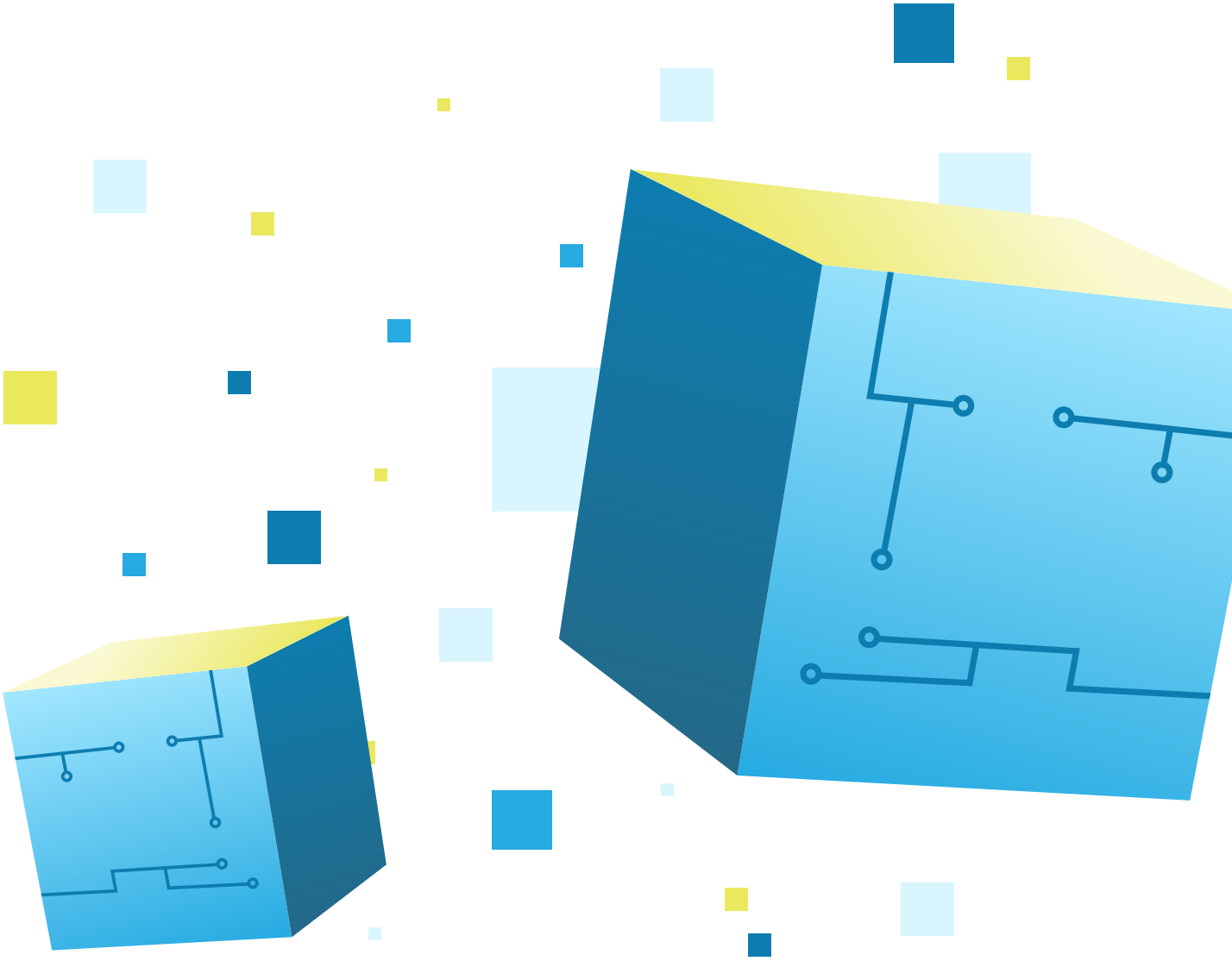
OPEN TECHNOLOGY FUND

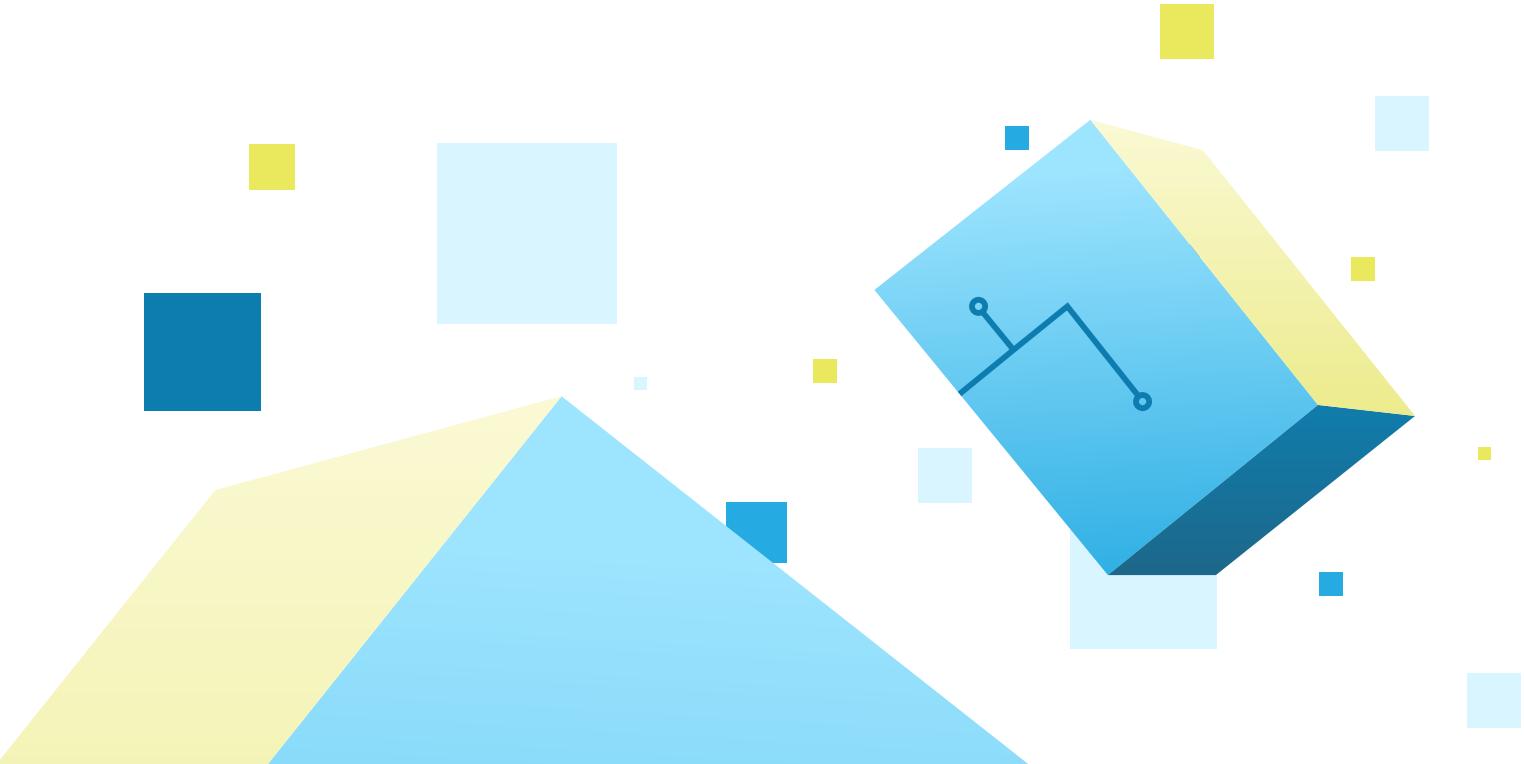


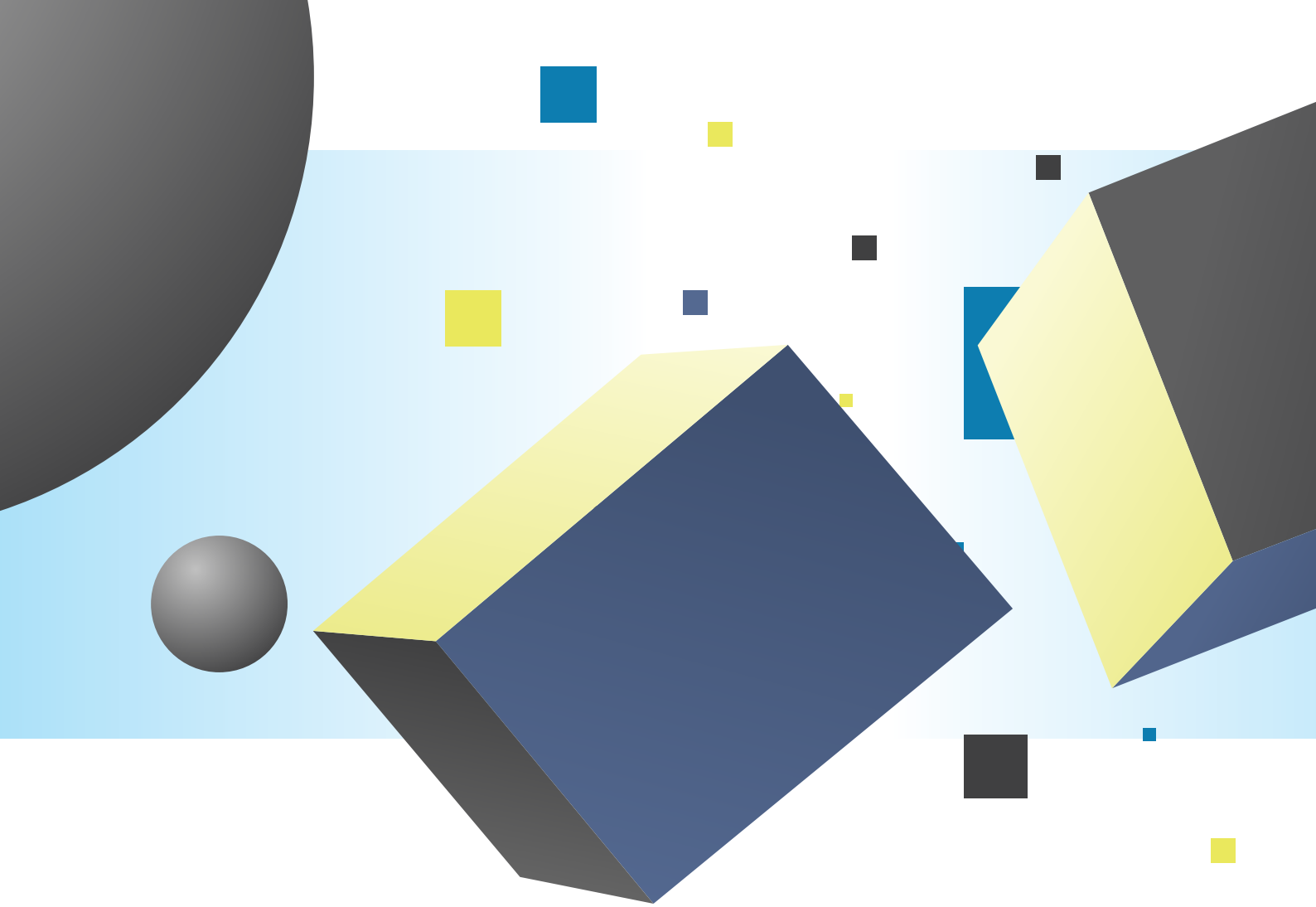
2021

ANNUAL REPORT

Table of Contents

Layout design by ura





01 About This Report

This report covers the activities supported by Open Technology Fund (OTF), with a small number of exceptions for highly sensitive projects, from March 2022 through December 2022 with FY2021 funds.

02

About OTF

Open Technology Fund (OTF) is a Congressionally authorized, independent nonprofit organization dedicated to advancing internet freedom globally. OTF works to advance internet freedom in repressive environments by supporting the applied research, development, implementation, and maintenance of technologies that provide secure and uncensored access to the internet to counter attempts by authoritarian governments to restrict freedom online and to enable citizens worldwide to exercise their fundamental human rights online.

Our Mission

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 internet to counter attempts by authoritarian governments to restrict freedom online and enable all citizens to exercise their fundamental human rights online.

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 the uncensored internet. This includes supporting the development and deployment of an array of circumvention technologies to counter increasingly sophisticated censorship techniques, new solutions to counter internet shutdowns, and applied research to help tool developers and users stay ahead of new censorship threats.
- **Protect journalists, human rights defenders, and marginalized communities from repressive surveillance and digital attacks** to help ensure they are able to safely access and share information online. This includes support for secure communication tools, targeted digital security interventions, and other forms of privacy and security technology.

Our Approach

To advance its mission to support internet freedom in repressive environments, OTF provides direct funding and support services to individuals and organizations around the world that are addressing threats to internet freedom, journalism, and human rights with technology-backed solutions. OTF provides funding and support through a variety of mechanisms in order to provide tailored and comprehensive assistance to internet freedom projects. Because internet censorship technology and tactics are constantly evolving, OTF receives, reviews, and contracts projects on an ongoing basis via open calls. OTF solicits project ideas through a fully open and competitive application process on its website. The process is designed to reduce barriers to applying for funding and 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.

In order to ensure a high degree of due diligence, OTF implements a rigorous multistage 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.

OTF Programs

During the time period covered by this report, OTF implemented the following funds, labs, and fellowship programs.

Funds

OTF provided direct funding to support the applied research, development, implementation, and maintenance of technologies that enable censorship circumvention and enhance user security and privacy online. OTF managed multiple funds that supported innovative global internet freedom projects, large-scale circumvention and secure communications technologies, and emergency support mechanisms.

These funds included:

- **Internet Freedom Fund (IFF)**

  The Internet Freedom Fund is the primary fund through which OTF supports innovative global internet freedom projects. IFF projects are primarily focused on technology development and implementation but can also include applied research and digital security projects.

- **Technology at Scale Fund (transitioning to the Surge and Sustain Fund in 2023)**

  The Technology at Scale Fund supports the large-scale circumvention and secure communication technology needs of USAGM's networks (Voice of America, Radio Free Europe / Radio Liberty, Office of Cuba Broadcasting, Radio Free Asia, and Middle East Broadcasting Networks). The fund solicits technology solutions that help deliver content to audiences in information-restricted environments and protects journalists and their sources. The fund also ensures that technologies used at scale by millions of users remain secure and effective.

- **Rapid Response Fund**

  The Rapid Response Fund provides emergency support to independent media outlets, journalists, and human rights defenders facing digital attacks. The support through this fund helps individuals and groups stay safe in repressive environments, regain online access, mitigate future attacks, and combat sudden censorship events. The fund also provides rapid support to mitigate new software vulnerabilities, including the development and deployment of emergency technical patches, to ensure that critical internet freedom tools remain secure.

Labs

OTF provided support to existing internet freedom projects through the organization's Resource Labs (Labs). OTF offers expert services to the internet freedom community through its five lab offerings: **Engineering Lab**, **Red Team Lab**, **Secure Usability and Accessibility Lab**, **Localization Lab**, and **Learning Lab**.

Together, these labs provide security code audits, usability assessments, engineering support, translation and localization assistance, and secure cloud storage. These services ensure that the technologies incubated and supported by OTF are as effective, secure, and usable as possible.

Engineering Lab

OTF's Engineering Lab helps to secure the technological infrastructure behind internet freedom technologies. This lab focuses on supporting the implementation and inclusion of established technologies into existing applications, organizations, and communities that are advancing internet freedom. This includes facilitating the widespread adoption of underlying circumvention and privacy technologies, supporting the infrastructure that addresses the unique needs of internet freedom developers and end-users, and gaining better insights into the costs required to enhance existing systems.

Red Team Lab

OTF's Red Team Lab conducts independent security audits of internet freedom technologies to help improve the security of projects and ensure a safer experience for people experiencing repressive information controls online. The primary work of this lab is reviewing and responding to security issues in internet freedom software and tools.

Secure Usability and Accessibility Lab

OTF's Secure Usability and Accessibility Lab improves the usability of open-source circumvention and digital security technologies. This lab supports software development teams in the creation and improvement of projects that aim to help journalists, human rights defenders, and everyday citizens communicate privately and securely. The Secure Usability and Accessibility Lab offers secure usability audits, user experience consultations, usability testing, user research, user studies, and more.

Localization Lab

OTF's Localization Lab helps to localize internet freedom tools into over 200 languages for different countries and regions. Addressing a major challenge for internet freedom technologies of reach and adoption, this lab helps adapt internet freedom tools that are relevant and appropriate for another country or culture.

Learning Lab

OTF's Learning Lab helps to tell the stories of OTF-supported projects and the results they produce. Through this lab, projects and fellows communicate the results of their projects. This lab helps to facilitate knowledge sharing and collaboration across the internet freedom community.

Fellowships

OTF supports individuals in carrying out cutting-edge applied research projects that examine how authoritarian states are restricting the free flow of information and explore ways citizens can overcome those tactics. OTF fellowships help cultivate the next generation of internet freedom experts by creating a career track for those who have the skills and passion for internet freedom.

- **Information Controls Fellowship Program (ICFP)**

  The Information Controls Fellowship Program (ICFP) supports research efforts to examine how authoritarian governments are restricting the free flow of information and to explore solutions to overcome these evolving tactics.

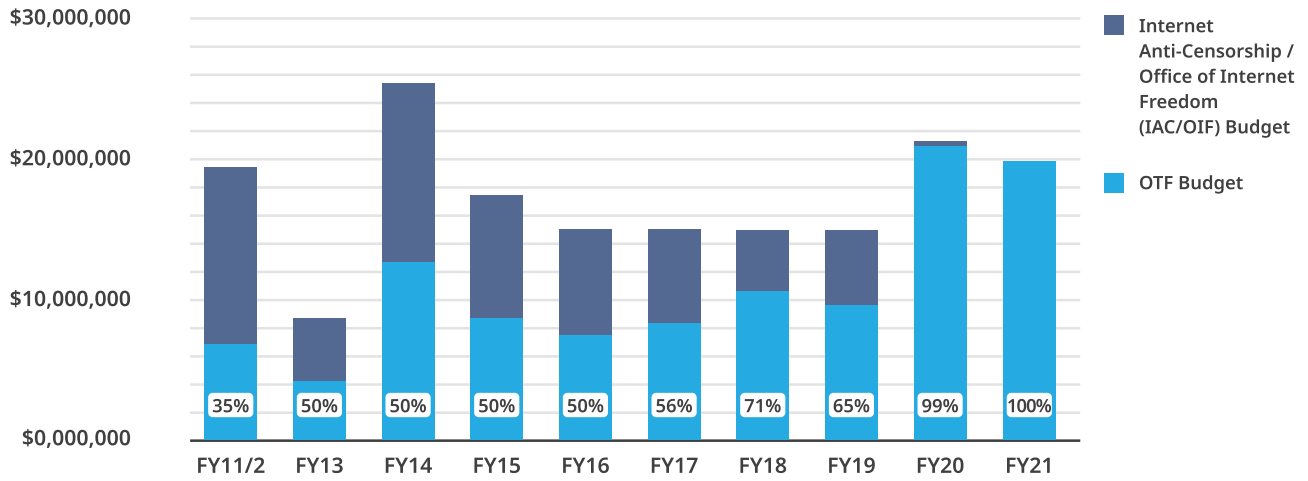
OTF Funding

OTF is a grantee of the U.S. Agency for Global Media (USAGM) and is funded by the U.S. government through annual appropriations passed by the United States Congress to support "programs to promote internet freedom globally." OTF's appropriations are included as a component of the Department of State, Foreign Operations, and Related Programs for each fiscal year.

Per Congressional appropriations requirements, each year, the USAGM submits an "Internet Freedom Spend Plan" to Congress outlining its proposed use of internet freedom funds appropriated in that fiscal year. The USAGM Internet Freedom Spend Plan is reviewed and approved by Congress prior to implementation.

In FY2021, Congress appropriated $40.7 million for "satellite transmissions and internet freedom programs" to USAGM, of which USAGM provided $19,877,529 to OTF to support internet freedom programs.

USAGM (BBG) Internet Freedom Funding History



03

Internet Freedom Under Threat

Authoritarian control of the internet is on the rise. Across the world, repressive regimes are utilizing more aggressive tactics to divide the open internet into more easily controllable digital territories, representing some of the sharpest downturns in internet freedom to date.[1]

Reliance on internet access has grown to unprecedented levels around the world due to the COVID-19 pandemic. This increase in adoption has resulted in a commensurate crackdown on free expression online as authoritarian governments work diligently to implement ever more stringent information controls. Online censorship is at an all-time high worldwide, and by relying on digital surveillance and censorship, repressive governments have gained access to extraordinary amounts of information on citizens. These efforts have only accelerated due to the proliferation of technologies such as artificial intelligence and facial recognition.

Historically, in most of the authoritarian world, online censorship has ebbed and flowed. Important state anniversaries, periods of political unrest, and unpredicted social phenomena could all trigger heightened public interest in information that would, in turn, lead to heightened censorship by authorities. This was naturally reflected in the use of OTF-supported circumvention tools, where surges in tool use routinely occurred around such events before returning to normal levels.

However, this predictable dynamic appears to be fundamentally changing as what were once temporary peaks in usage have now become new permanent plateaus. Following the 2021 coup in Myanmar, the 2022 Russian invasion of Ukraine, and the Mahsa Amini protests in Iran, online censorship in these countries has reached new heights. As a result, the use of OTF-supported circumvention tools has not only surged but also remained extremely high, confounding the old expectation of a return to baseline.

While the main indicator that is observable to us outside these countries is the continued use of circumvention tools beyond the apex of a political crisis, this is likely best understood as a necessary response to authoritarian regimes who, after stepping up censorship during a crisis, do not revert to a looser grip post-crisis. These dynamics are only further exacerbated by the blocking of large global social media platforms, which has gone from a China-only exception to an authoritarian norm.

Last year, Russian President Vladimir Putin moved aggressively to centralize power amid the country's invasion of Ukraine, utilizing the country's growing investments in repression technology to silence dissenting voices and curb the spread of information.

The digital environment in Russia deteriorated dramatically when the government blocked many of the most widely used global social media and content platforms, including Twitter, Facebook, and Instagram. Censors also targeted the websites of Radio Free Europe and Voice of America.[2]

1 https://freedomhouse.org/report/freedom-net/2022/countering-authoritarian-overhaul-internet

2 https://ooni.org/post/2022-russia-blocks-amid-ru-ua-conflict/

The challenges associated with reporting on the war in Ukraine for independent Russian news outlets have ballooned, as many ceased operations following Putin's signing of a "fake news" law that threatened imprisonment for any journalist deviating from the Kremlin's portrayal of the conflict.[3] The audiences for these outlets faced similar obstacles in accessing their content, resulting in dramatic growth in the adoption of circumvention tools. Despite repeated attempts to interfere with the functionality, tools such as the Tor Browser quickly adapted their technology to overcome these efforts.[4] This was a result of deepening collaboration between end users, researchers, and the tools themselves.

Meanwhile, China witnessed widespread protests in the fall of 2022. In response, the Chinese government deployed increasingly sophisticated censorship tactics, including interfering with censorship circumvention tools. As a result of these measures and the associated timing, in-country developers focused on overcoming the new tactics by collaborating and sharing what advanced techniques could pierce the blockade. China instituted a more limited and targeted escalation of censorship surrounding the 2022 Beijing Olympics by jailing activists and taking numerous steps to control the online narrative of the event.[5] This was in addition to ongoing efforts to control the algorithms used by the country's largest online platforms to ensure they "carry forward the Socialist core value view" and to censor open source code until it receives government approval.[6] In October 2022, China held the National Congress for the Communist Party and employed new techniques by utilizing TLS fingerprinting, likely through machine learning techniques, to interfere with many of the most utilized circumvention techniques.[7] [8] Nonetheless, the event that created the biggest challenges occurred the following month when unprecedented protests took place, voicing opposition toward the government's extensive use of lockdowns to control COVID outbreaks. The nature and scale of the mobilization left censors scrambling to keep up.[9] This development demonstrated that the country's censorship apparatus struggles to scale when the population expresses widespread discontent.

Similarly, protests broke out in Iran in the fall of 2022 following the death of Mahsa Amini. This resulted not only in internet shutdowns to curb the spread of content and silence protesters but also in the targeting of virtually every channel of communication.[10] The government sought to curb access to the two remaining and most popular social media platforms, WhatsApp and Instagram.[11] Government censors also took numerous steps to increase censorship through the targeting of encrypted DNS, HTTP/3, app stores, and browser extension repositories.[12]

3 https://www.cfr.org/in-brief/russia-censoring-news-war-ukraine-foreign-media-are-trying-get-around

4 https://www.wired.com/story/tor-browser-russia-blocks/

5 https://www.theguardian.com/world/2022/feb/03/nobody-can-say-anything-china-cracks-down-on-dissent-ahead-of-olympics

6 https://www.isdglobal.org/digital_dispatches/chinas-sweeping-algorithm-regulation-and-global-digital-governance/ ; https://www.technologyreview.com/2022/05/30/1052879/censoring-china-open-source-backfire/

7 https://www.theregister.com/2022/10/06/great_firewall_of_china_upgrades/

8 https://en.greatfire.org/search/alexa-top-1000-domains

9 https://www.nytimes.com/2022/11/30/business/china-protests-censorship-video.html

10 https://www.nbcnews.com/news/world/internet-freedom-activists-scramble-help-iranians-evade-tehrans-digita-rcna50232

11 https://ifpnews.com/55mn-iranians-using-social-media-statistics/ ; https://www.bourseandbazaar.com/articles/2022/12/28/how-shifts-on-instagram-drove-irans-mahsa-moment

12 https://ooni.org/post/2022-iran-technical-multistakeholder-report/

The government has attempted to poison the market for circumvention tools by deploying copycat apps to lure unsuspecting Iranians into installing malware.[13] Researchers also uncovered technology being relied on by the government to remotely manipulate cellular connections to access a device or prevent two-factor SMS authentication.[14] This is in addition to continuing to carry out hacking attempts targeting Middle East-focused researchers, civil society groups, and dissidents.[15] Despite these expansive efforts, usage of OTF-supported circumvention tools jumped from six million daily users to nearly 30 million.[16] This mirrors noteworthy increases in the broader VPN industry.[17] The results of these efforts are apparent in the extent of information critical of the government finding its way onto blocked platforms and the widespread usage occurring more generally.[18]

In addition to Iran, many other authoritarian governments have continued to rely on internet shutdowns to prevent access to the internet. As a result, internet shutdowns have quickly become a frequently used mechanism to quell protests, silence activists, and stymie the spread of information. In 2022, governments significantly disrupted or completely shut down the internet at least 187 times across 35 countries, marking a resurgence in use after a decrease during the height of the pandemic.[19] Troublingly, these shutdowns are more often used to target specific populations and are longer in duration than in previous years. India, the world's largest democracy, implemented 84 shutdowns last year, and it remains the country with the highest recorded shutdowns for the fifth consecutive year.[20] Other repressive states have been able to effectively deploy shutdowns to limit the flow of information, such as during protest movements in Iran and during elections in Kazakhstan and Turkmenistan. Meanwhile, sustained restrictions continue to obscure ongoing human rights abuses in Myanmar and Ethiopia's Tigray region. This comes despite the serious economic consequences that prevent all online commerce, regardless of how it is taking place.

Despite the rise of these global threats, a record 26 countries experienced improvements in internet freedom. Collaborative efforts between civil society, technologists, and policymakers in many countries have resulted in better legislation, media resiliency, and accountability among technology companies to foster progress for digital rights.[21] Still, as a result of increased surveillance and censorship, significant threats to internet freedom remain. The emergence of new technologies, including machine learning, has made large-scale censorship easier and faster. In addition, more authoritarian governments are adopting methods to establish national intranets to further control their citizens' access to information, while the proliferation of commercial spyware is making it easier for authoritarian governments to track and target civil society and human rights defenders.[22]

13 https://www.bitdefender.com/blog/labs/eyespy-iranian-spyware-delivered-in-vpn-installers/

14 https://theintercept.com/2022/10/28/iran-protests-phone-surveillance/ ; https://www.rferl.org/a/iran-two-factor-verification-codes-blocked/31994626.html

15 https://www.hrw.org/news/2022/12/05/iran-state-backed-hacking-activists-journalists-politicians

16 https://www.rferl.org/a/iranians-circumvent-internet-restrictions/31933593.html

17 https://www.cnbc.com/2022/10/07/vpn-use-skyrockets-in-iran-as-citizens-navigate-internet-censorship.html

18 https://www.nytimes.com/2022/09/29/world/middleeast/iran-internet-censorship.html

19 https://www.accessnow.org/internet-shutdowns-2022/

20 https://www.aljazeera.com/news/2023/2/28/in-2022-the-world-saw-187-internet-shutdowns-84-by-india-alone

21 https://freedomhouse.org/article/new-report-repressive-governments-are-fracturing-internet-driving-12th-consecutive-year

22 https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list ; https://www.apple.com/newsroom/2022/07/apple-expands-commitment-to-protect-users-from-mercenary-spyware/

04

Project Highlights

During the period covered by FY2021 funding, OTF funded over **35 innovative projects** to combat censorship and repressive surveillance. It supported **eight fellows** to engage in cutting-edge research and digital security interventions. It also funded **five labs** to improve the security, usability, resiliency, and interoperability of key internet freedom technologies and **numerous 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.

Surging Support for Circumvention Users

Over the past two years, authoritarian regimes around the world have intensified their efforts to censor content and crack down on access to the free and open internet. As a result, demand for OTF-support circumvention tools has increased from an average of nine million users worldwide to over 40 million users on a monthly basis.

Since the invasion of Ukraine, the use of OTF tools in Russia has surged from approximately 250,000 monthly users to over eight million users each month. Similarly, in Iran, the growth in users has leaped from a previous multiyear baseline of five million users per month to over 25 million users (a figure representing approximately half of Iran's adult population). The use of OTF tools has also increased notably in Myanmar and China.

Despite facing increasingly sophisticated forms of censorship, even at this unprecedented scale of usage, OTF-supported tools continue to perform at the highest technical levels, allowing users in censored areas to securely access blocked content quickly and reliably. In addition, this exponential growth is a testament to the trust that users place in OTF-supported tools, particularly in moments of crisis. Most importantly, these notable increases in demand demonstrate the convening power of technology in today's society and the importance of ensuring that citizens living under repressive regimes have access to information necessary to hold their governments accountable and to make decisions impacting their lives.

This phenomenon reaffirms the technical efficacy of OTF-supported circumvention tools as they are able to support large user populations in advanced censorship contexts on an ongoing basis. However, it does pose a significant budgetary challenge for both OTF and the circumvention tools, as funding and budgeting have traditionally reflected a need to absorb short surges but did not account for permanent states of consistent surge-level usage.

To address this need, OTF created the Surge and Sustain Fund. This fund is an innovative funding structure designed to offset the marginal carry cost of users in highly censored target countries. This is done on a reimbursement basis whereby the cost of a unique monthly user is offset to ensure that tools are able to support large user bases in countries where the need is greatest and few, if any, secure commercial alternatives exist. Initial providers under the Surge and Sustain Fund[23] include **Psiphon**, **Lantern**, and **NthLink**. These tools collectively supported nearly eight million unique monthly active users in Russia and over 20 million unique monthly active users in Iran, following sustained surges in use in each country. While not covered by FY2021 funds, the Surge and Sustain tools have since been broadened to include support for users in China and Myanmar.

Securing and Enhancing Circumvention Solutions

In order to ensure that circumvention solutions do not fall behind the continuous efforts of authoritarian regimes to evolve their censorship capabilities, OTF, with FY2021 funds, invested in research that sought to better understand the implementation of censorship practices by authoritarian regimes, secure new internet protocols, and better protect and support circumvention tool users.

In collaboration with researchers at Citizen Lab, Censored Planet, and Princeton CITP, **ICFP fellow Ramakrishnan Sundara Raman** built a general purpose, robust censorship traceroute mechanism that identifies the network location of devices performing censorship. The resulting toolkit generates various types of device fingerprints to identify censorship devices, measure their deployment in different countries and enables researchers and circumvention providers to continuously monitor the deployment of such devices.

Other FY2021 research investments sought to future-proof the new QUIC internet protocol against emerging censorship techniques through the work of **ICFP fellow Kathrin Elmenhorst.** The research lays important groundwork for monitoring and overcoming QUIC censorship in the future.

23 As well as the recipients of Rapid Response support that was provided in response to censorship events in Iran and Russia, as the Surge and Sustain Fund was set up.

The design of QUIC requires the application of new blocking methods for those aiming to censor information on the internet. Consequently, new measurement techniques are required in order to monitor QUIC censorship and better equip circumvention tools.

OTF strives to ensure that not only are Virtual Private Networks (VPNs) we support able to effectively evade censorship but that they are as secure as possible, given that most censoring regimes also surveil circumvention tool users. By examining the endpoints of a VPN tunnel and the low-level packet routing behaviors within the operating system kernels of the VPN client and VPN server, the **Attacking VPNs to Challenge Basic Security Assumptions** project aimed to reveal flaws in VPNs for security and privacy applications, disclose vulnerabilities to necessary parties, and examine potential fixes for VPN issues. The project further educated at-risk populations about the findings to improve their security postures.

One of the most daunting tasks for those in authoritarian contexts when it comes to adopting circumvention tools is how to navigate the murky, poorly regulated VPN market to find a tool that works and that they can trust, particularly given the preponderance of insecure tools, ranging from those with insufficient user data protections to outright imposter apps. To address this challenge, the **VPNalyzer** project has built a framework enabling systematic and automated investigation into the unregulated VPN ecosystem. The framework relies on a combination of crowdsourced investigations, in-depth reviews of VPN-provider practices, and a cross-platform desktop tool for users to test the security and privacy features of their VPN connection in order to better establish the security and trustworthiness of VPNs.

VPN-style circumvention tools are only one model for censorship circumvention that OTF supports. Particularly in countries where there are significant barriers to user adoption of circumvention tools, OTF works closely with USAGM and others to ensure that publishers can assume the circumvention burden by mirroring their websites. This allows their audiences to access content without the need to download a circumvention tool. In order to ensure this approach to circumvention remains reliably effective even as authoritarian targeting of the technique gets more sophisticated, OTF funded **Project Icarus**, which is pioneering new mirroring techniques built on technologies such as Tor and the InterPlanetary File System (IPFS) that make mirrors more secure and more difficult to block.

While OTF's research portfolio is focused primarily on countering the expanding array of technical means that authoritarian regimes block access to content, another common technique used to limit access to information is by flooding online spaces with coordinated disinformation to such a degree that it constitutes a form of censorship. To better understand and address this censorship tactic, the **Observatory on Social Media (OSoME)** developed an open-source suite of online disinformation and manipulation detectors. OSoME creates bot scores that allow researchers to identify technical coordination efforts to use disinformation campaigns as a form of censorship.

Tooling for Shutdowns

Over the past two years, we have seen the rapid evolution of internet shutdowns as a tool of repressive information control. Once thought to be too economically and politically costly to turn to for anything but as a last resort in a politically existential crisis, shutdowns as a tool of control are now regularly relied upon by authoritarian governments. In many countries, shutdowns can now be administered in a more targeted and nuanced manner, making them less costly for the authoritarian government imposing them while still being extremely difficult to technically mitigate.

As a result, OTF is funding shutdown mitigation solutions that attempt to address the technical challenges users face experiencing every level of shutdown, from those which disable only one form of communication in a targeted fashion to total communications infrastructure blackouts.

Two important contributions to the efforts funded with FY2021 funds include **Ouinet** and **SMS Without Borders**.

Ouinet is a free, open-source technology that allows web content to be served with the help of a network of cooperating nodes using peer-to-peer routing and distributed caching of responses. Built as an integration, it can be used to enable a network exchange of cached data to circumvent censorship and mitigate the effects of some forms of internet shutdowns. If a country cuts itself off from the global internet but national or subnational networks remain functional, Ouinet allows cached content to be shared in a way that mirrors traditional web browsing without needing to pull content from the global internet.

SMS Without Borders patches an important security vulnerability in what has become a common form of shutdown, in which a regime shuts down mobile data but leaves calling and SMS capabilities unaffected. One consequence of this form of shutdown is that those secure messaging apps requiring mobile data are rendered unusable, presenting users with the unsavory choice between communicating via easily surveilable SMS messages or not at all. SMS Without Borders encrypts SMS messages to ensure that if journalists or activists are forced to use SMS during an internet shutdown, the content of their communications can remain safe.

Identifying Threats and Advancing Security in Practice

As the cost of digital surveillance capabilities, once reserved only for global superpowers, becomes affordable to even modestly resourced authoritarians, the ability for journalists, activists, and human rights defenders to carry out their work relies on careful adherence to digital security best practices and innovative technological solutions.

In FY2021, OTF made investments in both threat identification and tracking as well as technologies that advanced the state of the art in applied digital security protections.

The **Global Surveillance Database** project compiled available data from export licensing authorities and relevant reporting on the use of surveillance technologies, including Pegasus in Thailand, IMSI-catchers in Indonesia, and global SS7-attacks (a security exploit that takes advantage of a weakness in the design of Signaling System 7 that enables data theft and eavesdropping) in Libya, Malaysia, Italy, Nicaragua, and Pakistan to better inform regional and local actors of specific threat vectors and encourage appropriate mitigations.

As advanced surveillance techniques have become more widely available, it is imperative that the capabilities of local journalism and human rights organizations to detect and repel digital attacks also increase. **PiRogue Tool Suite** is an open-source tool suite that provides a comprehensive forensic and network traffic analysis platform designed to greatly increase the ability of organizations under threat to assess the privacy and security of mobile devices. Increasing the availability of such advanced threat detection capabilities will help frontline organizations better protect their own security.

In order to further extend the protections of vital secure messaging apps, **Project Phoenix** aims to bring the new Messaging Layer Security (MLS) protocol into maturity in a user-facing app. The implementation of MLS to underpin a secure messenger app has the potential to combine Signal's metadata minimalism with Matrix's federation features and Wire's username-based approach and ease of use.

Secure file transfer is one of the most pressing needs of any journalist in a highly surveilled context. The **Filezilla** project will introduce security, privacy, and usability improvements to an implementation of SFTP, a private and secure protocol for file transfer that is relied on by many users in countries without free internet. Filezilla enables people to use SFTP to transfer files with far greater security guarantees.

In addition to on-network and on-device surveillance, OTF has also supported efforts to identify and analyze external surveillance mechanisms, including IMSI-catchers. IMSI-catchers are portable surveillance tools that act as fake cell phone towers to intercept cell phone traffic and are often used for surveillance at particularly crucial moments, such as protests. They present a particularly unique surveillance challenge in that they are very difficult to detect and defend against. The **FADE Project** expanded studies to detect the use of IMSI-catchers in a standardized way in Latin America to further develop the detection methodology, technical tools, and mitigation strategies for the civil society actors and journalists in the region.

Increasing Impact through Collaboration

The internet freedom landscape is an ever-evolving space in which authoritarians seeking to limit their populations' access to information are constantly innovating and learning from one another in attempts to create new norms for digital control. Thus, the global internet freedom community must collectively be able to dynamically identify new threats and opportunities and respond quickly to changing circumstances. OTF bolsters this capability through support to key community convenings.

With OTF support, **Team CommUNITY** organized both digital and in-person convenings focused on technical topics, specific communities of practice, and shared threats or needs. These efforts collectively facilitate trust, information sharing, and technical collaboration and result in a more cohesive response and bulwark against new digital threats.

Responding to Digital Emergencies

OTF has, with FY2021 funds, also responded to numerous extremely pressing digital emergencies. Among those of particular note were efforts to surge digital support to those on the frontlines of huge political and military events in Myanmar, Ukraine, Russia, and Iran.

Myanmar

In 2021, military leaders seized control of the government of Myanmar and immediately imposed vastly increased internet censorship and implemented routine short-term internet shutdowns. To address the security needs of human rights organizations based in Myanmar, OTF continued to provide emergency digital support to civil society organizations (CSOs) to improve freedom of expression and digital rights in the country. Services included digital security audits, recommendations on mobile devices and device security practices, enhancing digital safety protocols, expanding the organizations' secure communications infrastructure, and rebuilding web platforms to include modern security standards.

Ukraine

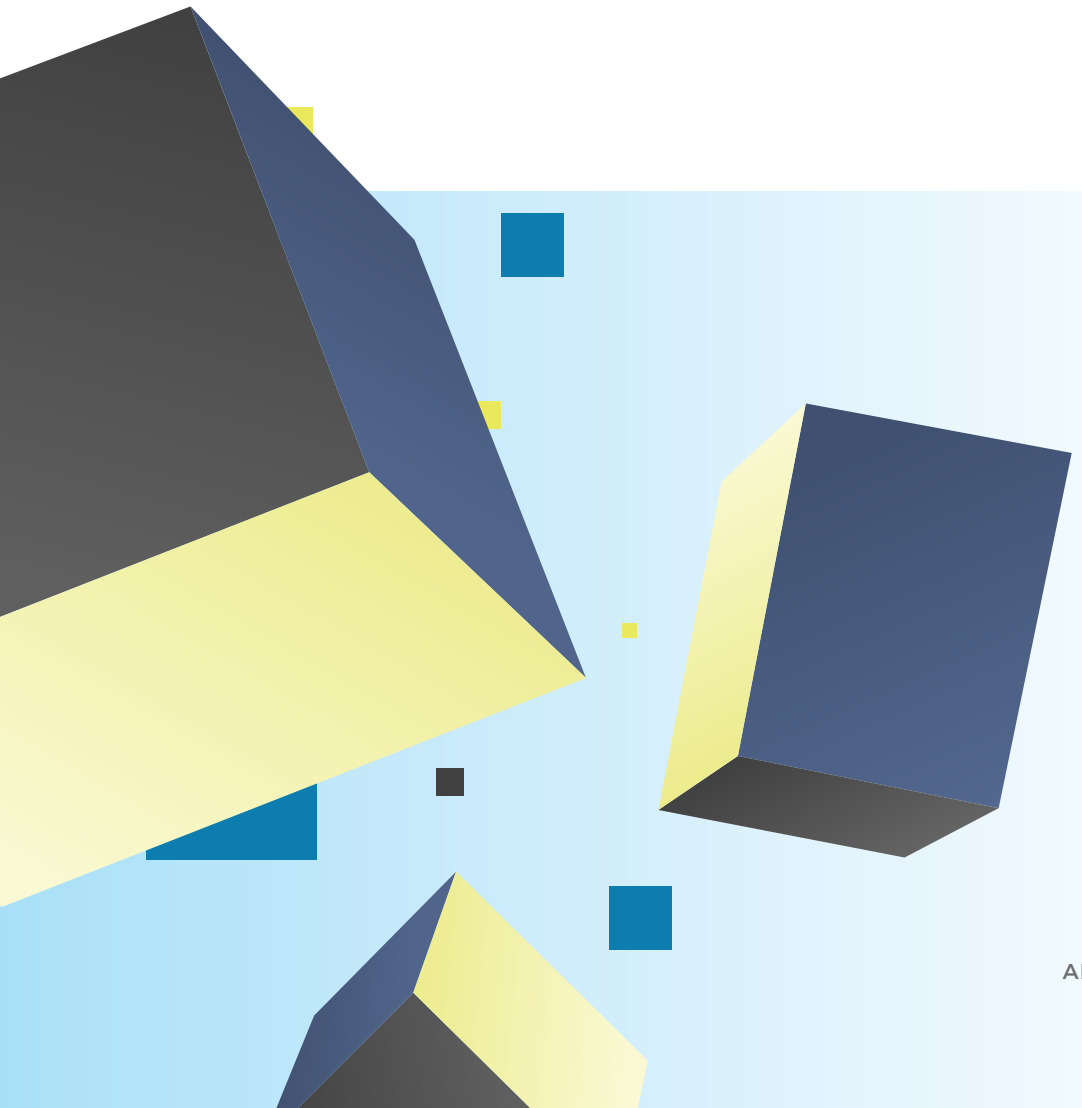
The Russian government invaded Ukraine in February 2022. Immediately following the invasion, OTF focused rapid response support to ensuring that Ukrainian civil society was prepared for the potential of digital attacks by launching **dComm**, a federated network of servers in Ukrainian cities offering decentralized communication services and tools. These servers are designed to remain accessible should external connectivity be restricted or cut. This support was complemented with advanced threat and Distributed Denial of Service Attack (DDoS) protection to dozens of websites representing key Ukrainian media and CSOs.

Russia

Following the invasion of Ukraine, the Russian government dramatically increased censorship efforts, targeting independent news sites (including RFE/RL and VOA) and social media platforms in particular. As a result, the use of OTF-supported circumvention tools increased from a few thousand users pre-invasion to nearly eight million daily users. In response, OTF provided rapid surge funding to these tools to support increased usage. In addition to censoring independent news and social media platforms, Russian authorities also began censoring Tor in the run-up to the invasion of Ukraine. Due to its circumvention, security, and privacy guarantees, Tor is widely used in Russia to access content censored by the Russian government. In response, OTF supported new circumvention deployment methodologies for Tor, which were further refined and extended post-invasion to ensure that Russians could continue to safely access outside news and information despite new restrictions and legal threats.

Iran

In September 2022, 22-year-old Mahsa Amini was arrested by Iran's Ersahd morality police and died in custody. In response to her death, massive protests against Iran's morality laws erupted across the country. In an attempt to crack down on the protests, the Iranian government quickly shut down mobile networks and internet access across the country and further intensified online censorship, including blocking social media platforms. As a result, the use of the OTF-supported circumvention tools skyrocketed, increasing from five million users per month to over 25 million users. In response, OTF provided rapid surge funding to these tools to support increased usage.



05

Direct Support with FY2021 Funds

Technology at Scale

OTF's Technology at Scale Fund supports the large-scale circumvention and secure communication technology needs of USAGM's networks (Voice of America, Radio Free Europe / Radio Liberty, Office of Cuba Broadcasting, Radio Free Asia, and Middle East Broadcasting Networks). The fund solicits technology solutions that help deliver content to audiences in information-restricted environments and protects journalists and their sources. The fund also ensures that technologies used at scale by millions of users remain secure and effective.

Psiphon Inc.

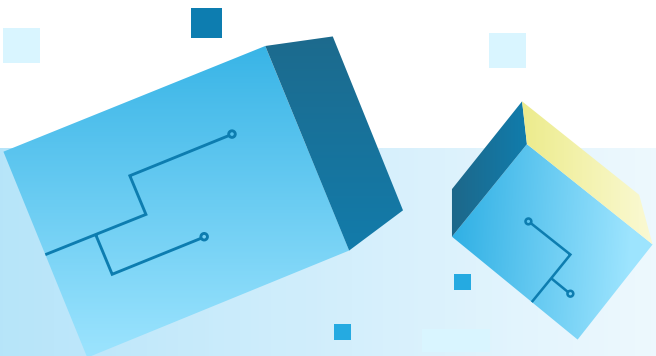
$8,083,938

Psiphon is one of the most technically advanced and widely used circumvention tools in the world, providing millions of users with uncensored access to USAGM content, as well as access to the broader internet. Psiphon's technology uses a combination of secure communication and obfuscation technologies and has proven consistently effective in the world's most highly censored contexts. OTF provided support for SDK (software development kit) services and to support the increased and sustained usage of Psiphon's circumvention tool for those living in repressive environments seeking to access USAGM content.

Lantern

$1,842,780

Lantern is a free internet censorship circumvention tool that delivers fast, reliable, and secure access to the open internet. It provides a way to bypass state-sanctioned filtration through a network of trusted users. Through its mobile application, Lantern's peer-to-peer (P2P) functionality allows mobile users in uncensored regions to provide access to content for users in censored regions. Lantern provides its circumvention technology services to USAGM, allowing for the secure development and distribution of USAGM digital content, and helps facilitate access to USAGM content, as well as access to the global internet. OTF provided funding to Lantern to support the huge increase in monthly users in Russia and Iran.



nthLink

$1,165,975

nthLink is a powerful anti-censorship mobile application capable of circumventing internet censorship and self-recovering from blocking events. It incorporates strong encryption to protect the information flow between the consumer and the source. nthLink aims to create a robust and simple Open Application Programming Interface (API) and Software Development Kit (SDK) for USAGM and other news organizations to integrate their Android and iOS apps with the nthLink censorship circumvention platform to safely and reliably deliver content to at-risk populations in authoritarian regions. OTF provided funding to nthLink to support the nearly 10-fold increase of nthLink monthly users in Russia and Iran. This additional support aided nthLink's response by increasing server instances to support the surge in users.

NewNode

$268,734

NewNode is the first decentralized peer-to-peer content delivery protocol, enabling data distribution free from censorship, spying, and attack. The tool allows users to request and receive internet content using an encrypted, distributed content delivery network (CDN). NewNode allows global media apps censored in their target countries to function as intended, adds communication options for users in countries that tier national and international traffic, and offers greater freedom for anyone living in heavily filtered internet regimes. NewNode provides circumvention technology services to USAGM in the form of a Software Development Kit (SDK), integration, and customer support.

Circumvention Integration in Pangea

$22,610

This project contributes to the development of technologies that provide and enhance access for those using USAGM newsreader apps in censored contexts, ensuring audiences continue to receive USAGM content. The project aids RFE/RL's web app in integrating, testing, and performing maintenance tasks on circumvention Software Development Kits (SDKs) for each of RFE/RL's Pangea web apps to test the performance of Lantern as a possible in-app circumvention solution for censored services using Pangea.

Guardian Project

$1,007,143

The Guardian Project aims to create easy-to-use apps, open-source firmware and software libraries, and customized solutions that can be used around the world by any individual looking to protect their communications and personal data from unjust intrusion. The Guardian Project is using its expertise in the anti-censorship space to help USAGM broadcasters reach their audiences during times of increased censorship and even shutdowns.

Tor Project

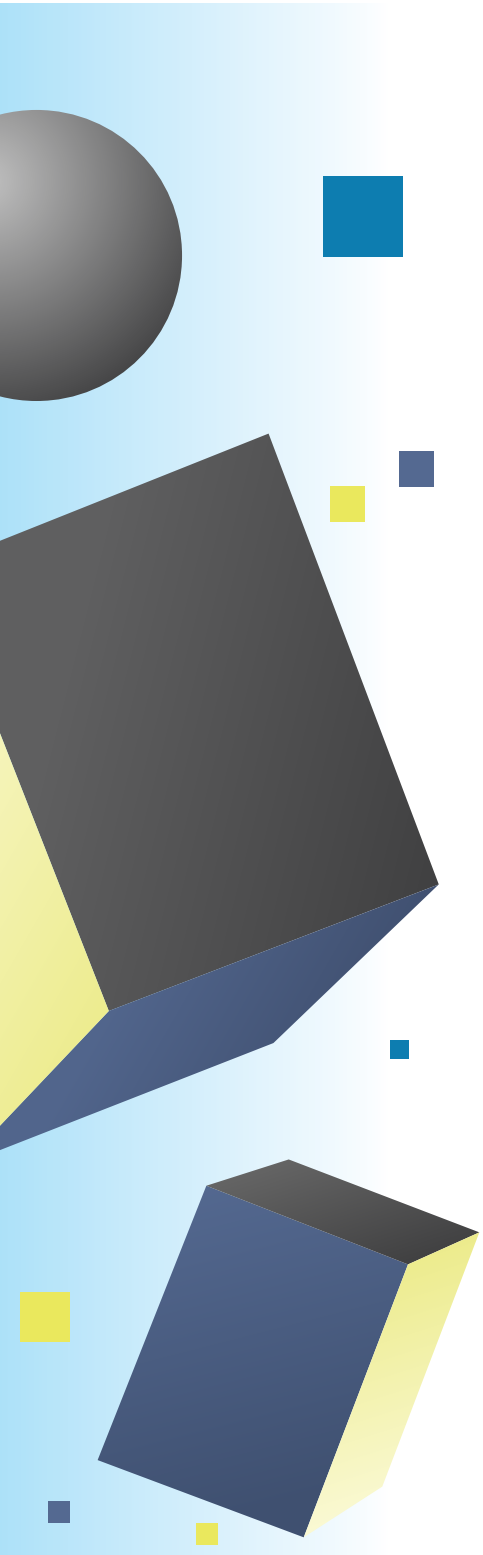
$412,276

Tor, short for "The Onion Router," is a free and open-source software for enabling anonymous communications online. Tor ".onion" web addresses have proven to be one of the most successful mechanisms in overcoming censorship and protecting users' privacy. The Tor Secure Access Package involves a holistic solution for each USAGM entity website and provides an end-to-end solution for USAGM web content to be distributed in censored or surveilled areas.

eQualit.ie

$359,189.96

eQualit.ie creates decentralized internet services and open-source solutions in support of a more equal and equitable network. eQualit.ie provided a white label release of the CENO Browser application for internet shutdown resilience for USAGM entity websites. CENO Browser will serve all USAGM affiliate content over a peer-to-peer network made up of current and future app users, backed by infrastructure for content distribution and web content scraping.



Internet Freedom Fund

The Internet Freedom Fund is the primary fund through which OTF supports innovative global internet freedom projects. IFF projects are primarily focused on technology development implementation but also include applied research and digital security projects. OTF continuously solicits IFF project proposals through a fully open, transparent, and competitive process.

Breakpointing Bad

$19,135

Breakpointing Bad's "*Attacking VPNs to Challenge Basic Security Assumptions*" focuses on increasing the security and privacy of VPNs and VPN-like technologies, which are tools that enable users to send and receive data privately and anonymously. The majority of censorship circumvention, privacy, and anonymity tools work in ways that are essentially VPN-like. The project investigates flaws in VPNs and communicates the findings to at-risk populations, educates users about risks surrounding VPN technologies, and examines potential fixes for VPN issues.

GreatFire

$100,400

GreatFire is an anonymous organization based in China that is monitoring and challenging internet censorship in the country. The organization is helping bring transparency to online censorship in China and focuses on helping the Chinese to access information freely. GreatFire implements the concept of "collateral freedom" by making their technology available to providers who need to unblock their content in China and other countries through a censorship-resilient mobile app that mirrors websites that have been blocked.

FileZilla Server

$22,823

While many ways exist to transfer files online, Secure File Transfer Protocol (SFTP) remains the most private and secure protocol for file transfer and is still relied on by many users in countries without free internet. FileZilla Server is a tool that enables people to use SFTP to transfer files confidentially. This project aims to introduce security, privacy, and usability improvements to the FileZilla Server software through Let's Encrypt integration, user impersonation, user documentation, and other deliverables.

Article 19 (Internet Freedom Festival)

$307,822

The Internet Freedom Festival (IFF) brings together activists, journalists, developers, humanitarian workers, and others working on freedom of expression, privacy, and security from around the world to improve coordination, collaboration, and information sharing across the internet freedom community. Despite challenges due to the COVID-19 pandemic, IFF still hosted numerous virtual discussions and convenings to support continued collaboration among groups and individuals working on internet freedom issues, including discussions on VPN standardization as well as regional convenings focused on internet freedom developments in Africa, Asia, the Middle East, and Latin America.

Stitching Global Voices

$5,090

Localization plays an important part in the adoption and safe use of internet freedom technologies. Global Voices seeks to map and document the language-related challenges facing their existing networks of frontline digital activists from dozens of communities working in under-resourced languages. This includes both indigenous and other minority languages in Latin America, Africa, and Asia. The project will produce 18 case studies featuring a select group of language communities to provide nuanced analysis and accompanying infographics summarizing the research findings.

Trustees of Indiana University (Observatory on Social Media)

$217,423

As people around the world gain greater access to critical news and information through social media, the vulnerabilities of these platforms and their users to abuse and manipulation through inauthentic actors and coordinated disinformation campaigns are posing a critical threat. To help mitigate these vulnerabilities, the Observatory on Social Media aims at lowering the entry barrier for social media researchers, journalists, and the general public to research online disinformation and manipulation. The project seeks to develop accessible and feature-rich versions of Botometer, Hoaxy, and BotSlayer—a free and open suite of tools for the detection, interactive visualization, and analysis of social media data. Botometer checks the activity of a Twitter account and analyzes its behavior to determine how likely it is that account is automated. Hoaxy allows individuals to visualize the spread of claims and fact-checking from account to account on Twitter. BotSlayer is an application that helps track and detect potential manipulation of information spreading on Twitter.

Protecting At-Risk Populations in Asia from Surveillance, Censorship, and Targeted Attacks

$246,654

Protecting At-Risk Populations from Surveillance, Censorship, and Targeted Attacks is a reverse-engineering effort implemented by Arizona State University Foundation for A New American University in partnership with TibCERT. The project aims to study everyday mobile applications in East and Southern Asian app markets through phylogenetic clustering of similar apps and directly engage local partners to scale up analysis, identify risky apps, and educate at-risk users. The project is focused on three types of problematic behaviors: *(1)* insecure update mechanisms that could be exploited via a man-in-the-middle attack, *(2)* poor crypto that puts private user data at risk, and *(3)* keyword-based censorship or surveillance baked into an app.

Fake Antenna Detection Project (FADe)

$111,042

FADe aims to address repressive surveillance and monitoring of private cell phone communications of journalists and human rights defenders in Latin America by testing and measuring the potential presence and use of International Mobile Subscriber Identity (IMSI) data across various devices. The project uses SeaGlass, a system designed to measure IMSI-catcher use across a city, and will engage in advanced technical testing, research, and data collection in various countries to help communities understand the threat environment, ultimately allowing for a better digital safety approach.

Social Media Exchange (SMEX)

$50,001

Bread&Net is an annual conference that promotes and defends internet freedom across Arabic-speaking countries in the Middle East and North Africa. The event, hosted by Lebanon-based SMEX, is built for and sustained by hundreds of activists, technologists, journalists, researchers, lawyers, academics, entrepreneurs, and human rights defenders worldwide. The project aims to bring experts together to share knowledge and experience and advocate for internet freedom.

Icarus Project

$113,734

Icarus Project is a technical research laboratory dedicated to testing, analyzing, documenting, and developing internet censorship circumvention solutions. The project aims to collect as many circumvention techniques as possible and document them in the forms of technical analysis and step-by-step implementation guides and will explore and test a variety of solutions with targeted media.

Azerbaijan Internet Watch

$78,676

Azerbaijan Internet Watch (AIW) was launched in 2019 to track Azerbaijan's internet freedom landscape in real time. Since then, the platform has published numerous documented cases and investigations of information controls in Azerbaijan. The goal of this project is to examine how relevant institutions in Azerbaijan restrict information and deploy censorship mechanisms, offer reliable data for relevant audiences and stakeholders, and support individuals and civil society organizations in the country to combat censorship.

Building a Global Surveillance Database

$16,075

Recent crackdowns in Hong Kong, Myanmar, and Bangladesh have shown how surveillance technologies sold by private companies are being used by government agencies to monitor and repress activists, journalists, and political opposition. This project aims to develop a database of information on the surveillance industry and will include comprehensive and up-to-date information on what types of surveillance technology are on the market, which companies are selling them, which governments are supporting their use, and where they are being used. The database will increase transparency, inform key stakeholders, and spur activism, ultimately leading to better human rights protections for people around the world.

PiRogue Tool Suite

$152,370

PiRogue Tool Suite (PTS) is an open-source tool suite that provides a free and comprehensive network traffic analysis platform that targets Android and iOS mobile devices, Android mobile apps, internet-of-things devices (devices that are connected to the mobile users' apps), and any device using WiFi to connect to the internet. Capturing, reading, and analyzing network traffic is a difficult technical task—PTS makes this process easier by clarifying what (and to whom) data and network traffic is collected, sent, and received by a device when it is being used.

SMS Without Borders

$93,226

SMSWithoutBorders is an open-source platform that enables secure communication with online services using SMS messages in the event of an internet shutdown. The project aims to provide journalists and activists experiencing internet shutdowns with an alternative form of secure communication via SMS messaging.

VPNalyzer

$161,281

VPN usage is growing rapidly among internet users due to increasing awareness of online censorship, adversarial networks, security and privacy risks, massive data breaches, and geographic restrictions. VPNalyzer is a tool that conducts a systematic and automated investigation into the unregulated VPN ecosystem. This project aims to further develop VPNalyzer's capabilities, increasing the breadth and representation of studied VPN services to help identify potential areas for technologists, security, and privacy experts to focus their efforts on protecting users.

GFW Analysis

$6,000

Analyzing and documenting information on China's "Great Firewall" is key to advancing our understanding of how censorship occurs inside China. This project provides an analysis of internal documents related to China's "Great Firewall," identifying numerous underlying aspects of Chinese censorship, including the speed at which information is censored, the techniques utilized, and the associated gaps as a result of those techniques.

Divvi Up

$845,444

Most internet applications generate metrics about their users. Such metrics are valuable for application owners because they are the basis for insights into users' behaviors; however, for most user data, there are insufficient privacy safeguards. The Internet Security Research Group aims to provide an easy-to-use service that application owners—from government and public benefit entities to private companies—can use to easily collect user population metrics while respecting user privacy. This project will develop a specification that will eventually become an internet standard that can be adopted by anyone, with the potential to dramatically improve users' privacy across the entire internet.

Tella

$215,060

Tella is a human rights documentation tool that allows users to hide and encrypt sensitive material in a secure container on their mobile device and securely send it to the servers of the organization or partner they are working with. Tella is already in use by at-risk individuals and groups to protect themselves from repressive surveillance as they document rights violations and injustices. This project aims to improve the performance and maintainability of Tella on Android, achieve feature parity between iOS and Android for security and privacy features, and improve Tella's security and privacy across all versions of the tool.

Project Phoenix

$387,085

Project Phoenix seeks to design, spec, and implement all vital components of a modern, private, and secure messenger. It is designed to support the needs of activists, journalists, human rights defenders, and other vulnerable groups and fill the gaps present in other secure messengers. The tool is based on the new Messaging Layer Security (MLS) protocol and aims to combine Signal's metadata minimalism with Matrix's federation features and Wire's username-based approach and ease of use.

nthLink Multi-Protocol Architecture

$181,000

The nthLink team, who have helped USAGM journalists and audiences stay online, is experiencing increased blocking from censors in China. This project will develop a new multiprotocol architecture that incorporates the strength of V2Ray (a protocol for building proxies to bypass network restrictions) to create a robust circumvention service with strong blocking recovery, scalability, and high availability.

Venezuelan Cyber Dialogue

$32,592

The Venezuelan Cyber Dialogue is a community convening of civil society activists, technologists, journalists, and allies to share knowledge and strategies in an interdisciplinary environment. The convening covered multiple topics, including digital attacks on individuals and the press, biometrics, cell phone surveillance, and censorship. Organizers also built a digital security toolkit for community activists in Venezuela and other high-risk areas.

Forum on Internet Freedom in Africa (FIFA)

$74,240

The Forum on Internet Freedom in Africa is a landmark event hosted by the Collaboration on International ICT Policy for East and Southern Africa (CIPESA). The Forum convenes a spectrum of stakeholders from across the internet governance and digital rights arenas in Africa and beyond to deliberate on gaps, concerns, and opportunities for advancing privacy, free expression, the free flow of information, civic participation, and innovation online. OTF supported multilingual digital security clinics and skills workshops at FIFA, allowing participants to access new innovative internet freedom technology, privacy and data protective tools, measurements, and platforms in order to respond to their emergent digital security concerns.

Secure UX Workshops

$15,372

Designers at Secure UX are creating curricula and an accessible website that will teach individuals about design and security in plain terms. The Secure UX checklist is a methodology and taxonomy designed as a how-to guide for researchers, engineers, product managers, designers, and teams who are working with journalists, civil society, and high-risk communities. It includes a series of actionable best practices and guidelines for those who build tools for and with human rights communities from the ideation stage through to the finished product.

USAGM Entity Support

eQualit.ie

$33,845.50

eQualit.ie provided urgent digital security training to RFE/RL in the form of three 2-day workshops for journalists and staff members, focusing on raising awareness of existing digital security risks in various aspects of their work, including online communications, document storage, device integrity, and in-the-field assistance.

Rapid Response Fund

OTF's Rapid Response Fund (RFF) provides emergency support to independent media outlets, journalists, and human rights defenders facing digital attacks. The support through this fund helps these individuals and groups stay safe in repressive environments, regain online access, mitigate future attacks, and combat sudden censorship events.

In FY2021, OTF facilitated timely and comprehensive emergency responses around the world. OTF provided security audits, website sanitation, secure hosting, security protocol improvements, and more to civil society organizations while also providing direct funding for in-country internet freedom support. OTF's Rapid Response support is global and has supported activities in Russia, Ukraine, Iran, Afghanistan, Philippines, Myanmar, Egypt, Hong Kong, Tibet, and more.

OTF works exclusively with community partners who are highly sensitive to and well aware of the specific needs and challenges of human rights activists, journalists, and the internet freedom community. To respond to requests as quickly as possible, OTF maintains ongoing contracts with partners to provide the following services.

Cooperativa Tierra Comun

$150,000

Tierra Comun provides organizational security and digital security support. This includes digital security audits for organizations, urgent risk mitigation, rapid assessment and crisis response planning, organizational security improvements, and digital security mentoring.

Greenhost

$147,872.46

Greenhost provides hosting and data privacy services for the internet freedom community. Greenhost's Rapid Response web hosting services include clustered web hosting, cloud platforms, Deflect anti-DDoS protection (Distributed Denial-of-Service Attack protection), Infrastructure as a Service (IAAS), and real-time monitoring.

Labs

OTF provides support to existing internet freedom projects through the organization's Resource Labs (Labs), which aid the internet freedom community in tackling the diverse nature of challenges posed by authoritarian governments. These resources assist the relatively common needs for tools and technologies operating in this space and include items such as secure hosting, code audits, communications and localization assistance, usability design, and more. OTF's Labs provide these expert services to the internet freedom community through its offerings: Red Team Lab, Secure Usability & Accessibility Lab, Localization Lab, and Learning Lab. These services ensure that the technologies incubated and supported by OTF are as effective, secure, and usable as possible.

Red Team Lab

The Red Team Lab offers services that look to strengthen the security of open-source internet freedom software by providing security audits, advancing projects' software security best practices, validating privacy and security claims of projects, and more. By focusing on improving the software security of projects that advance OTF's internet freedom goals, supported projects can ensure that the code, data, and people behind each project have the tools they need to create a safer experience for those experiencing repressive information controls online.

Include Security

$250,000

Include Security has worked with numerous clients on more than 200 security assessments. Working with a wide range of companies, Include Security specializes in Grey Box security assessments which allow consultants to be significantly more efficient in finding vulnerabilities. Grey Box assessments are conducted where the consultant has access to both a working instance of an application and the source code for the application. Include Security aids OTF and its projects by providing security services for web applications, cryptography services, and adversarial audits.

Cure53

$250,000

Cure53 offers penetration tests for online services, security analysis and architectural advice, training and consulting, incident management, and web malware analysis. Through the Red Team Lab, Cure53 performs professional audits of programming code, offers penetration testing of systems and networks, and provides detailed reports of their findings.

Radically Open Security

$250,000

Radically Open Security, a nonprofit computer security consultancy, aids OTF as a Red Team Lab vendor by providing professional audits of programming code, penetration testing of systems and networks, organizational and operational security training, and providing detailed reports on findings alongside recommended solutions. Radically Open Security's unique nonprofit business model supports transparency, openness, and giving back to the community.

Subgraph Technologies

$250,000

Subgraph is an open-source security company with specialized experience in application security. As a Red Team Lab partner, Subgraph supports the security needs of OTF-supported projects and projects from the broader internet freedom community through security audits and penetration testing based on well-established principles from the security and cryptography industries.

7ASecurity

$250,000

7ASecurity is a EU-based and GDPR-aware team of highly skilled security professionals who produce short and to-the-point penetration test reports with proven security vulnerabilities. 7ASecurity has performed hundreds of penetration tests against all kinds of web applications, online services, hardware interfaces, mobile applications, libraries, and crypto tools. 7ASecurity efforts support OTF's commitment to establishing high-level internet freedom technology privacy and security standards.

Eaton Cybersecurity SAFE Lab (Rochester Institute of Technology)

$250,000

The RIT's Global Cybersecurity Institute educates and trains cybersecurity professionals; develops new cybersecurity and AI-based knowledge for industry, academia, and government; and performs systems and network security testing for a wide range of partners. As a designated Center of Academic Excellence in Cyber Defense and the home of America's National Technical Institute for the Deaf, RIT is committed to building a diverse and inclusive cybersecurity workforce. SAFE Lab helps OTF projects by providing security services for various software applications, cryptographic services, adversarial audits, and detailed reports of the findings and recommended solutions.

Trail of Bits

$250,000

Trail of Bits helps secure some of the world's most targeted organizations and products. They combine high-end security research with a real-world attacker mentality to reduce risk and fortify code. Their mission is to find better bugs, be better code reviewers, and engineer safer cryptography. Trail of Bits assists OTF and its projects by providing numerous privacy and security opportunities, including cryptography services, adversarial audits, forensic audits, and general security services.

Learning Lab

The Learning Lab helps OTF-supported projects capture, communicate, and share their research, analysis, and findings. These can take the form of final research write-up reports, editing of applications and websites, and helping OTF-supported projects and fellows as their projects come to a close. The Learning Lab provides graphic design and visualization assistance for when improved user interface or user experience enhancements are warranted and provides communications training services.

John Stith

$300,000

Providing writing and copywriting services, editing services, and written communications contributions in support of OTF's Learning Lab.

3 Bridges

$300,000

Through strategic communications planning, writing, and editing, 3 Bridges helps OTF projects and fellows find vivid narratives in their work in both single documents and overall strategies.

Christy and the Moon Tide Collective

$300,000

Christy and the Moon Tide Collective assists the Learning Lab with writing, editing, and strategic communications services.

Superbloom

(formerly Simply Secure)

$300,000

Superbloom is a nonprofit focusing on building technology that enhances and protects human rights by centering the needs of marginalized populations. They are experienced design professionals, supporting projects around developing materials essential to communicating results. Superbloom provides graphic design, visualization assistance, and communications training to OTF-supported projects.

Ura Design

$300,000

Ura Design is an open-source design collective focused on secure and privacy-preserving software projects, accessibility support, UX design, user research, and visual design services. Ura Design provides graphic design, visualization assistance, and communications training to the Learning Lab.

Secure Usability and Accessibility Lab

The Secure Usability and Accessibility Lab (SUA Lab) offers secure usability and user-interface assistance to internet freedom and digital security tools to help them recognize and solve usability challenges that could undermine the adoption of their tools. OTF partners with service providers that offer secure usability and accessibility coaching, consultation, and audits that help the advancement of the internet freedom community and the accumulation of practical knowledge through peer-to-peer learning.

Okthanks

$200,000

Okthanks works to advance human rights through the design of software and technology, providing support for activists and journalists living in repressive environments where censorship and surveillance lead to marginalization and violation of basic human rights. OKThanks provides support for usability testing for early-stage prototypes and existing applications, user experience design, and accessibility audits.

Superbloom

(formerly Simply Secure)

$200,000

Superbloom is a nonprofit focused on building technology that enhances and protects human rights by centering the needs of marginalized populations. Superbloom works with practitioners to expand their skill set around human-centered design, helping to solve design challenges. Superbloom provides usability audits, UX reviews, user research, and strategy consultations.

Ura Design

$200,000

Ura Design is an open-source design collective based in Albania, focused on secure and privacy-preserving software projects, accessibility support, UX design, user research, and visual design services. Ura Design provides visual identity and brand strategy support, usability reviews, and UX design.

Accessibility Lab (A11y Lab)

$200,000

A11y Lab works to ensure the inclusion of people with disabilities and their integral development through accessibility in the digital world. A11y Lab's services include accessibility training and guidance creation for web content accessibility, digital document remediation, and accessible software development.

Plaintext Design

$200,000

Plaintext Design is a UX collective specializing in internet freedom technologies. Plaintext works with developer teams across various domains and software layers to help projects where they are on their UX journey. Plaintext Design's support includes UX research and discovery, UX content and interface design, and UX coaching.

Localization Lab

$1,093,620

The Localization Lab provides localization support to internet freedom tools, including translating tools into over 200 languages for different countries and regions. Addressing a major challenge for internet freedom technologies of reach and adoption, this lab helps adapt internet freedom tools that are relevant and appropriate for another country or culture. OTF's Localization Lab partners utilize a vast community of translators able to provide scalable translation platforms for large or small diverse projects.

Engineering Lab

$183,000

The Engineering Lab focuses on supporting the implementation and inclusion of established technologies into existing applications, organizations, and communities that are advancing internet freedom, supporting the operating and infrastructure costs associated with tool and resource deployment, and conducting assessments of existing apps or websites for recommended privacy, security, and anti-censorship improvements.

Information Controls Fellowship Program

The Information Controls Fellowship Program (ICFP) supports research efforts to examine how authoritarian governments are restricting the free flow of information and to explore solutions to overcome these evolving tactics. Fellows receive a monthly stipend and a small travel budget that varies based on the length of their fellowship.

OTF supported eight ICFP fellows with FY2021 funds. The group will focus on advancing research, analysis, and tool development on topics related to internet censorship. This includes research on potential or existing circumvention techniques, the use of circumvention tools during censorship events, mitigating security vulnerabilities in access and privacy tools, identifying the specific tools used in individual countries for information controls, and more.

Benjamin Mixon-Baca

Host Organization: *Censored Planet, University of Michigan*

Duration: *Twelve months*

Lack of transport security where an attacker can spy on personal identifiable information (PII) and inject malware into a machine is an immense and underestimated threat to at-risk users because they operate in environments where the attacker controls the network infrastructure. While there have been efforts to analyze this lack of transport security, they typically do so either on a per-app basis, are not automated, or require some pre-existing knowledge of the apps being analyzed.

To fill this gap, Mixon-Baca developed CryptoSluice, a tool to automatically analyze potentially insecure applications that use poor or no encryption in the transport layer, in an ethical way—that is, without also extracting PII that would normally violate user privacy—and without the need for preexisting knowledge from the part of the analyst.

Ramakrishnan Sunday Raman

Host Organization: *Citizen Lab*

Duration: *Seven months*

While censorship technologies have advanced, techniques to identify and monitor them are still limited, and are developed on a case-by-case basis. To address this, Raman developed a set of network measurement methods to locate and examine devices performing censorship, and to measure their deployment in different countries. This measurement toolkit identifies devices scalably through passive and active measurement techniques.

Running case studies in Azerbaijan, Belarus, Kazakhstan, and Russia, Raman's work identified that censorship policies are often deployed in networks that are upstream to the user—sometimes even in a different country—and that many devices manufactured by commercial vendors such as Cisco and Fortinet are used for censorship. In addition, the project identified similarities and differences in the behaviors of these devices.

The tools developed through this project are fully open source and can be used to monitor the proliferation of censorship devices in different countries.

Michael Collyer

Host Organization: *Oxford Internet Institute*

Duration: *Twelve months*

The language surrounding internet shutdowns and how they fit into the broader field of information control warrants further research. In order to better understand the types of internet shutdowns and the existing resources and data, Collyer proposed a framework for types of internet shutdowns, and one for grouping existing taxonomies surrounding shutdowns. The goal was to simplify the language and classification of this phenomenon. He also created an interactive shutdown database to centralize shutdown data to highlight the value of data triangulation and make it easier for future researchers to carry out analysis.

Gurshabad Grover

Host Organization: *Open Observatory of Network Interference*

Duration: *Twelve months*

Grover's research examined jurisdictions with decentralized information controls. In these jurisdictions, internet service providers (ISPs) and other infrastructure providers are responsible for implementing government orders for censorship. ISPs' technical and policy decisions can exacerbate or minimize the effect of state-directed censorship. Historically, much of the literature on internet censorship and measurement has tended to focus on jurisdictions with centralized information controls, such as China. Grover's research shed more light on how internet censorship plays out in South Asian countries with a decentralized approach.

The project uncovered how ISPs in India are engaging in arbitrary blocking of websites, and using opaque techniques of blocking that hide critical information from internet users. Grover also studied the efforts of authorities in Pakistan to centralize infrastructure for censorship, and the effects of Indonesian regulations that allow ISPs to block websites at their own discretion.

Kathrin Elmenhorst

Host Organization: *Open Observatory of Network Interference*

Duration: *Three months*

QUIC is a fast growing, new internet protocol which uses encryption by design and is the transport for HTTP/3. Elmenhorst's fellowship focused on measuring the level and type of QUIC censorship in various countries, and exploring approaches for circumventing this method of censorship—the protocol has promising potential for circumvention since it's implemented on the application layer. Investigating networks in China, India, Iran, Kazakhstan, Russia, Uganda and Venezuela, Elmenhorst found impairment of HTTP/3 traffic in most of these countries, while the censorship techniques varied between networks.

She created a repository documenting known QUIC censorship methods and observed cases of HTTP/3 censorship, an analysis of QUIC features that can be used for censorship evasion, and building blocks for (automated) QUIC censorship evasion.

Ain Ghazal

Host Organization: *Open Observatory of Network Interference*

Duration: *Twelve months*

While many users rely on VPNs for improving their privacy online, reducing their personal exposure, and bypassing censorship, interference with VPN traffic is a growing trend. More, better data and accurate models of censor behavior will help to improve circumvention. To this end, Ghazal contributed to ongoing research to quantify censor interference over VPN connections, improving existing metrics and performing novel experiments.

The fellow collaborated with the Open Observatory of Network Interference (OONI) on a proposal for a new data format enabling OONI to receive external reports about VPN failure rates, intended for VPN providers to aggregate and submit reports from their client apps. This cross-actor gathering of real-time intelligence about censor capabilities can help circumvention tools prepare for future blocks in a genuinely resilient way.

Mona Wang

Host Organization: *Citizen Lab*

Duration: *Nine months*

With over 1.2 billion monthly active users, WeChat is the most popular messaging and social media platform in China and the third most popular messaging app in the world.

For vulnerable populations that must use WeChat (for instance, domestic journalists and foreign correspondents, grassroots and diaspora activists), precise threat modeling is of utmost importance. This kind of risk assessment requires a more granular security and privacy analysis to understand the shape and nature of the risks. During her fellowship, Mona will reverse-engineer WeChat's custom transport-layer encryption protocol and provide tooling for other researchers to intercept and decrypt network traffic. She will use this tooling to perform an in-depth security and privacy review of the application, including an analysis of popular MiniPrograms on the WeChat application ecosystem.

Hamas Bin Tanveer

Host Organization: *Censored Planet*

Duration: *Six months*

During the course of this fellowship, Hammas aims to understand the censorship mechanisms around Tor bridges over IPv6. His previous work has revealed that there are censorship implementation gaps between DNS over IPv4 and IPv6, resulting in lesser DNS censorship over IPv6. This fellowship aims to find similar censorship gaps between Tor bridges over IPv4 and IPv6 and explore the possibility of creating censorship-resistant Tor bridges using the vast address space of IPv6.

OPEN TECHNOLOGY FUND

2021

ANNUAL REPORT