct further research into improving the overall protocol and engage in efforts to raise WireGuard awareness and adoption.

MassBrowser

$91,660

Developed by the Secure, Private Internet (SPIN) Research Group at the University of Massachusetts Amherst, MassBrowser is a free and open source tool designed to circumvent

internet censorship through a novel, peer-to-peer system that allows volunteers in “uncensored” locales to help users in censored contexts. OTF’s support aided in the development of a final release desktop version of MassBrowser, as well as an Android version. The project also helped advance a performance measurement framework, usability improvements, and adoption by third-party systems.

Certbot

$185,000

Certbot is a tool built by the Electronic Frontier Foundation (EFF) to help expand internet encryption by installing Let’s Encrypt SSL/TLS certificates for free. Making it easy for website administrators to deploy the use of HTTPS encryption on their sites increases security for users and makes it harder for repressive governments to censor individual websites. Building better tools for HTTPS deployment is therefore a critical security and anti-censorship task to assist vulnerable communities around the world. OTF support for Certbot focused on expanding Certbot to support Windows-based servers and building a better distribution system. The project built on prior OTF funding by enabling more users to take advantage of the security enhancements offered by Certbot. Thanks in part to efforts like Certbot, Let’s Encrypt recently issued its billionth certificate.

Deltachat

$299,850

Delta Chat is a new messaging app that functions like any intuitive text messaging tool but is built with an email backend, enabling enhanced user privacy and security with end-to-end encryption. Delta Chat is unique in that it does not require a phone number, has no central server, and leverages existing infrastructure used by email to do so. These features create a resilience to surveillance that is vital for users in repressive contexts. OTF support focused on maturing Delta Chat's development, building cross-platform and multi-device support, and conducting user research in order to improve usability features.

Tahoe-LAFS

$200,000

Human rights and media organizations need to protect multiple levels of sensitive digital information, including information stored on worker devices, information in transit between communicating parties, and information on organizational infrastructures. The Tahoe-LAFS project helps organizations in repressive contexts protect this critical information by better utilizing Least Authority’s open source, secure options for file storage, sharing, and management. The project addresses threats to information at rest and shared within an organization by deploying secure file storage and sharing capabilities. It also makes it easier for other organizations to manage deployments on their own. At the end of Phase 1, Tahoe-LAFS partnered with four organizations to determine their storage and sharing needs. In Phase 2, the project will focus on addressing identified needs such as version control, sharing workflow, and

related user-interface improvements within Gridsync to improve file sharing.

Trust Through Trickery

$39,000

The design of secure messaging apps needs to be studied closely because journalists and activists risk their safety on a daily basis when they use these apps to communicate with their networks. This project analyzed how private and secure a user's data and profiles are in reality versus how private their profiles appear to be from the user perspective as a result of certain design and UX features. This project also analyzed if the design of these messaging apps and platforms helps facilitate or create these feelings of trust and privacy. This project created recommendations and research on different platforms while analyzing if there are new design patterns of trust that trick users or provide a false sense of security.

Open Observatory of Networking Interference (OONI)

$300,000

OONIThe Open Observatory of Networking Interference (OONI) is the leading open source network testing framework used around the world to help detect internet censorship by continuously collecting data from thousands of networks. OTF's support of OONI allowed for the creation of standalone desktop applications for Windows and MacOS as well as a command line interface. The project was also able to overhaul the measurement engine, improve testing to increase resiliency during network outages, add additional tests, and create a glossary and FAQ. Other improvements included decreased measurement times, an RSS feed of potential blocking events, and reports on censorship events in Zimbabwe, Gabon, Cuba, Benin, China, Nigeria, Jordan, Ethiopia, Egypt and Venezuela. OONI-probe, an associated test for detecting internet censorship, is regularly used hundreds of thousands of times per month to capture measurements from more than 200 countries worldwide.

Internet Outage Detection and Analysis (IODA)

$199,913

IODA is an operational prototype system that monitors the internet in near real-time to identify macroscopic outages affecting the edge of the network. This is accomplished by combining measurements at the control plane, active probing, and passive traffic analysis. Support from OTF improved IODA methods and accuracy in detecting outages, and also allowed for the creation of new user features, public reports about internet outages in Gabon and Benin, and increased engagement with advocates and researchers.

App Store Censorship

$72,000

The App Store Censorship project helps track Apple iOS applications for instances of censorship in over 150 countries, and documents when and how apps are removed in order to provide increased transparency. This project allows researchers to better identify censorship by Apple and track whether apps are being blocked locally at the government's request (which could provide an indication of local censorship) or globally. It also enables advocates who know their local context to connect when censorship occurs due to civil society actions and political events. The project has already helped to identify censorship of apps related to religious freedom in China, the Tibetan diaspora, and protests in Hong Kong. The data and information generated by this project are being made accessible to policymakers, journalists, advocates, and everyday citizens on the applecensorship.com website.

Ouinet

$251,010

Ouinet enables users to circumvent censorship and reduce the impact of network shutdowns by utilizing peer-to-peer networking and distributed storage to cache the types of online content that are often requested inside censored regions. Ouinet is the open source library that powers the Censorship.no (CENO) project, which enables users to access the web and avoid network censorship. The Ouinet library is designed as a core technology that supports multiple transports and storage protocols, opening up possibilities for cooperation with projects like Tor, IPFS, and NewNode. OTF support focuses on improving the scalability and reliability of Ouinet's existing technical components, further enabling the technology to be integrated into existing circumvention tool networks. Ultimately, Ouinet adds an important building block to the existing ecosystem of censorship circumvention tools by helping users access or distribute content that would otherwise be unavailable due to network interference.

Qaul.net

$248,567

Qaul.net is a communication tool created by and for people in repressive internet environments designed to make information exchange possible by creating a decentralized peer-to-peer local communication network capable of operating in inconsistent connectivity situations. OTF support focused on building qaul.net version 2.0, complete with updated technologies that allow for new interconnection possibilities, including making it possible for user devices to directly connect and communicate with one another.

Ayanda

$86,950

The Ayanda project is developing an open source library that offers tools for offline network communication based on sending data through BlueTooth, WiFi, and ultrasonic-sound

technology. During times of large-scale civic engagement and issues of national significance, numerous autocratic regimes throughout Africa have limited their citizens' ability to freely express themselves online, and at times have completely shut off the internet. Ayanda's open source solution to these issues is localized for the types of low-end devices and low-resource environments that are found throughout the global south, and in sub-Saharan Africa in particular. Ayanda's proposed ultrasonic-sound technology will simplify the process of pairing devices and lead to better cross-device compatibility. In addition, the project also intends to make the open source library more user-friendly for projects that require the use of offline communication solutions.

Onions on Apples

$174,657

This project improves the usability and functionality of the Tor Browser's Onion Browser app for Apple iOS and its underlying framework. The Tor Browser provides a critical safety tool for those targeted by repressive government actors. Because of the singular benefits of Tor technologies, the network and browser are used by more than 1.5 million people each day around the world including journalists, activists, political dissidents, human rights workers, whistleblowers, companies, and privacy-sensitive individuals in some of the world's most heavily surveilled contexts. The Onion Browser app, however, has received far less attention and support than Tor's Android and desktop platforms. Onions for Apples therefore addresses existing shortcomings by improving user experience on the app as well as the Tor connection experience. The project is also working to create currency with Core Tor Improvement, implement a new File Download Feature, and lead an Onion Browser Awareness & Community Support campaign.

Tibetan Computer Emergency Readiness Team (TibCERT)

$244,050

The Tibetan Computer Emergency Readiness Team (TibCERT) project seeks to create a formal, coalition-based structure for reducing and mitigating online threats in the Tibetan community. The project also seeks to ensure greater online freedom and security for all of Tibetan society by expanding Tibetans' technical research capacity on threats in the diaspora, as well as surveillance and censorship inside Tibet's borders. Currently, diaspora-based Tibetans are aggressively targeted with malware as a community, and therefore need to share, analyze, and develop real-time responses to threats. Unfortunately, however, no formal collaboration currently exists. Likewise, even though Tibetans in Tibet face constant censorship and surveillance because of their identity, very few tailored mitigation solutions exist, and there is no formal structure for researchers to engage with Tibetans in analyzing the particular risks they face and potential solutions. TibCERT addresses these unique needs and issues, and is working to build long-term capacity for Tibetans to help secure their communal digital space in the face of dire security threats.

Zanga

$95,000

Zanga is an Arabic-language third-party app store facilitating access to circumvention, privacy, and digital security tools. The store prioritizes open-source tools and those that are tried and trusted by the digital rights and civic tech communities. Zanga combats censorship occurring at the app store level by offering a trustworthy app-exchange medium outside of the Google Play Store or Apple App Store. The project's goal is to bridge the gap between tool developers and end-users in the Middle East and North Africa in order to improve the responsiveness of tools to growing global needs (a necessary development in the absence of resources for dedicated user-support targeted for each language or region/country).

RAWRR - Risk Assessment Workflow for Recommendation Roadmaps

$149,102

The RAWRR project aims to develop a standardized organizational security intervention workflow and accompanying software tool for conducting digital audits and assessments. A unified workflow and single tool where users can record findings in a structured way will help eliminate inconsistencies and strengthen overall report generation and roadmap development. The software tool being developed by RAWRR will simplify data gathering, report generation, and roadmap development for audits and assessments. It will also help reveal risks and priorities, and measure and evaluate the effect of utilizing different security measures. The project additionally includes usability testing and security evaluation for at-risk organizations, which will help increase organizational security and test RAWRR implementation.

InfoSec for the Balkans

$41,096

This project, conducted by Open Data Kosovo, works to improve digital security for investigative journalists and civil society organizations (CSOs)in southeast Europe. CSOs and those involved in investigative journalism in the region face constant information controls, cyber attacks, and surveillance from local authorities. To help address these issues, Open Data Kosovo conducted information security auditing and counseling for six CSOs in Kosovo, Albania, Serbia, Macedonia (Metamorphosis), Bosnia and Herzegovina, and Montenegro. After completing penetration testing for each organization, the project team visited the organizations to discuss vulnerability findings and potential steps to increase security. Country reports were delivered to each organization to set out recommendations and findings. The project also released the InfoSec Manual for Journalists and Civil Society, a guide that focuses on teaching basic digital security skills and practices for actors in the region. The guide is available in Albanin, Bosnian, Macedonian, Montenegrin, Serbian, and English.

Digital Security Support in Pakistan

$62,969

Digital spaces are increasingly coming under attack in Pakistan, with enforced disappearances, cyber harassment, and stringent free speech regulation. Many activists and journalists in the country have been targeted specifically on the basis of their speech in online spaces. This project allows the Digital Rights Foundation to expand its cyber harassment helpline in order to enhance the organization's digital security capacity and provide support to human rights defenders and activists online. Hours and personnel at the helpline need to be increased given the significant demand for services (1,476 calls in the first year alone). A dedicated digital security expert will be created for the hotline because a significant portion of callers face problems concerning hacked devices and accounts. Digital experts will also dispense advice on how to guard against fake profiles, blackmailing, and information leaks, while providing in-person training to human rights defenders as needed.

Strengthening Digital Security for Journalists and HRDs in Mexico

$50,000

Journalists and human rights defenders in Mexico must overcome violence, heavy workloads, and low economic resources in order to defend at-risk communities and individuals. This project is working with four organizations operating within this context to help ensure they have sufficient capacity to protect themselves from digital risks like loss and theft of information, unauthorized communication intervention, lack of digital security protocols, and website failure. In doing so, the project is diagnosing each organization's current threats, creating IT policies, providing digital security training and technical support, and supplying feedback to security tool developers countering similar threats in other contexts.

Digital Security Skill Building for Grassroots NGOs in Chiapas

$61,497

This project is working to develop an improved methodology for digital security training and support with grassroots organizations in Chiapas, Mexico. These efforts accompany security training workshops delivered to six grassroots organizations in the region. Through the project, the organizations receive digital security guides tailored to their organizational needs and threat models, a methodology for long-term digital security support, and provide feedback to digital security tool developers.

Security Support for Sexual Minorities in Nigeria

$120,000

This project provides security trainings to a network of highly-targeted LGBTQI organizations in Nigeria, helping them to build capacity for human rights defenders to protect members of these at-risk communities from digital harm. The project also increases capacity within the

organizations to maintain and multiply knowledge of organizational safety and document success and failures (so this information can be used by other trainers in the infosec community). Feedback from the experience of these targeted groups is provided to the developers of open source security tools in order to help them stay ahead of emerging surveillance tactics in repressive contexts.

Security Training and Support for LGBTIQ Communities and Allies in Indonesia

$145,190

This project conducts a series of holistic digital security training for several LGBTIQ organizations and their allies in Indonesia. LGBTIQ organizations in the country have faced increasing scrutiny and threats over their work, resulting in attacks both online and offline. This project addresses these issues by providing various levels of digital security training, as well as mentoring and technical guidance to help build crisis management systems and better organizational security policies. These efforts seek to ensure a more sustainable practice of security at both personal and organizational levels, while also creating an example that can be leveraged by other at-risk communities around the world.

Claims and Meme Database (CMDb)

$144,850

The Claims and Memes Database (CMDb) is a programmer-accessible repository of fact-checked claims and debunked visual misinformation from repressive countries where disinformation and social network manipulation have become key censorship strategies. The creation of this repository improves awareness of these practices and helps to counter them. The overarching goal of the project is to preserve citizen access to credible information, arm journalists with greater awareness of disinformation patterns and limit the impact of viral disinformation within affected communities. OTF support helped improve CMDb's technical infrastructure and allowed for the collection of more than 1,000 non-English claims and memes in the database. The CMDb team also helped form an Images and Memes working group (chaired by the International Center for Journalists) and, as part of the W3C Credible Web Community Group, supported the development of a list of indicators of credibility for different types of content. The team presented their findings and research at a number of activist and academic international conferences.

Improving Test Lists of Censored Online Content

$80,572

This project works with researchers around the globe to update Citizen Lab's test lists, which are used by leading network measurement tools to uncover instances of website blocking. These updates are necessary because although network probes have greatly evolved over the years, test lists for certain countries and regions remain out-of-date and negatively affect the quality of collected measurements. To address this problem, Netalitica's team of country specialists (in collaboration with other stakeholders and grassroots organizations) are updating

old test lists with fresh URLs, removing faulty entries, and developing recommendations for streamlining the list revision process.

Measuring and countering slowdown as a censorship mechanism

$150,000

This project works to systematically measure and document slowdown/throttling, a technique research shows is utilized by repressive regimes to attack encrypted connections currently being used effectively to circumvent censorship. The project also plans to build a prototype open source tool that can be used to counteract throttling, and then investigate ways the tool can be integrated within existing anti-censorship solutions.

Ukraine Censorship Monitoring

$119,980

The Ukraine Censorship Monitoring project utilizes the Open Observatory of Network Interference to document the systematic blocking of websites in Ukraine and reveal the extent to which such censorship is occurring. This work is carried out by establishing a sustainable system of censorship monitoring and measuring within all parts of Ukraine (including the occupied Crimea and Donbas regions through use of local monitors). Additionally, the project's testing methodology can be used as a blueprint for monitoring in other censored environments.

Core Infrastructure Fund

In order for internet freedom tools to be effective and secure, the basic foundations upon which they are built must also be functional and secure. Beginning in 2015, OTF recognized that a number of core infrastructure technologies routinely relied upon by internet freedom tools were victims of neglect, kept running only thanks to the efforts of volunteers in their spare time. In the context of this wholly unsustainable situation, the Core Infrastructure Fund (CIF) was created to help support the essential "building block" technologies used every day by internet freedom tools. Unlike IFF projects, CIF projects require alternate criteria for evaluation and support, and often directly benefit and are used by developers of end-user tools, rather than end-users themselves. Each year, OTF sees more technologies moving into this realm and receives more applications for their support.

NewNode

$150,000

The NewNode project created a software development kit (SDK) for content delivery through secure peer-to-peer distribution, that works even if access to the source of the material is blocked. The utilization of peer-to-peer technology provides a means to bypass filtering and deep packet inspection technology deployed on national gateways and internet service provider networks. NewNode allows any app incorporating it to provide access to content faster, cheaper, more reliably, and in a censorship-resistant manner . When a publisher uses the SDK,

users in restrictive countries can access the publisher's content without any negative performance impact—even if the publisher is censored in their country—by getting it from a peer. OTF's funding supported the second of two phases for the project, in which NewNode integrated a new peer-to-peer protocol, created a transport encryption layer (to protect the protocol against detection, snooping, and tampering), and formally released the SDK for Android and iOS.

Reproducible Builds

$100,000

The Reproducible Builds project creates independently-verifiable paths from source code to the binary code used by computers, allowing for technically reliable verification that no vulnerabilities or backdoors were introduced during a compilation process for an open source tool. OTF support of this project focused on developing and deploying reproducible installer images (to ensure secure means of performing the first-time installation), enhancing the diffoscope tool (which provides in-depth comparison of files, archives, and directories), and improving the distribution infrastructure (in order to deliver a reproducible operating system).Increased community participation in the Reproducible Builds project was also encouraged by promoting its benefits, tools, and ideals.

Make Tor's Onion Services More Secure and Easier to Use

$499,510

Onion services by the Tor Project are a tool that website administrators can adopt in order to offer an anonymous, metadata-free location for users to visit. An onion service version of a site protects the user as well as the administrator from being exposed. Onion services are already used by many important global publications and projects to allow for people in repressive countries to securely route around censorship (the BBC, ProPublica, New York Times, RFE/RL, Radio Free Asia, DW, and Facebook all have dedicated .onion sites). This project worked to improve onion services for website administrators and enhance user experience. Specifically, on the development side, the project enabled onion services to become more stable, scalable, and resistant to attacks, allowing more organizations to adopt and deploy their own onion services. On the usability side, the project helped make the use of onion services a more seamless experience by improving how users find, interact, and engage with onion service sites.

DEfO (Developing ESNI for OpenSSL)

$94,300

Although significant amounts of traffic metadata is invisible to network intermediaries, the name of a server is completely unencrypted information that can be used for monitoring, censorship, and other kinds of control. Fortunately, the Internet Engineering Task Force TLS working group is working to make Encrypted Server Name Indication (ESNI) part of the TLS standards. The DEfO project helps to ensure ESNI standardization is finalized as soon as possible by

developing resources to prototype specifications, and by providing and maintaining an ESNI implementation for OpenSSL (by far the most commonly used software for providing TLS). As part of DEfO, Tolerant Networks Limited provides client- and server-side support for ESNI in OpenSSL. The team is also working via application prototyping to ensure OpenSSL with ESNI supports censorship circumvention techniques like "domain fronting" without requiring users to violate any Terms of Service or proffer white lies in connection requests.

FORT RPKI Validator

$75,000

Internet routing is one of the most important components of the internet's overall infrastructure, yet it remains largely insecure. Routing systems can be easily hijacked to conduct website blocks, surveill users, and redirect traffic to bogus (and possibly malicious) destinations. In response, internet standards bodies have started developing Resource Public Key Infrastructure (RPKI) as a method to add signatures that can be used to verify the authenticity of routing information. Through the FORT RPKI Validator project, LACNIC and NIC.MX are contributing to RPKI development efforts, conducting a deployment campaign in Latin America and the Caribbean, and documenting routing incidents in the region.

PyPi

$80,000

PyPi is the official software repository for the Python programming language, which is used by many internet freedom projects including Tor, OONI, and WireGuard. These tools and many others rely upon the third-party packages hosted on PyPi, and as a result, it is a high value target for bad actors who want to inject malware into popular applications that run on Python. With OTF support, PyPi implemented security-enhancing mechanisms for users and expanded availability into new languages through localization efforts.

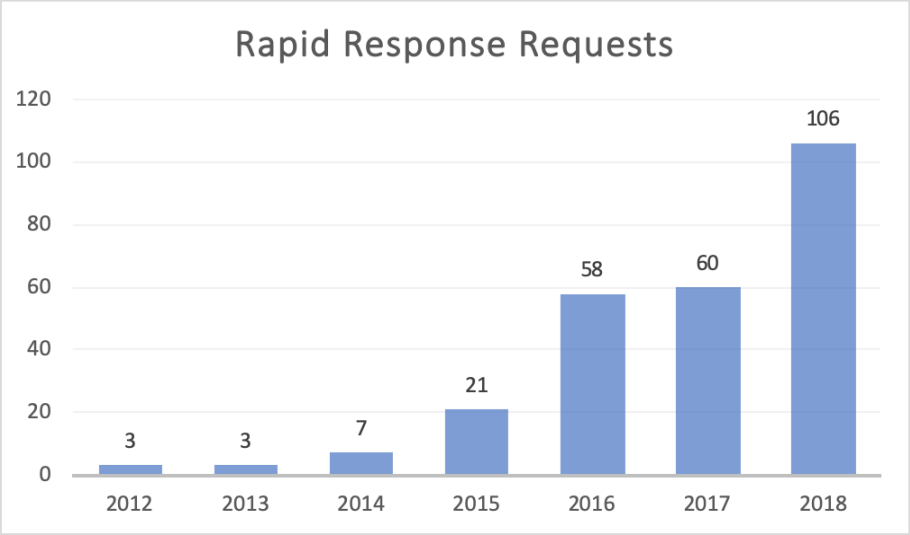
Community Prototype Fund

In 2019, OTF launched the Community Prototype Fund (CPF), a new fund which aims to support the rapid development of innovative internet freedom technology prototypes that serve the immediate needs of the human rights and internet freedom communities. The CPF supports technologists and activists by helping to bring to life ideas that advance inclusive and safe access to global communications networks, counteract censorship and surveillance, and mitigate digital security threats for people in repressive environments. Applicants to the CPF can receive support for up to $6,000 for a project with a maximum timeline of 12 weeks. While the fund became active during the period covered by this report, FY2019 funds will be used to support these projects and will be included in a future report.

Rapid Response Fund

The Rapid Response Fund (RFF) is a broad initiative which facilitates the development of a strong digital emergency response community that can work together to resolve threats to internet freedom in a timely and comprehensive manner. In FY2018, OTF provided emergency support for a variety of digital emergencies experienced by high-risk internet users and organizations, including journalists, bloggers, cyber activists, civil society organizations, and human rights defenders. Through the RFF, OTF offers a permanently open application window to ensure the organization can act quickly when emergencies arise. OTF's rapid response service providers offer assistance with secure and resilient hosting, website audits, forensic analysis of digital attacks, urgent digital security consultations, infrastructure improvements, and VPN services.

The majority of support provided through these partners is in small increments, generally less than $5000 per engagement. This allows OTF to provide direct support to numerous projects while staying below the RFF's $50,000 per project limit. RFF support has been utilized by entities around the globe, including those focused or residing in Azerbaijan, Burma, Egypt, Iran, Iraq, Jordan, Lebanon, Serbia, Syria, Uganda, and Zimbabwe. In calendar year 2018, OTF received 106 requests for rapid response support, and ultimately provided funding for 22 engagements. Six engagements that were not brought to the lab through service partners are detailed below. The total amount of requests for funding nearly doubled that of the prior year.



Digital Security Assistance for Ukraine

$18,130

Following the annexation of Crimea, Ukranian civil society organizations committed to free expression faced an escalating set of threats to their digital security while performing work in the region. One particular organization's staff faced extreme safety risks due to this changing environment, and thus urgent digital security assistance was provided to protect against a host of threats including data release from devices with sensitive data, hacked social network accounts and email and intercepted phone conversations.

Syrian Media Emergency Project

$16,020

With support from the RFF, the digital security assistance organization Nothing2Hide provided urgent organizational security assistance to a Syrian independent media organization facing threats from the pro-Assad diaspora. Nothing2Hide provided this urgent assistance by auditing the media organization's new IT infrastructure, creating a secure remote data backup mechanism, and improving security procedures for journalists and other staff.

Emergency Trainings and Amplification of Gendered Practices of Digital Security

$35,000

In the wake of violent attacks against prominent Black feminist free expression activists engaing in online activism, members of these communities in Brazil requested digital security trainings out of concern for their own safety. The rapid response project delivered emergency digital security workshops over a short-term period, while also creating structures to help ensure digital security knowledge is more sustainable and resilient in these communities in the medium/long-term.

Digital Security Audits for Human Rights Defenders in DRC

$19,700

In the Democratic Republic of Congo, internet freedom has been increasingly stifled by the country's national intelligence agency, the Agence Nationale des Renseignements (ANR). To safeguard against anticipated threats that the ANR would monitor and intercept mobile communications during the December 2018 election periods, this project assisted LUCHA, FILIMBI, and other human rights defenders enhance their digital security practices, as well as those of civil society organizations, protests organizers, journalists, and election observers.[57]

Learn and Share

$18,315

This project addressed the dire safety situation of Colombian human rights activists by providing risk-aware digital security training, as well as feedback collection, on four Guardian Project digital security tools to improve and adapt their functionality. These efforts provided the activists under thread with sufficient resources to obtain the necessary protection and security required to continue with their work, document crimes against their rights, and improve their safety protocols.

[57] Due to unforeseen circumstances this project was ended before funding was fully

Indian Rapid Response

$45,000

Following a highly publicized online harassment incident against an Indian organization's staff, which jeopardized their personal safety and resulted in multiple digital attacks against their website and online accounts, this project worked closely with security professionals to secure the organization's devices and create a mitigation plan going forward.

Fellowship Programs

Digital Integrity Fellowship Program

The Digital Integrity Fellowship Program (DIFP) provides fixed monthly stipends to individuals working to address short-term and long-term threats to online freedom of expression around the world. DIFP fellows use their digital security expertise to provide hands-on, comprehensive internal support to organizations and communities most affected by internet freedom violations (such as journalists, human rights defenders, NGOs, activists, and bloggers) . At the same time, fellows also educate the broader internet freedom field about the threats and vulnerabilities they encounter, helping to ensure emerging and existing technologies continue to meet the needs of at-risk communities.

The DIFP welcomed seven new fellows after receiving 22 submissions in the 2018 application round. Fellows receive a $5,000 monthly stipend and a small stipend for equipment and subscription purchases to enhance the security of the organizations they help support. As part of the application process, applicants identify and propose to work with organizations that have experienced threats to their digital security.

Atnafu Brhane

Atnafu worked with a prominent Ethiopian human rights organization to improve their digital security practices in the context of the escalating capacity of the Ethiopian government to carry out successful malware attacks and other sophisticated surveillance measures against human rights activists, journalists, opposition groups, bloggers, the diaspora, and netizens.[58] Although the organization was well-versed in physical security protection measures, they were severely lacking in digital security guidance. To help shore up their digital security practices, Atnafu conducted a thorough and participatory threat model analysis to inform the implementation of a context-appropriate digital security training program for the organization. He also developed an interactive, contextualized, and participatory digital security guideline used by the organization and the broader human rights community in Ethiopia. The guideline is available in English, Amharic, and Afan Oromo.

[58] Bill Marczak, Geoffrey Alexander, Sarah McKune, John Scott-Railton, and Ron Deibert, "Champing at the Cyberbit: Ethiopian Dissidents Targeted with New Commercial Spyware," *The Citizen Lab*, December 6, 2017, <https://citizenlab.ca/2017/12/champing-cyberbit-ethiopian-dissidents-targeted-commercial-spyware/>.

Rima Sghaier

Rima worked to improve the digital security skills of at-risk communities in the Middle East and North Africa (MENA) region. She specifically addressed the failure of many at-risk organizations in the Mashreq and Maghreb region to implement a safe first contact channel with their audience or community. Operating without a safe first contact channel puts all involved at risk, even when digital security training has been provided and individuals are using secure digital tools in their internal team communications. Working with the Hermes Center For Transparency and Digital Human Rights, Rima focused on auditing and improving the first contact and community-building methods of at-risk communities in MENA, including independent journalists/media, bloggers, religious minorities, civil society/political activists, sexual minorities, and human rights NGOs/HRDs.

OTF Fellow Working in South Sudan and Sudan

Women human rights defenders (WHRD) in Sudan and South Sudan face a significant risk of experiencing human rights violations at the hands of the Sudanese government and armed groups (paramilitary groups, NISS, rebel groups). They are also particularly vulnerable to digital security threats due to a general lack of access to knowledge about digital security and how it can be adapted to their specific needs and situation. OTF's fellow for this project engaged with key WHRD from all over South Sudan and Sudan in an effort to analyze their digital security strategies and cooperatively develop a tailored set of tools and strategies to fit their digital security needs and raise awareness of the issue. By helping to design a training based on these tools and strategies, and continuing to train others with these tools, WHRD all over Sudan and South Sudan can benefit and widen their spaces of action and impact while staying safe.

David Choi

David helped assess and identify threats in South Korea's journalism community for those operating in high threat environments. He also provided digital security assistance, consultations, and trainings to mitigate the digital threats facing their important journalism work on the Korean Peninsula.

OTF Fellow Working in Malaysia

OTF's fellow in Malaysia worked with two prominent human rights defender organizations to help build their digital security capacity from within and strengthen their knowledge of digital security and responsiveness to emergency threats. This project specifically focused on helping the host organizations customize and develop their own security policy guidelines, which was made in a shareable template format suitable for further dissemination to other organizations in the country, as well as throughout the Southeast Asia region in general.

Iryna Chulivska

Iryna worked with the investigative journalism team at Bihus.info in Ukraine to help enhance their digital security practices. Faced with frequent hacking attempts, Iryna conducted a deep

digital security audit for the team to identify any technical vulnerabilities. She also provided digital security staff consultations, and developed and implemented a digital security policy to help the team maintain their security practices after the conclusion of her fellowship.

Vivian Zuniga

Vivian worked in four Central American countries (Guatemala, Honduras, Nicaragua, and Costa Rica) to help strengthen knowledge pertaining to secure communications and effective forms of communication and management of sensitive information. Her efforts also focused on digital equality and the narrowing of the digital divide, particularly in the current political situation in the region. She worked with groups of women, indigenous peoples, journalists, and other emerging networks and organizations that previously did not have access to training on secure communications.

Information Controls Fellowship Program

The Information Controls Fellowship Program (ICFP)[59] cultivates research, outputs, and creative collaboration on topics related to repressive internet censorship and surveillance. The program expands collaboration on capacity building as fellowships are hosted at premier organizations and research institutions, including University of Toronto's Citizen Lab, International Computer Science Institute, Data & Society, Hivos, and Oxford Internet Institute. Applicants either propose or are connected with a host organization (an entity engaged in the internet freedom space, including academic institutions and civil society organizations). Fellows receive a $4,200 monthly stipend and a small travel budget that varies based on the length of their fellowship.

The ICFP welcomed eleven fellows after receiving 50 submissions in the 2018 application round.

Valentin Weber

Host organization: Harvard University's Berkman Klein Center for Internet & Society
Duration: Six Months

Valentin researched the diffusion of the Russian and Chinese information control models. During his fellowship Valentin co-authored a paper on mobile app store censorship, with a special focus on the availability of VPN apps in China and Russia's major mobile app stores. The paper found that despite both countries having restrictive VPN laws, there are still many VPN apps available in Russia but only a handful in China. He summed up the findings in a blog post for OxPol. Valentin's final report defined the Chinese and Russian models of information control and traced the export of these filtering/surveillance technologies and techniques to 110 countries. In the report, he analyzed the benefits of this diffusion for Beijing and Moscow, and

[59] NB: OTF's 2017 ICFP funding included three fellows from the 2018 class.

assessed the impact it has on citizens across the globe. His final report was presented at the National Endowment for Democracy and in an OTF blog post. The report is available in English, Chinese, and Russian.

Alexei Abrahams

Host organization: Citizen Lab, Munk School of Global Affairs, University of Toronto
Duration: Twelve months

Alexei investigated information manipulation on social media in the Arabian Gulf. Combining big data science with regional and language knowledge, Alexei documented how Arabian Gulf states use automation of centrally controlled accounts (bots) and elite social media influencers to alter the political opinions of domestic and foreign audiences. He authored a thought piece and co-authored two academic articles (here and here), as well as an op-ed analyzing the tactics of Gulf states with a particular focus on Saudi Arabia and Qatar. He was also quoted in numerous media outlets.

William Tolley

Host organization: International Computer Science Institute, UC Berkeley
Duration: Twelve months

William researched previously unexplored vulnerabilities in VPNs that can be exploited by malicious actors. The results of his research highlighted how the websites visited by a VPN user on nearly any platform can be discovered or even hijacked. William and the other researchers on the effort responsibly disclosed these vulnerabilities and encouraged the implementation of various mitigations. One of the first entities to implement these recommendations was the IFF-supported WireGuard protocol referenced above.

Mahsa Alimardani

Host organization: Oxford Internet Institute
Duration: Nine Months

Mahsa researched the effect of information controls on user behavior in Iran, particularly in their use of social media and messaging platforms. Her research, which relied on both qualitative and quantitative data, is expected to be published in the spring of 2020.

Nguyen Phong Hoang

Host organization: Calipr research group at University of Massachusetts, Amherst
Duration: Twelve months

Phong studied the Invisible Internet Project (I2P) with a focus on the network's censorship resistance. I2P is a well-known and widely used anonymity network that can be utilized to

protect online privacy or bypass censorship. Phong carried out numerous projects to improve the I2P ecosystem. He built a metrics portal for I2P that provides useful data for other researchers, published numerous papers identifying where and how access to I2P is blocked around the globe, and investigated and implemented solutions to make I2P more resistant to blockage. As a result of this work, I2P is now more accessible to end users who need the tool to circumvent internet censorship and online surveillance. A blog post summarizing Phong's work completed over the course of the fellowship can be found here.

[Name Redacted]

Host organization: Open Observatory of Networking Interference
Duration: Twelve Months

This fellow worked with OONI to document internet censorship and surveillance in Manipur, a disputed region of India, and determine the impacts on local marginalized communities (with a particular focus on women). Information on the Manipur region has only recently become available due to the rapid penetration of mobile internet. The project's outputs will offer a deep and comprehensive understanding of the nature and impact of local censorship, internet filtering, and surveillance.

[Name Redacted]

Duration: Eight Months

The fellow analyzed network interference in Egypt and documented arrests based on digital expression. Their research situated these technological interventions within the broader social, economic, and political context in Egypt since 2013. Their project resulted in a data set of 333 digital expression arrests in Egypt from 2011 until 2019. Analysis of the data revealed a yearly increase in the number of digital expression violations, with a surge in the occurrence of these violations beginning in 2016 and continuing until mid-2019. The project's final report was released in October 2019.

Sylvia Kanari[60]

Host organization: East and Horn of Africa Human Rights Defenders Network
Duration: Nine Months

Sylvia studied the application of information controls in Tanzania. Her study sought to investigate the ways in which government and other non-state actors are limiting freedom of expression and other rights online. The primary focus of the project was on detecting, documenting, and analyzing technical and legislative threats to online freedoms.

[60] This fellowship concluded early due to unforeseen circumstances.

Gabrielle Lim

Host organization: Data & Society
Duration: Twelve Months

Gabrielle worked with Data & Society to better conceptualize and map out the influence of disinformation and media manipulation in Malaysia, given recent efforts to limit freedom of the press and increase online information controls. The project explored how "security threats" can be utilized to enable authoritarian practices as well as the risks that "fake news" can have on freedom of expression and information access when securitized by the state. Gabrielle's paper, entitled "Fake News" As National Security Threat And Its Implications For Censorship, Digital Dissent, And Resistance, was published in coordination with Data & Society, along with a blog post.

Rebekah Overdorf

Host organization: École polytechnique fédérale de Lausanne (EPFL)
Duration: Twelve Months

Rebekah is working to develop a comprehensive methodology to identify fake online social network accounts, map their connections to other accounts, and monitor and assess their activities. The methodology will combine state-of-the-art artificial intelligence methods with investigative journalistic tactics, using Kyrgyzstan as its case study. By automating this detection, the project can analyze the extent, tactics, and impact of the effort. Rebeka's research is expected to be published in the summer of 2020.

Marcus Michaelsen

Host organization: Hivos
Duration: Twelve Months

Marcus worked with Hivos to investigate digital threats against diaspora activists from Egypt, Iran, and Syria. His research assessed the methods, motivations, and capabilities of state actors targeting human rights defenders and journalists beyond their borders. It also examined the impact of these threats on the targeted communities and their strategies of resistance. Marcus' research revealed that digital technologies are at the heart of this repression against activists living outside their homeland. The tools most often used include online monitoring and surveillance, account and device hacking, aggressive disinformation campaigns, and online publication hacking. Marcus' findings were summarized in a blog post on the OTF website. His full paper, entitled The Silencing Effect of Digital Transnational Repression, was published in coordination with Hivos.

Labs

Despite the diverse nature of challenges being tackled by those in the internet freedom community, there remains a set of relatively common needs for tools and technologies in the space, including secure hosting, code audits, localization, usability design, and event support. In addition to directly funding projects through regular open calls, OTF therefore also offers a range of services through its Labs aimed at bolstering the robustness of internet freedom via narrow, cost-effective effective service interventions. The organization's unique position within the broader community helps OTF coordinate the provision of these Lab services in a manner that achieves economies of scale, improves quality control, and helps standardize terms and concepts. Services offered through OTF's Labs are generally available to both OTF-funded projects and other significant internet freedom efforts through applications associated with each Lab.

Engineering Lab

The Engineering Lab houses OTF's technical service offerings which include eclips.is, the OTF-supported Secure Cloud Infrastructure, Amazon Cloud credits, Google Apps credits, and other engineering resources that are frequently needed by projects. In FY2018, OTF expanded the Engineering Lab to include developer services to help integrate key internet freedom technologies into projects and tools. One such example is partnering with major public broadcasting networks (including The BBC, Deutsche Welle, Radio Free Asia, Radio Free Europe/Radio Liberty, and Voice of America) to make their websites available via dedicated "mirror sites" using Tor .onion addresses, allowing them to reach readers in countries where their websites would normally be blocked or censored.

Red Team Lab

The Red Team Lab ensures that the tools and technologies relied upon by the internet freedom community are as secure as possible. The Lab focuses on improving the software security of projects that advance OTF's internet freedom goals by ensuring that code, data, and people behind the tools have what they need to create a safer experience for people experiencing repressive information controls online.

Community Lab

The internet freedom community is grassroots in nature, comprised of many different actors across the globe each responding to distinct local or national threats. Yet the repressive actions they seek to combat often receive the full support of some of the most powerful nation states in the world. As such it is vital that those striving to advance internet freedom are able to convene nationally, regionally, and globally to share best practices, discuss emerging threats, and establish networks of support and trust. In FY2018, OTF supported events focused on regional communities dealing with the challenges of repressive censorship and surveillance in Africa, Latin America, the Middle East, and Asia. More technical gatherings were also convened to help tackle key challenges such as network and censorship monitoring.

Internet Freedom Festival

$300,000

The Internet Freedom Festival (IFF) is one of the largest gatherings in the world that brings together activists, journalists, developers, humanitarian workers, and others working on internet freedom, privacy and security, and freedom of expression. In 2019, the IFF hosted 775 participants from 101 countries. More than 54% of participants were from the Global South and other communities not traditionally well represented in the internet freedom community or the broader technology industry. The Internet Freedom Festival Diversity & Inclusion Fund was awarded to 86 individuals (44 women, 36 men, and six gender fluid) from 36 countries across eight regions. Using an unconference format, the event focused on hands-on creation and collaboration. Sessions in 2019 covered topics such as: On the Frontlines, The Next Net, Training and Best Practices, Hacking the Net, Community Resilience, and Journalism and Media. The Glitter Meetups, weekly online meetups hosted on IFF's Mattermost platform, were also launched this year to help the IFF community connect and share on a more regular basis.

Citizen Lab Summer Institute

$47,000

The Citizen Lab Summer Institute on Monitoring Internet Openness and Rights is a series of intensive research workshops hosted annually at the Munk School of Global Affairs. It is a key event for the information controls research community, including the current class of OTF Information Controls Fellows. Knowledge shared during the event is a crucial component for identifying and pursuing future collaborative research projects.The workshop had its highest ever level of attendance in 2019, bringing together diverse experts from different disciplines all focused on studying technologies and policies that can threaten or promote freedom of speech online. The four research topics focused on during the event were Network Interference and Freedom of Expression Online, Surveillance and Counter Surveillance, Policy and Transparency, and Security and Privacy of Apps. A full summary of the event can be found here.

Reproducible Builds Summit

$17,250

The Reproducible Builds Summit 2018 was a three-day workshop designed to continue and grow the Reproducible Builds effort. Reproducible Builds provides a means to independently verify that software used by individuals and journalists has not had backdoors or other vulnerabilities introduced during the process of converting the source code into the form used by a computer or other electronic device. The 2018 Summit was attended by nearly 50 people. Attendees exchanged information and updates about the status of Reproducible Builds in various projects and worked together to improve collaboration between projects. The group also brainstormed designs for tools enabling end-users to get the most benefits from Reproducible Builds. Overall, the summit fostered strategic and long-term thinking tol help Reproducible Builds become more usable and meaningful to users and developers in the future.

Underexposed

$8,660

Underexposed is an annual event designed to elevate previously ignored issues in tech that need to receive attention from the design and usability community. OTF supports the participation of internet freedom projects in the program, including Least Authority, HTTPS Everywhere, SecureDrop, DarkCrystal, and Dice Secrets. During the weeklong residency, the security-focused group worked together on the specific challenges faced by communication freedom tools Since the program's completion, fellows and mentors have published outputs and reflections from the residency, allowing them to share the experience with members of their communities.

Global Voices Asia-Pacific Summit

$52,855

The Global Voices Asia-Pacific Summit 2019, was held in Taipei, Taiwan, on June 2, 2019 The Summit brought together Global Voices community members, citizen media organizations, activists, journalists, academics, technology experts, and policy makers from the Asia-Pacific region to discuss new techno-political challenges to cross-border dialogue and digital rights, including the rise of state-directed online populism, new technology of censorship and surveillance, activism entangled in localism, and rebuilding the cross-border public sphere. In addition to discussions, the Summit also provided training for over 60 participants on digital security. Two networks were formed during the summit, including an alternative belt-and-road citizen media network and a cross-border collaborative journalism network.

Iran Cyber Dialogue

$41,754

The annual Iran Cyber Dialogue (ICD) is organized to support and build practical, collaborative, and long-term responses to internet freedom challenges in Iran. The event specifically focuses on tackling challenges to online access to information and freedom of expression, with an eye for improving privacy and digital security. ICD 2019 covered topics including online access to information, freedom of expression, digital security, bridging tech and human rights, using civic tech to amplify efforts on the ground, and long-term community-building and capacity-building. Additionally, in an effort to seed year-round conversations, the event also piloted seven working groups to lead discussions throughout the year.

Bread&Net

$64,719

Bread&Net is an Arabic-language unconference, organized by SMEX, designed to bring together stakeholders from across the Middle East and North Africa region to strengthen efforts to advance human rights in digitally networked spaces. In November 2019, in Beirut, Lebanon, activists, technologists, lawyers, artists, trainers, journalists, researchers, and entrepreneurs all

convened over three days to set a collective, forward-looking agenda promoting digital freedoms throughout the region. As a participant-driven gathering, where all content was designed by attendees, Bread&Net provided space to develop improved strategies for engaging broader, more diverse communities in the development and critique of practices and policies that implicate human rights in digital spaces.

Future Paths to a Public Interest Internet Infrastructure

$25,000

This workshop brought together 30 scholars, technologists, and practitioners for a two-day, hands-on meeting centered on discussing ways to ensure the internet infrastructure serves the public interest. Discussions like these are critical because the means by which technologies such as internet protocols and standards are designed, defined, and subsequently implemented in the internet infrastructure significantly impact the ability of internet users to exercise and enjoy their rights to freedom of expression and privacy.

Usability Lab

The Usability Lab, though its service providers, offers usability and user experience (UX) services to internet freedom projects that help activists, journalists, and everyday citizens facing repressive surveillance and censorship. To this end, Usability Lab provides additional capacity and expertise to project teams when needed, and also dedicates resources to help solve some of the hardest and most emerging usability challenges that hamper tool adoption and cause insecurity.

Okthanks

$70,000

Okthanks is a detail-oriented team passionate about making tools simple to use and understand. Through prototypes and testing, the team creates clear, effective user experiences and brand messages. In 2018, Okthanks worked on a methodology for matching unique and impactful technologies with communities in need.

Simply Secure

$80,000

Simply Secure is a nonprofit dedicated to helping teams make technology that meets the needs of users, especially technology that deals with issues of security, privacy, and transparency. They were founded in 2014 to support the internet freedom and open-source communities by helping the communities make their tools more usable. They offer UX coaching, user-study design, and other services in addition to a growing set of resources in their online Knowledge Base.In 2018, Simply Secure's work included producing a case study on their secure usability minded redesign of the popular privacy enhancing tool Noscript.

Torchbox

$50,000

Established in 2000, Torchbox is a U.K.-based, award-winning independent digital agency. They specialize in digital strategy, UX design, website development, software engineering, and digital marketing for people who are trying to make the world a better place. They design and build beautiful, responsive websites and applications for some of the world's great universities, think tanks, charities, NGOs, and membership organizations.Torchbox's work in 2018 included a UX review of the Apple Censorship website by Greatfire.

Ura

$70,000

Founded in Albania in 2016, Ura is a digital agency focused on visual communication solutions tailored for open source and internet freedom projects. They strive to improve usability and UX by keeping each project's unique community consensus model in mind. The agency offers UX design, design systems research, and visual identity services to help support project needs. In 2018, Ura worked on many internet freedom projects, including upgrading Thunderbird's style guide and identity and securely redesigning the HTTPS Everywhere browser plugin.

Localization Lab

Because even the most technically robust internet freedom tools are effective only if they are practically accessible to end users in their native languages, the Localization Lab works to make internet freedom tools and resources relevant, accessible, and more usable for global communities in need. The Lab creates space for end users, developers, CSOs/HROs, and trainers to communicate by way of localization, user research, and translation efforts. OTF supports these efforts by providing direct support to the Localization Lab and by providing funding for the Transifex platform on which the Lab is run.

Localization Lab, Inc

$225,500

The Localization Lab translates and localizes internet freedom tools, supporting documentation, and training materials to help grant access to users living under repressive governments who would otherwise lack access to these critical tools. The Lab further enables adoption of internet freedom technology by facilitating usability research, testing products, and growing a user base for the tools through coordinated community outreach and trainings. Across five years, the Lab has assisted 88 projects, managed 6,400 community translators (who are also end users of the tools), and helped make internet freedom tools available in 217 languages around the world.

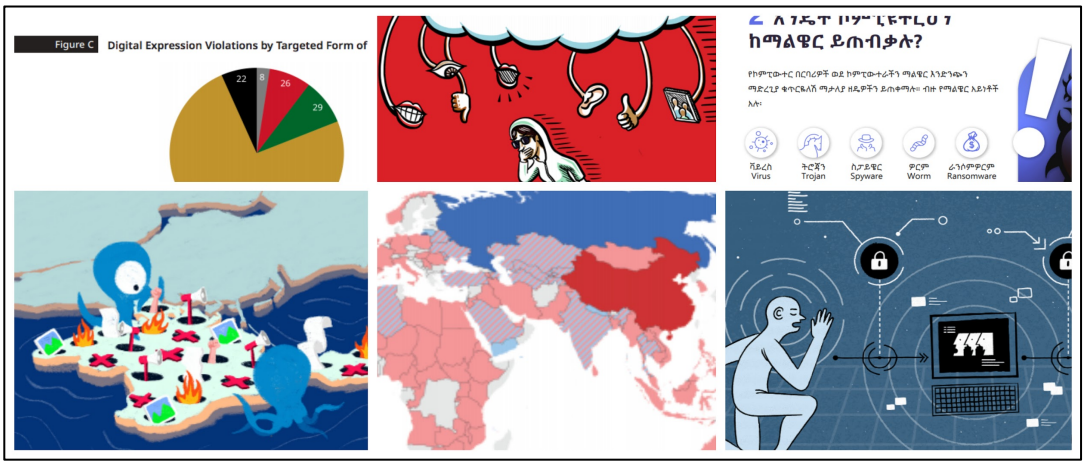
Transifex Platform

$230,886 [61]

To perform its work, the Localization Lab needs a web-accessible, easy-to-use system to allow translators and technology projects to submit and pull translations to be utilized by internet freedom tools and projects. Transifex provides the platform through which language translations can be submitted and managed across projects and individuals.

Learning Lab

The Learning Lab connects OTF-supported projects and fellows with service providers offering writing, graphic design, and layout services. By collaborating with Learning Lab partners, these projects and fellows are able to better tell their unique stories, broadcast and market their work, and ensure their outputs effectively communicate their message in a well-written manner.



Chad B. Anderson Editing and Writing

$20,000

Chad B. Anderson is a freelance editor and writer. Chad and partner John Stith help OTF-supported projects draft, edit, and fine-tune written outputs such as reports, web content, and blog posts. In their first year as Learning Lab partners, John and Chad worked with more than ten projects and fellows from across the internet freedom community.

Cartoon and Design Services

$20,000

OTF hired an independent designer, cartoonist, and consultant working at the intersection of storytelling, technology, and social change. This consultant is adept at translating complex concepts and ideas into compelling visuals and has worked with many groups and individuals from across the internet freedom community.

[61] The Transifex Platform is renewed on an annual basis. The cost for this renewal was partially drawn from multiple fiscal years.

Ura Design

$20,000

Ura Design is a digital studio which focuses on visual communication solutions tailored for open source and internet freedom projects. In addition to offering services through the Usability Lab, Ura also provided specialized assistance to projects through the Learning Lab for graphic and layout/design needs.

Fiscal Year 2018 Spending

Direct Support		
Funds (Projects)		
	Internet Freedom Fund	$3,970,406
	Core Infrastructure Fund	$1,037,377
	Rapid Response Fund	$312,019
Labs		
	Community Lab	$294,123
	Usability Lab	$65,083
	Localization Lab	$648,612
	Engineering Lab	$905,258[62]
	Learning Lab	$110,000
Fellowships		
	Information Controls Fellows	$325,700
	Digital Integrity Fellows	$415,000
Convenings		
	Conferences[63]	$405,244
	OTF Summit 2019	$189,700
	Programmatic travel	$258,294
Program Operations		
	External consultants	$46,200
	Non-salaried team and consultants	$270,904
	Team travel	$82,000

[62] Costs for the Red Team Lab fall under the heading of the Engineering Lab in this budget.
[63] This represents OTF's support for the Internet Freedom Festival, which is co-funded by the State Department's Bureau of Democracy Human Rights and Labor.

	Admin and other	$78,755
	General and other	$56,441
	Office space in DC	$28,884
Totals		
	Direct Support	$8,936,816
	Program Operations	$563,184
	Total Programmatic Spending	$9,500,000
	Designated for Salary and Benefits	$1,200,000
	Total Spending	$10,700,000