OPEN TECHNOLOGY FUND

FY 2022

ANNUAL REPORT

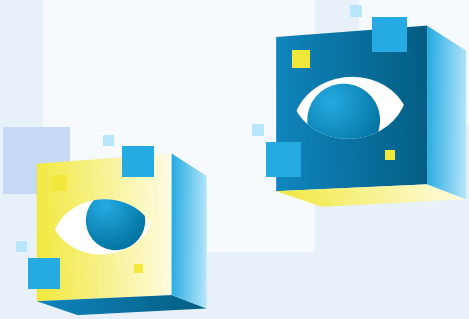
Table of Contents

Layout design by Ura Design

OPEN TECHNOLOGY FUND

Learn more about OTF at opentech.fund.
Follow us on X (formerly Twitter) and LinkedIn.

@OpenTechFund @Open-Technology-Fund



A Fragmented Future?: The Global Internet at Stake

Once considered politically extreme and technically implausible, digital authoritarianism is now embraced worldwide as more and more countries are rejecting the promise of a free and open internet. In an audacious attempt to extend dominance beyond geographic borders, we see authoritarians going to extremes to impose on the global internet the same level of absolute control they expect to wield domestically. As a result, the fight for internet freedom is no longer simply a tactical cat-and-mouse game but rather a normative battle to define the future of free expression.

> ***"The fight for internet freedom is no longer simply a tactical cat-and-mouse game but rather a normative battle to define the future of free expression."***

Authoritarian governments around the world are harnessing technological advances to increase the scale, scope, and efficiency of digital repression. Online censorship is more sophisticated and widespread than ever—with an increasing number of governments blocking more content than ever before. A clear indicator of this trend is skyrocketing demand for VPNs. In the past, only those living in the most information restricted environments needed VPNs to access a limited number of censored websites. Today, VPNs are an essential prerequisite for tens of millions of people around the world to access the totality of the global internet.

On top of this, the commercial availability of advanced, population-scale surveillance capabilities and the normalization of their use by committed state actors, is making civil society more vulnerable than ever before. Once only available to a small number of well-resourced autocrats, highly advanced surveillance technologies are now widely accessible to nation-states and other illiberal non-state actors around the globe. Over the last decade, at least 75 countries—nearly 40 % of all nations—have acquired commercial spyware, giving rise to a mercenary spyware industry now worth billions that jeopardizes the security of journalists and human rights defenders worldwide.

Beyond deploying new, more sophisticated censorship and surveillance technologies, repressive regimes are also committing significant time and resources to fundamentally reshape the internet to match their vision of control. Authoritarians, led by China and Russia, are now attempting to reconfigure and manipulate foundational elements of the internet to undermine its interoperability and security, effectively redesigning the internet from its very core to enable control rather than connection.

The rapid acceleration of digital authoritarianism can be attributed largely to autocratic learning. Put simply, authoritarians are increasingly iterating on and sharing censorship and surveillance techniques and technologies with one another. While this has implications for both the speed and effectiveness of deployment, it critically normalizes expansive information controls, threatening the very principles on which internet freedom is premised.

As a result, there is no longer a meaningful distinction between digital authoritarianism and authoritarianism of any other kind as online information control has become foundational to illiberal governance. Internet freedom cannot be wholly differentiated from the broader fight for human rights and free expression, because it is an integral part of how these will be actualized.

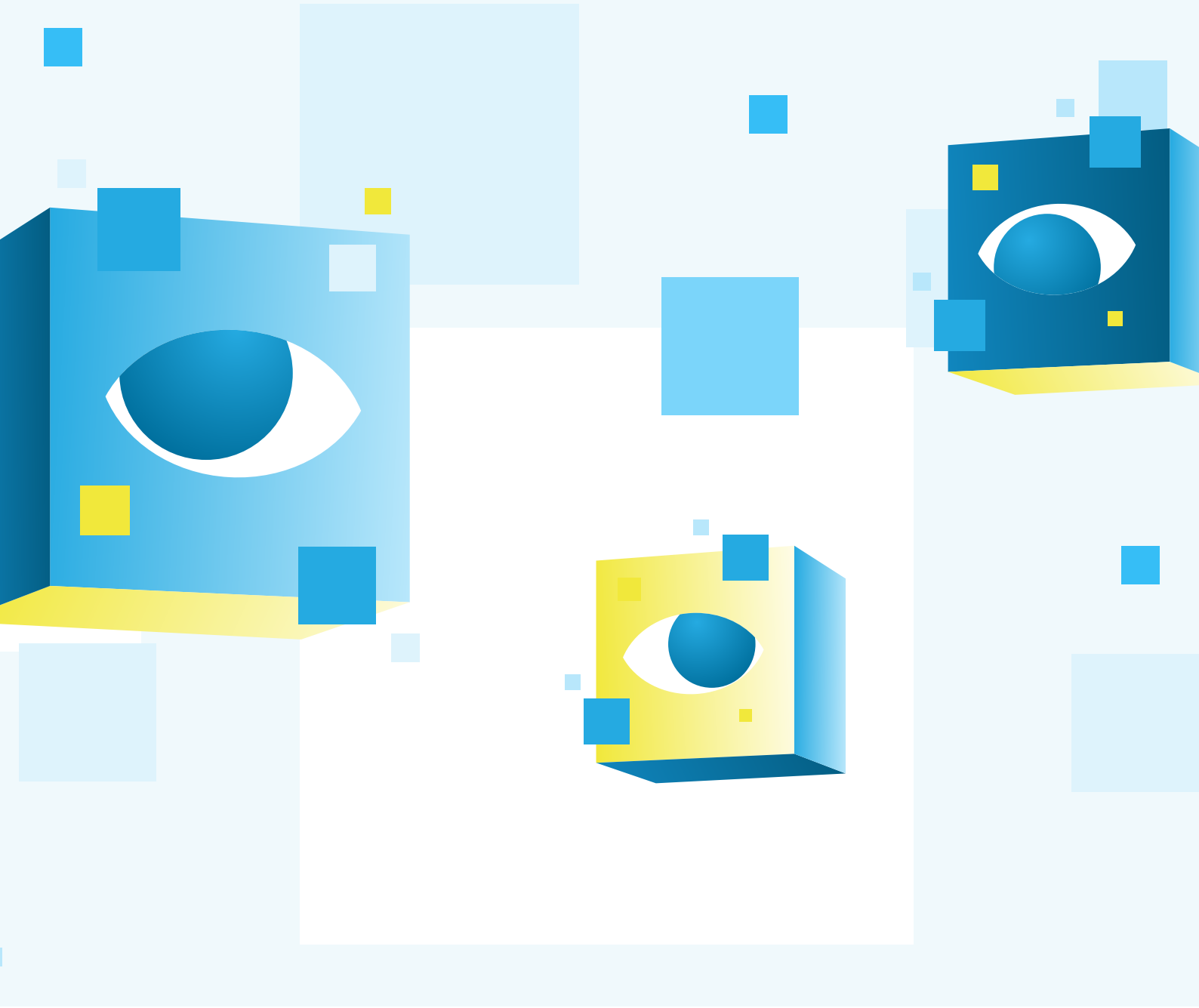
What does this mean as we look ahead?

The stakes have never been higher. As authoritarians become more dogged and ambitious, protecting and preserving a free and open global internet will be more difficult, more expensive, and far from guaranteed. We need to be prepared for evermore complex and challenging fights—and ready to take bold action.

Most importantly, as digital authoritarians continue to unite in their efforts to undermine the very concept of a free and open global internet, so must we unite in dedication to its defense by supporting those in the vanguard. Because in the face of an increasingly uneven playing field, our combined creativity, shared vision, and tenacious commitment is our greatest strength.

This annual report catalogs the projects that OTF has supported over the past year, but more importantly, it captures the incredible effort and accomplishments of our partners. We are proud to support this critical work and look forward to working together to amplify the strength and impact of our community to meet the challenges ahead.

Laura Cunningham
President, OTF



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 January 2023 through December 2023 with fiscal year (FY) 2022 funds.

02 About OTF & Its Mission

OTF is a congressionally authorized, independent nonprofit organization that advances internet freedom in repressive environments by supporting the applied research, development, implementation, and maintenance of technologies that provide secure and uncensored access to the free and open internet. For over ten years, OTF has supported pioneering open source internet freedom technologies that counter authoritarian information controls and enhance digital security and privacy so that all people can exercise their fundamental human rights online. Today, over two billion people around the world use OTF-supported technology on a daily basis, and more than two-thirds of all mobile phone users have OTF-incubated technology on their devices.

OTF supports projects to:

- **Provide unrestricted access to the internet to individuals living in information-restrictive countries** to ensure they are able to safely access the uncensored internet. This includes supporting the development and deployment of circumvention technologies to counter increasingly sophisticated censorship techniques, the incubation of new solutions to counter internet shutdowns, and the advancement of applied research to help tool developers and users stay ahead of new censorship threats.
- **Protect journalists, human rights defenders, and at-risk communities from repressive surveillance and digital attacks** to 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-enhancing technology.

2 Billion

People using OTF-supported technology daily

2/3

Mobile phone users with OTF-incubated technology

03 OTF's Approach

OTF provides direct funding and support services to individuals and organizations around the world that use technology-backed solutions to address threats to internet freedom, media freedom, and human rights. The organization offers 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 the majority of projects on a rolling and competitive basis via public open calls. The process is designed to reduce application barriers to make funding more accessible to qualified individuals and organizations around the world. OTF's process attracts innovative applications from groups that traditionally are unable 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 through which successful applications are ultimately improved and refined. To provide further feedback and guidance, all proposals are reviewed by OTF's specialized staff of subject matter experts as well as OTF's Advisory Council—a volunteer group of technical, regional, and specialized experts from a wide range of relevant disciplines. 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.

04 OTF's Programs

OTF implemented the following funds, labs, and fellowship programs in 2023 to fulfill its mandate in support of global internet freedom.

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 provided resources to innovative global internet freedom projects, large-scale circumvention and secure communications technologies, and emergency support mechanisms. These funds included:

Internet Freedom Fund

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

Technology at Scale Fund
(transitioned to the Surge and Sustain Fund in 2023)

The Technology at Scale Fund supports the large-scale circumvention and secure communication technology needs of the U.S. Agency for Global Media's broadcasting 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 can deliver content to audiences in information-restricted environments and protects journalists and their sources. It 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. Support through this fund helps individuals and groups stay safe in repressive environments, regain online access, protect against future attacks, and combat sudden censorship events. The fund also provides rapid support to address new software vulnerabilities—including the development and deployment of emergency technical patches—to ensure critical internet freedom tools remain secure.

Resource Labs

OTF provided support to internet freedom projects through the organization's Resource Labs (Labs). Expert services, solicited through competitive processes, are offered to the internet freedom community through the Learning Lab, Red Team Lab, and Secure Usability and Accessibility Lab.

Together, these Labs ensure the technologies incubated and supported by OTF are as effective, secure, and usable as possible.

Learning Lab

OTF's Learning Lab provides communications support to tell the stories of OTF-supported projects and the results they produce. This Lab also facilitates knowledge sharing and collaboration across the internet freedom community.

Red Team Lab

The Red Team Lab conducts independent security audits of internet freedom technologies to improve the security of projects and ensure a safer experience for people using these in repressive environments. 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 and accessibility of open source circumvention and digital security technologies. The Lab supports software development teams in the creation and improvement of projects designed to help journalists, human rights defenders, and their audiences communicate privately and securely. Services include secure usability and accessibility coaching, consultation, and audits.

Fellowships

OTF supports individuals in carrying out cutting-edge applied research that examines how digital authoritarians restrict the free flow of information online—and how these tactics can be overcome. OTF fellowships help cultivate the next generation of digital rights experts by creating a career track for those who have the skills and passion for internet freedom.

Information Controls Fellowship Program

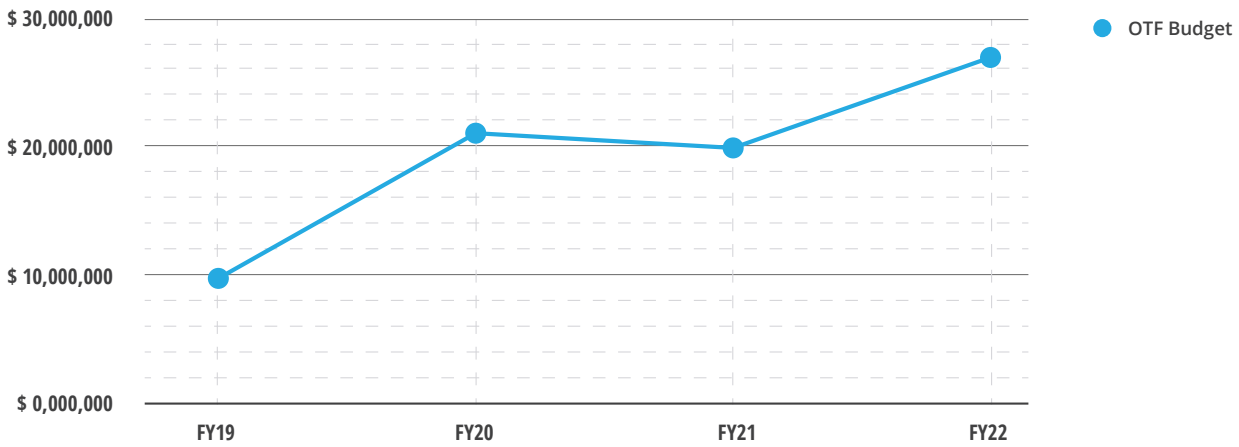
The Information Controls Fellowship Program (ICFP) supports research examining the means by which authoritarian governments restrict the free flow of information online and the solutions to overcome these evolving and repressive tactics.

05 OTF's Funding

OTF is a grantee of the U.S. Agency for Global Media (USAGM) and is funded by the U.S. congressional appropriations process 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 USAGM submits to Congress an Internet Freedom Spend Plan 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 FY 2022, Congress allocated $77.5 million for programs to promote internet freedom globally, representing a $7.5 million increase from FY 2021. Of the funds allocated for internet freedom, $27 million was designated for OTF through USAGM. OTF's FY 2022 budget allocation—an increase of roughly $7 million over the organization's previous fiscal year allocation—reflects a bipartisan recognition of the importance of OTF's work in advancing internet freedom in repressive environments and securing digital rights around the world.

OTF Budget Growth Over Time



06 Threats to Internet Freedom

Global internet freedom declined for the 13th consecutive year and attacks on free expression grew more common around the world during the time period covered by OTF's FY 2022 appropriations.[1] While continuing to rely on conventional and blunt forms of censorship, authoritarian regimes also harnessed artificial intelligence (AI) technology to increase the scale, speed, and efficiency of digital repression. Internet shutdowns additionally proved pervasive and prosecution of free online expression became increasingly common.

In a troubling development, authoritarians are also increasingly learning censorship and surveillance techniques from one another—and nowhere is this more apparent than in China and Russia. Documents leaked in 2023 reveal growing cooperation between the two governments on how to best stifle dissent and control information.[2] Russian officials are keen to learn from their Chinese counterparts how to disrupt circumvention tools like VPNs, crack encrypted internet traffic, and regulate messaging platforms.[3] In exchange, Chinese officials seek expertise on regulating media and managing popular dissent.[4]

The widespread use of the repressive censorship and surveillance threats detailed below—and particularly the manipulation of the rule-of-law to criminalize online expression—further confirms that censors are now taking cues from each other when it comes to restricting internet freedom.

AI Continues to Supercharge Censorship & Surveillance

Developments in AI technology continue to increase the scale, speed, and efficiency of censorship and surveillance. Sophisticated surveillance systems trawl social media for "undesirable" content. Biometric surveillance, such as facial scans, pair with massive databases to identify and track pro-democracy protesters. And improved and more accessible generative AI creates a deluge of disinformation polluting the public square.

Legal frameworks in at least 22 countries, including Vietnam and India, now mandate or incentivize digital platforms to deploy machine learning to remove disfavored political, social, and religious speech at a speed and scale that would be impossible for human censors or less sophisticated technical methods to achieve.[5]

1 https://freedomhouse.org/sites/default/files/2023-10/Freedom-on-the-net-2023-DigitalBooklet.pdf.
2 https://www.rferl.org/a/russia-china-internet-censorship-collaboration/32350263.html.
3 https://www.nytimes.com/2024/03/15/technology/russia-internet-censors-vladimir-putin.html.
4 https://www.rferl.org/a/russia-china-internet-censorship-collaboration/32350263.html.
5 https://freedomhouse.org/sites/default/files/2023-10/Freedom-on-the-net-2023-DigitalBooklet.pdf.

In early 2023, India required YouTube and Twitter to use automated scanning tools to sweep up posts relating to a BBC documentary, which the government believed portrayed Prime Minister Narendra Modi in an unfavorable light.[6] Vietnam's Information Ministry similarly ordered international tech firms to use AI to automatically find and remove so-called toxic content.[7]

Roskomnadzor, Russia's federal agency responsible for monitoring, controlling, and censoring Russian mass media, launched their own internet surveillance system called Oculus in February 2023. The new AI system automatically detects "illegal" content, including any digital speech with "extremist themes, calls for mass rallies, suicides, or LGBT propaganda."[8] Oculus enables Russian authorities to easily and quickly censor the vast amount of online expression criminalized by the government in the lead up to, and aftermath of, the full-scale invasion of Ukraine.

This advanced censorship and surveillance tactic may have developed, in part, from the Russian government's desire to "learn" from Chinese censors. Documents leaked in 2023 show an increasing level of cooperation between the two nations in regard to cybersecurity.[9] Across several meetings from 2017 to 2019, documents reveal knowledge sharing occurred on ways to censor apps and handle popular dissent. In one meeting, Russian officials specifically asked how the Chinese government uses AI to identify and block prohibited content.

Russia is also harnessing the power of biometric surveillance to target protesters and anyone critical of Vladimir Putin's regime. More than 60 regions in the country have installed half a million cameras with facial recognition technology.[10] A 2023 report revealed this technology played an important role in the arrests of hundreds of protesters in Russia.[11]

Radio Free Europe/Radio Liberty's Balkan Service recently conducted an investigation into the expansion of video-surveillance systems in more than 40 cities and municipalities in Serbia.[12] In Belgrade alone, the government is introducing approximately 8,000 Huawei surveillance cameras with facial-recognition capabilities (Huawei is a Chinese company).[13] On the other side of the world, authorities in Mexico announced a new layer of monitoring for a 20-story surveillance tower in Chihuahua.[14] Gas stations, businesses, restaurants, and private citizens will all be asked to feed their cameras into the system, which already includes plans for 3,065 cameras as well as biometric filters to support facial recognition.[15]

---

6 https://time.com/6249393/the-modi-question-documentary-bbc-india-controversy/.

7 https://www.voanews.com/a/vietnam-orders-social-media-firms-to-cut-toxic-content-using-ai-/7201741.html.

8 https://cybernews.com/news/russia-oculus-tool-lgbt-ukraine/.

9 https://www.rferl.org/a/russia-china-internet-censorship-collaboration/32350263.html.

10 https://therecord.media/russian-region-primorsky-krai-snitching-chatbot.

11 https://www.reuters.com/investigates/special-report/ukraine-crisis-russia-detentions/.

12 https://www.rferl.org/a/serbia-surveillance-cameras-china/32526515.html.

13 Id.

14 https://therecord.media/torre-centinela-sentinel-tower-chihuahua-ciudad-juarez-texas-surveillance.

15 Id.

Content Generation and Manipulation Increases with AI

Improved and inexpensive (or free) AI-generated image tools, such as Midjourney, now allow virtually anyone to instantly create fake images online. Version 5.2 of Midjourney, released in June 2023, produces more detailed and realistic images than earlier models.[16] Assessing the veracity of such images can be difficult. AI detectors, which can be used to check whether an image or text is possibly AI-generated, are still very error-prone and often only make decisions as likely probabilities—not with 100% certainty. As a result, the rise in AI-generated content makes users feel less confident about what they view online.[17]

According to *Freedom on the Net 2023*, at least 16 countries utilized generative AI to distort information on political or social issues.[18] When influenced by state-controlled information sources, these tools can serve as "force multipliers for censorship."[19] This is especially concerning in countries like China where the information landscape is already tightly controlled.

China is also employing a deliberate import-substitution policy to eliminate foreign technologies and replace them with home-grown alternatives.[20] Domestic AI-generated tools are a central component of a years-long initiative to integrate the Chinese Communist Party's censorship goals into the country's content-recommendation algorithms and synthetic media.[21] In August 2023, the Cyberspace Administration of China approved the release of five chatbots, which are required to promote "core socialist values" and exclude content deemed to be undesirable by the ruling party.[22]

In response to these alarming global developments, civil society is increasing its calls for an AI regulatory framework to protect human rights and information integrity in the digital age.

16 https://www.washingtonpost.com/technology/2023/03/30/midjourney-ai-image-generation-rules/.

17 https://www.dw.com/en/fact-check-ai-fakes-in-israels-war-against-hamas/a-67367744.

18 https://freedomhouse.org/sites/default/files/2023-10/Freedom-on-the-net-2023-DigitalBooklet.pdf.

19 Id.

20 https://www.wsj.com/world/china/china-technology-software-delete-america-2b8ea89f.

21 https://freedomhouse.org/sites/default/files/2023-10/Freedom-on-the-net-2023-DigitalBooklet.pdf.

22 Id.

Spyware: A Growing Global Surveillance Crisis

Government-sponsored mass and targeted surveillance or intrusion using manufactured spyware, such as Pegasus from the NSO group, has increased significantly over the past several years.

The European Investigative Collaborations media network recently collaborated with Amnesty International's Security Lab on the Predator Files—an investigation into the proliferation of invasive spyware in at least 25 countries across Africa, Asia, Europe, and the Middle East. Released in October 2023, the report focuses on the "Intellexa alliance," a complex, shifting group of interconnected companies operating without oversight or accountability.[23] "Predator" is its highly invasive spyware. The technology and its rebranded variants can access unchecked amounts of data on devices—gaining access when a user simply clicks on a malicious link, or through tactical attacks, which can silently infect nearby devices.[24]

Two other reports released in 2023 by Microsoft and Citizen Lab revealed the Israeli spyware company QuaDream's hacking tools have been used against minority politicians and journalists in several countries.[25] Citizen Lab's report identified at least five civil society victims in North America, Central Asia, Southeast Asia, Europe, and the Middle East.[26]

Surveillance scandals have long plagued Mexico, too, yet 2023 marked the first time a high-ranking member of the government was the victim.[27] Alejandro Encinas, Mexico's undersecretary for human rights, was targeted by Pegasus while investigating abuses by the national army.[28] Pegasus has also targeted exiled members of the Russian media, including prominent independent Russian journalist Galina Timchenko—the founder of Meduza, an independent Russian news outlet outlawed by the Kremlin.[29] Timchenko's case is the first publicly reported instance of the invasive surveillance tool being used against a significant Russian target.[30]

---

23 https://www.amnesty.org/en/latest/news/2023/10/global-predator-files-investigation-reveals-catastrophic-failure-to-regulate-surveillance-trade/.

24 Id.

25 https://www.washingtonpost.com/technology/2023/04/11/quadream-spyware-reports-citizen-lab/.

26 https://citizenlab.ca/2023/04/spyware-vendor-quadream-exploits-victims-customers/.

27 https://www.nytimes.com/es/2023/05/22/espanol/alejandro-encinas-pegasus-espionaje.html?smtyp=cur&smid=tw-nytimes.

28 Id.

29 https://www.theguardian.com/world/2023/sep/25/latvia-russia-meduza-phone-hack-galina-timchenko.

30 https://www.washingtonpost.com/technology/2023/09/13/pegasus-infection-meduza-founder/.

Increasingly Widespread Conventional Censorship

Despite advances in AI and its adoption by more authoritarian regimes, conventional forms of censorship—such as the blocking of websites, VPNs, and forced content removal—remain widespread across the world.

In 2023, the governments of 41 countries imposed outright blocking of websites that hosted political, social, and religious speech—an all-time high in Freedom House's 13 years of reporting on online freedom.[31] Russia, one of the worst such offenders, continues to ban more than 10,000 websites and apps for content about the full-scale war in Ukraine, as well as several commercial VPNs.[32]

India similarly blocked independent news sites and passed an amendment to its IT Rules 2021 to target purported "fake" content online. The amendment requires intermediaries such as Facebook to remove any information the government deems to be "false" or "misleading."[33]

In Iran, many foreign or independent applications are blocked and the entire Google Play store remained blocked late into 2023.[34] Given that roughly 90% of mobile users in Iran use Google's Android operating system, this pervasive form of censorship makes it incredibly difficult for residents to acquire safe and secure VPNs.[35]

Notably, authoritarian governments are also encouraging peer-to-peer censorship by launching apps that enable citizens to censor one another online. Released in 2023, Iraq's Ballegh app allows citizens to report social media content that "violates public morals, contains negative or indecent messages, and undermines social stability."[36] Certain regions in Russia have set up a Telegram chatbot for citizens to report colleagues and neighbors promoting "anti-Kremlin propaganda."[37]

LGBTQ+ content and communities, in particular, faced an uptick in conventional censorship in 2023. Lawmakers in Ghana deliberated on amendments to the country's Promotion of Proper Human Sexual Rights and Family Values Bill (2021).[38] The bill prohibits advocating for LGBTQ+ rights, explicitly assigns criminal penalties for such speech posted online, and threatens online platforms—specifically naming Twitter and Meta products Facebook and Instagram—with criminal penalties if they do not restrict pro-LGBTQ+ content.[39] Kenya followed this legal tract with its Family Protection Bill (2023), prohibiting homosexuality with imprisonment for a minimum 10 years and mandating life imprisonment for convictions of "aggravated homosexuality."[40]

---

31 https://freedomhouse.org/sites/default/files/2023-10/Freedom-on-the-net-2023-DigitalBooklet.pdf.

32 https://www.wired.com/story/amnezia-vpn-russia-censorship/.

33 https://rsf.org/en/modi-visits-washington-dc-indian-government-preparing-censor-internet.

34 https://www.article19.org/resources/tightening-the-net-iran-one-year-on-from-mahsa-jhina-amini-uprising/.

35 Id.

36 https://smex.org/iraqs-controversial-ballegh-platform-for-combating-indecent-content/.

37 https://therecord.media/russian-region-primorsky-krai-snitching-chatbot.

38 https://www.techpolicy.press/ghanas-antilgbtq-agenda-will-be-a-disaster-for-human-rights-online-and-off/.

39 https://www.eff.org/deeplinks/2023/06/around-world-threats-lgbtq-speech-deepen.

40 Id.

Passage of the bill will limit the right to free expression and a slew of other human rights both offline and on. During this same time, Russia increased its blocking of websites that host LGBTQ+ content.[41]

Traditional champions of free speech also began to consider imposing conventional forms of censorship in 2023.[42] Norms around the acceptability of censorship are changing—in large part because China has made the technology readily available. As a result, restrictions on free speech and access to information that were once taboo for many in the international community are no longer so—illustrating the fragility of internet freedom and creating risks for even established democracies.

Internet Shutdowns Remain Pervasive

Access Now's mid-year update on shutdowns in 2023 reported 80 shutdowns across 21 countries—18 of which began in 2022.[43] The report indicated the worst offenders from previous years, including Iran and India, were continuing to double-down on their use of this blunt form of repression as a tool of political control.[44]

The prevalence of internet shutdowns could be due, in part, to the fact that AI-powered moderation and filtering tools are not always equipped to keep up with a surge of unexpected content and expression of dissent, like that which can occur during times of crisis or protest.[45] Following the death of Mahsa Amini in 2022, mass protests in Iran continued into 2023—overwhelming the government's technically advanced censorship apparatus and leading authorities to cut off services, including in targeted regions. In addition to regular shutdowns of the entire internet, the regime enacted "digital curfews" to curtail access when protests were likely to occur.[46] Iranian authorities also increasingly cut off mobile internet access in response to regional protests in Khuzestan, Kurdistan, Sistan, and Baluchestan.[47] Cutting mobile connections has become a favored censorship method, as many people in Iran rely on smartphones for connectivity.

For five years running, India has overseen the highest number of internet shutdowns in the world.[48] As of May 2023, 13 states in the country imposed a total of 33 shutdowns, including nationwide access cuts as well as local blackouts in response to protests, religious anniversaries, and communal violence.[49]

In Myanmar, millions of people continue to struggle with a near-total lack of connectivity as part of the brutal crackdowns initiated by the military junta that seized power in 2021.[50] Regions where the military faces armed resistance remain the heaviest hit by this extreme censorship.

41 https://freedomhouse.org/sites/default/files/2023-10/Freedom-on-the-net-2023-DigitalBooklet.pdf.

42 https://freedomhouse.org/sites/default/files/2023-10/Freedom-on-the-net-2023-DigitalBooklet.pdf.

43 https://www.accessnow.org/publication/internet-shutdowns-in-2023-mid-year-update/.

44 Id.

45 https://freedomhouse.org/sites/default/files/2023-10/Freedom-on-the-net-2023-DigitalBooklet.pdf.

46 https://carnegieendowment.org/2023/11/29/aggressive-new-digital-repression-in-iran-in-era-of-woman-life-freedom-uprisings-pub-91025.

47 Id.

48 https://www.accessnow.org/press-release/india-must-withdraw-the-telecommunications-bill-2023/.

49 https://www.accessnow.org/publication/internet-shutdowns-in-2023-mid-year-update/.

50 Id.

Similarly, the two-and-a-half year internet shutdown for many in Tigray, Ethiopia, continued in 2023 despite a peace agreement between Tigrayan and Ethiopian armed forces. War in the region broke out in November 2020 and has resulted in the deaths of hundreds of thousands of people and displacement of millions.[51] Amhara, another region in Ethiopia, suffered from a complete shutdown in August 2023 after the government declared a state of emergency.[52]

Despite this overall bleakness, one bright spot did emerge. Of the 18 countries Access Now identified for increased risk of internet shutdowns during elections, seven maintained access to the internet during voting periods in 2023.[53]

Prosecution for Online Expression Grows More Common

Individuals faced legal repercussions for expressing themselves online in a record 55 of the 70 countries covered in Freedom House's *Freedom on the Net 2023* report.[54] Unsurprisingly, the harshest penalties were meted out in the most authoritarian contexts.

Following the full-scale invasion of Ukraine, Putin's regime expanded use of its "foreign agent" labeling, enacted legislation to penalize and criminalize free speech, and increasingly punished citizens for any online expression it considers critical of the war—from fines to imprisonment to even the loss of child custody.[55] Facing a decade in prison for an Instagram post questioning Ukrainians' reaction to a bridge attack, 20-year-old Olesya Krivtosa fled the country to avoid prosecution.[56] Meanwhile, a court in the Russian city Kazan sentenced a blogger to three years in prison for urging Russian military personnel to desert the war in Ukraine.[57]

China, which maintained its status as the world's worst abuser of internet freedom for the ninth consecutive year (per Freedom House), ordered one of its citizens to pay one million yuan (approximately USD $140,000) for using a VPN.[58] This is considered to be the most severe financial penalty ever issued to an individual for circumventing China's "great firewall." [59]

In response to protesters and activists opposing mandatory regulations and refusing to wear the hijab in public and on their social media accounts, Iranian authorities introduced the 2023 "Hijab and Chastity Bill" in an effort to codify the criminality of these acts.[60]

51 https://www.voanews.com/a/ethiopia-tigray-rebel-officials-meet-to-review-implementation-of-peace-deal-/6885861.html.

52 https://therecord.media/ethiopia-internet-blackout-amhara-region.

53 https://www.accessnow.org/campaign/2023-elections-and-internet-shutdowns-watch/.

54 https://freedomhouse.org/sites/default/files/2023-10/Freedom-on-the-net-2023-DigitalBooklet.pdf.

55 https://www.nytimes.com/2023/03/22/world/europe/russia-ukraine-social-media-crackdown.html.

56 Id.

57 https://therecord.media/russian-region-primorsky-krai-snitching-chatbot.

58 https://amp.theguardian.com/world/2023/oct/09/chinese-programmer-ordered-to-pay-1m-yuan-for-using-virtual-private-network.

59 Id.

60 https://www.article19.org/resources/tightening-the-net-iran-one-year-on-from-mahsa-jhina-amini-uprising/.

The new law also contains a special provision for "celebrities" who defy the Islamic Republic's hijab restrictions—with violators facing confiscation of up to 10% of their total assets.[61] This effort is among the latest by hardliners in the regime to suppress support for the "Woman, Life, Freedom" protest movement, which has gained the support of many Iranian actors, athletes, and social media influencers.[62]

Egypt, Iraq, and Myanmar also arrested and sentenced their citizens to prison for expressing themselves online. In Egypt, Patrick Geroge Zaki was sentenced to three years in prison for using digital media to write about the hardship and discrimination faced by Coptic Christians in the country.[63] The Egyptian government's deepening crackdown on free expression has made digital expression precarious for even those who post seemingly apolitical content.

In January 2023, authorities arrested content creator Mohamed Hossam El-Din on terrorism charges for posting a satirical video of himself that gained more than 7.5 million views on Facebook.[64] The video contained no overtly political message.

In Iraq, citizens have been charged and prosecuted for what authorities consider "indecent" or "immoral" content on social media—nebulous terms that give authorities the power to hand down punishment for essentially any online expression they deem to be offensive.[65] In Myanmar, individuals have been similarly arrested for sharing anti-regime posts or even simply expressing their sorrow over airstrikes in a village.[66]

Other countries are also passing laws criminalizing online expression that authorities deem to be unfavorable. In Jordan, for example, a new cybercrime law criminalizes online content that the government considers to be false news or hate speech, or otherwise undermines national unity or incites immorality.[67] These harsh, real-world consequences for expressing one's opinion online ultimately lead to self-censorship, a diminished public square, and a desolate information landscape where authorities control the narrative—a totalitarian dream.

Combatting These Threats

Fortunately, this bleak picture of internet freedom is incomplete, as the online landscape was punctuated by an array of OTF-funded tools that helped at-risk communities defy the repressive censorship and surveillance techniques described above.

The following section highlights some of the progressive research, technology development, and community support funded by OTF during FY 2022.

61 https://observers.france24.com/en/middle-east/20230728-iranian-parliament-to-consider-law-targeting-celebrities-who-defy-hijab-rules.

62 Id.

63 https://www.accessnow.org/press-release/civil-society-condemns-sentencing-of-egyptian-academic-and-researcher-patrick-george-zaki/.

64 https://www.wsj.com/articles/egypt-arrests-social-media-influencers-in-deepening-crackdown-b26835bc.

65 https://www.accessnow.org/press-release/joint-statement-iraqi-authorities-must-cease-their-chilling-crackdown-on-free-speech/.

66 https://engagemedia.org/2023/myanmar-digital-coup-quarterly-february-april-2023/.

67 https://www.dw.com/en/jordan-cybercrime-law-slams-free-speech-as-criminal-content/a-66630443.

07 Project Highlights

OTF used FY 2022 funds to support over 40 innovative projects to circumvent censorship and enhance digital privacy and security, seven fellows engaged in cutting-edge research on information controls, and 19 rapid response interventions to address digital emergencies. In addition to direct financial support, OTF also offered services through various Labs to improve the security, usability, and accessibility of internet freedom tools—contributing to increased adoption and greater community trust.

This section highlights key projects that exemplify OTF's mission to advance internet freedom globally. A full list of projects supported by FY 2022 funds is included at the end of this report.

Surging Support for Circumvention Tools

As China, Iran, Russia, and other authoritarians invest in increasingly sophisticated online information controls, demand for OTF-supported circumvention tools continues to rise. In 2021, 9 million monthly active users (MAUs) utilized OTF-supported circumvention tools. Today, by contrast, OTF regularly supports as many as 46 million MAUs. The organization's investment in these tools continues to unlock an expanding audience for independent media outlets operating in closed spaces, including those funded by USAGM.

Through the Surge and Sustain Fund (formerly the Technology at Scale Fund), OTF provides resources on a competitive basis to large-scale, open source circumvention tools with a documented track record of success in closed information environments. Without these critical resources, circumvention tool operators would be forced to throttle or limit usage of their tools in these countries at a time when they are needed most.

When the most advanced censor in the world, the Chinese government, blocked many circumvention protocols in 2021, circumvention tool **nthLink** relied on OTF support to develop V2Ray—a multi-protocol architecture for censorship-evasion with strong blocking recovery. As a result, nthLink is one of the most continuously effective circumvention solutions for users in China today.

Psiphon, another OTF-supported tool, is one of the most technically advanced and widely used circumvention tools in the world, helping more than 37 million people every month overcome censorship and connect to the open internet. Following the full-scale invasion of Ukraine in February 2022, Psiphon experienced a surge of over 2.6 million MAUs in Russia in just one month. In Iran, usage of the tool spiked to 17.7 million MAUs after the wide-reaching internet censorship imposed by the Iranian regime in the aftermath of Mahsa Amini's death in September 2022. OTF's Surge and Sustain Fund supported the infrastructure costs associated with carrying these additional users, helping nearly 5 million people in Russia and nearly 18 million users in Iran retain access to the broader internet.

Providing Timely & Accurate Censorship Detection

As censorship tactics continue to evolve, so too must circumvention techniques. In order to develop the most effective tools, investigating when, where, and how censorship is occurring is essential. Yet conducting large-scale internet censorship measurement is challenging—particularly if it is to be done quickly. In an effort to meet this challenge, OTF utilized FY 2022 funds to invest in novel censorship-measurement projects to more swiftly and reliably determine the scale of—and response to—digital authoritarianism around the world.

Measuring wide-ranging internet censorship is difficult because it involves triggering censors through artificial requests and identifying abnormalities from corresponding responses. Due to the lack of "ground truth" on the expected responses from legitimate services, many efforts to conduct large-scale censorship measurement typically require unscalable manual inspection. To address this, OTF funded **Disguiser**, a novel framework that enables end-to-end measurement for accurately and automatically detecting censorship activities and deployment. When deployed in the field, the framework's granular measurements revealed that the country-level aggregation of censorship relied upon in existing studies is far from accurate. This enhanced understanding of the variety of techniques used within national boundaries will help developers craft more effective and variable circumvention solutions going forward.

Information Controls Fellow Amir Gh's project **Monitoring Censorship with Comprehensive Network-Level Error Logging** similarly helped to develop new tools and frameworks for measuring network disruptions and blocking through a comprehensive set of network-level error logging and reporting. The information generated from Gh's research will help circumvention tools better adapt to evolving censorship tactics.

OTF also invested in **GreatFire's Applecensorship.com**, a transparency project that monitors Apple's complicity in China's censorship and surveillance of iOS users —often through the removal of apps from the App Store. The project compares the availability of App Store applications globally and monitors when Apple removes or blocks apps in China and other countries.

The project has discovered nearly 10,000 apps available elsewhere in the world are unavailable in the China App Store, including Apple's own News App, the Session App, and other OTF-supported apps. Session, one of the best secure messaging apps in the world, was removed from the App Store in China just before the Tiananmen Square Massacre commemoration in 2022. The critical tool is still unavailable today, denying people in China a vital resource for communication and organizing. By publicly documenting Apple's App censorship, AppleCensorship.com sheds light on how Apple's practices limit free expression, privacy, and human rights.

And while authoritarians increase their use of artificial intelligence (AI) for censorship, OTF is supporting projects that harness generative AI for censorship detection and circumvention. OTF recently invested in **Geneva**[1], a novel experimental algorithm that automates the discovery of censorship evasion strategies to expedite circumvention product-development timelines. The AI's genetic algorithm trains against real world censors and automatically learns how to circumvent censorship without affecting traffic flow. Geneva has been successfully deployed against censors in China, India, Iran, Kazakhstan, and Turkmenistan. In 2023, a Geneva-assisted measurement tool examined Turkmenistan's internet censorship—the largest measurement study to date—and discovered more than 100,000 blocked domains.[2] It also uncovered five new censorship evasion strategies, demonstrating AI's potential to be harnessed as a public good to counteract its information-control application.

Exposing Privacy Vulnerabilities in Widely Used Applications

Government-sponsored mass and targeted surveillance has increased significantly over the past few years—often through leaked personal identifiable information (PII) from popular browsers and apps. In response, OTF used FY 2022 funds to invest in multiple research projects to expose vulnerabilities and educate users about threats to their digital security. As a result of these efforts, users can better protect their digital security and privacy on popular browsers, apps that are required to access essential services, and various messaging and social media platforms. The findings also help progressive web application (PWA) developers design around browser vulnerabilities to provide a safer experience for individuals using PWAs to access censorship circumvention and privacy tools.

Mobile Surveillance Monitor identifies active digital surveillance threats to at-risk individuals and groups around the world. The tool classifies threats by type, attack method, and network technology, as well as threat-activity volume. The OTF-supported project increases transparency into targeted attacks, enabling journalists, human rights defenders, and security researchers to improve their forensic capabilities. The tool also provides actionable insights into authoritarian surveillance for policymakers and the private sector.

1 Not supported with FY 2022 funds

2 https://dl.acm.org/doi/10.1145/3543507.3583189.

Information Controls Fellow Mona Wang evaluated the privacy and security practices of **WeChat**, the most popular messaging and social media platform in China (and third most popular in the world, with over 1.2 billion MAUs). The platform captures massive amounts of user data and has built-in, real-time censorship capabilities—so understanding what user data is transmitted is critical given WeChat's dominance and the implications of its censorship for news audience engagement strategies in the Chinese market. Prior to Wang's research, there had been little investigation into the specific security and privacy properties of WeChat and its proprietary transport encryption protocol. Notably, she found extensive activity-tracking when a user accesses other apps embedded in WeChat.

The **Protecting At-Risk Populations from Surveillance** project uncovered security vulnerabilities in six prominent Chinese web browsers commonly used in Asian markets. Browsers in China are often used to access censorship circumvention or privacy tools through PWAs, as apps themselves are increasingly restricted for users in the country. Researchers for the project discovered all six browsers (Baidu Searchbox, Alibaba's UC Browser, OPPO Browser, Redmi Browser, Tencent's QQ Browser, and VIVO Browser) collect data and send it with poor or missing cryptography, and also leak web or search activity (or both) along with other PII and network/device information. These findings are beneficial to developers of PWAs and users alike as they work to safely adapt to China's increasingly invasive and criminally-punitive information controls.

OTF also funded research into a surveillance method known as "**HTTPS eavesdropping**"—an interception attack in which a malicious actor cooperates with a Certificate Authority (CA) to obtain a rogue certificate, circumventing traditional protection mechanisms. This type of attack became more prevalent when the Russian government released its own root certificate authority in March 2022, granting the domestic CA (RTCA) the ability to inspect the traffic of users communicating with domains with RTCA-issued certificates. In an effort to inform users of these new risks to their privacy, Information Controls Fellow Alexandra Dirksen first studied the development and use of RTCA to reveal HTTPS interception and then created a prototype for a browser extension to provide users with security information. When deployed, the extension requests a certificate for the same domains the user is looking for from a server located outside of the attacker's reach, compares the certificates, and provides a visual warning to the user if the two diverge.

Another similar project, **Reversing Bloatware**, uncovered privacy and security vulnerabilities in nine major applications with millions of users in Latin America. People in the region are often incentivized through promotions and access to government services to keep these apps installed, despite the region's complicated history with state-based information controls. Government-sponsored mass and targeted surveillance using spyware is particularly pronounced in Mexico due to the large amount of applications that are pre-installed on end devices ("bloatware"). Information Controls Fellow Beau Kujath found that many apps leak PII and have weak network security, allowing malicious actors to access personal information and messages. Given that the tested apps are installed on millions of devices, these vulnerabilities create a huge opportunity for a domestic security agency to surveil its citizens.

Developing & Enhancing Privacy-Preserving Technologies

Today's digital authoritarians are more willing than ever to use targeted online harassment and surveillance to threaten the online and physical safety of journalists and human rights defenders. In a continued effort to counter mounting threats to digital privacy, OTF used FY 2022 funds to prioritize investments in secure communication technologies to enable users—especially those engaged in high-risk work such as human rights activists—to communicate privately and securely.

One such resource is **Tella**, a free, open source 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 their partner organization. Activists, journalists, and human rights defenders use Tella to protect themselves from physical and digital repression, and shield their data from censorship, tampering, and destruction. It is currently available in 15 languages, including Burmese, Karen Sgaw, and Russian.

Another free resource supported by OTF is **Mailvelope**, an open source software for encrypting email traffic with a growing user base. Mailvelope uses OpenPGP standards and works via a browser extension (allowing users to select the webmail provider and email address of their choice), ensuring a secure and user-friendly experience.

OTF also used FY 2022 funds to invest in improving the privacy of the transport layer security (TLS) protocol. The **DEfO-2: Developing Encrypted ClientHello for OpenSSL** project integrates Encrypted ClientHello (ECH) into more web servers and clients—utilizing ECH to plug a privacy-hole in the TLS protocol and hide previously visible details from observers. The most important, newly shielded detail is the name of the website the user wishes to visit—which, when visible, provides a straightforward method for censors to block websites and internet services. This critical effort strengthens the privacy of OpenSSL, a widely used library.

As persecution for online expression grows more common, high-risk individuals also need better digital safety tools—which is why OTF supported **Círculo**, an open source app for Android and iOS that offers a secure place to share locations and check-in while engaging in investigative journalism or human rights work in repressive countries. Originally designed to strengthen support networks among female journalists in Latin America, the app complements protocols-of-action established by a group of people, in which each member knows their role in possible high-risk scenarios.

Supporting Innovative Technology to Combat Conventional Censorship

While some authoritarians are using increasingly innovative and sophisticated censorship regimes to implement large-scale information controls, traditional methods still remain common. Although existing circumvention tools continue to be generally effective in circumventing these types of conventional controls, OTF used FY 2022 funds to support several unique approaches to skirt these censors and stay a step ahead.

One such OTF-funded VPN that remains accessible in Russia—even after the full-scale invasion of Ukraine—allows users to set up their own servers. Different from commercial VPNs that route traffic through company servers that can be blocked, the unique approach of this free, open source VPN allows users to choose their own IP address and use circumvention protocols that are harder to block. Given that most independent news outlets are now blocked in Russia, and dissenting expression is criminalized, providing a secure tunnel option to access vital news and the open internet helps preserve the availability of fact-based information for a population otherwise subject exclusively to Kremlin disinformation.

In response to censorship via the Domain Name System (DNS) becoming increasingly commonplace, OTF invested in the **Decentralized and Private DNS Lookup with Quad9** project. Unprotected DNS services, which remain dominant in most network environments, allow censors to prevent the translation of domains they deem "malicious." In highly repressive environments like Russia and Iran, blacklists include independent media, any expression critical of the authoritarian regime, and LGBTQ+ information. To prevent this type of censorship, Quad9 provides encryption protection as a basic part of the DNS service.

Bolstering Shutdown-Resilient Tools

Internet shutdowns are a pervasive form of authoritarian political control—putting human rights defenders and journalists at enormous risk, and limiting their connectivity as autocrats become emboldened to act with impunity. Technology that remains resilient in the face of shutdowns, the most blunt form of censorship, is therefore absolutely crucial. While there was once enormous social and economic cost to the use of wide-scale internet shutdowns, norms have evolved and shutdowns are now used more frequently to curtail free and fair elections, political demonstrations, and other forms of opposition. In response, OTF used FY 2022 funds to support the development of a number of tools that can operate with little-to-no connectivity, including communications resources, information networks, and human-rights documentation. OTF's support of shutdown mitigation technologies like these allows activists, journalists, and the general public to continue to communicate and organize—mitigating the efficacy of this crude form of information control.

Delta Chat is an offline-first, shutdown-resilient messaging app for users in repressive environments. It enables decentralized secure messaging through email-provider infrastructure with end-to-end encryption. Delta Chat is novel in that it does not require a phone number and has no central server, so it is harder to block. Its secure chat-mail feature also allows for instant onboarding with pseudonymous accounts and offers ephemeral messaging with sub-second delivery speeds. Even during periods of limited connectivity, the tool allows human rights organizations, independent media, and rapid response groups to communicate and collaborate securely and reliably with both each other and the communities they support.

The **Building Resilient Community and Communications** project brought Resilient Communications Boxes (aka "RCBoxes") to individuals in shutdown or low-connectivity areas in Colombia, Venezuela, and Zimbabwe. Without requiring a user to have internet or mobile data, the RCBox offers access to a customizable collection of mobile applications and digital resources useful in both day-to-day life and emergencies. These include password protection, offline map applications with local map files, nearby communication solutions that work over bluetooth and WiFi direct, medical and first-aid guides, and secure and encrypted note taking and documentation tools. The available set of apps and content can be curated and updated by the local provider of the RCBox, enabling the resource to remain up-to-date and useful in low- or no-connectivity political contexts.

In addition to stand-alone tools and toolkits, OTF also continued to invest in **Awala**, a shutdown-resilient network that enables compatible apps to use the internet as normal when it is available, but then switch to a secure sneakernet (which is the transfer of digital information by physically moving media such as a USB drive) when the internet is cut off. Developers can use Awala to make existing internet services resilient to internet blackouts, or build Awala-native apps to unlock additional benefits. The team behind Awala recently created Letro, an Awala-native service analogous to email. Native apps such as Letro will increase the network's utility and adoption.

Responding to Digital Emergencies Around the World

This past year was unprecedented in terms of the number and scale of digital threats—ranging from brutal crackdowns on protestors to heavy-handed persecution for online expression deemed to be "anti-regime." In turn, OTF increased Rapid Response Fund investments to meet the growing needs of communities in crisis. The majority of these interventions supported individuals in countries like Iran, Myanmar, and Russia, which are some of the most digitally repressed in the world.

Circumvention Tools & Digital Security Support for Users in Iran

Usage of OTF-supported circumvention tools surged in Iran following the Iranian government's brutal response to anti-regime protests. This surge persisted into 2023 and quickly became the new "normal," as Iranian authorities continued to increase censorship as part of their violent crackdown against demonstrators. OTF supported the infrastructure costs of carrying these additional circumvention users—approximately 26 million—for VPN providers **Lantern**, **nthLink**, and **Psiphon**. Notably, OTF's increased support for circumvention tools during this period of time corresponded to dramatic increases in audience traffic amongst USAGM networks' Persian-language news services.

OTF also helped to increase the availability of the **Tor Browser** (a secure web browsing service) within the country, and localized corresponding support and resources for individuals in Iran in response to rapidly increasing demand. The protocol most commonly used to access the Tor Browser for censorship circumvention is Snowflake, a pluggable transport that disguises a user's Tor connection as ordinary traffic to well-known web services, such as Skype. With OTF support, the number of Snowflake users in Iran increased fivefold and the number of Snowflake proxies (intermediaries between clients and servers) increased approximately 40%.

Another priority for OTF in 2023 was ensuring the most at-risk communities in Iran, such as journalists and activists, had access to practical digital security guidance. Partnering with an Iranian security team, FY 2022 funds were used to support the rapid publication of a 15-topic security manual with direct, actionable advice to help mitigate risk and ensure online and offline activities remain secure. The security team behind this effort also provided direct training for activists and journalists, and published 83 educational pieces.

Helping Independent Media in Myanmar Reach Audiences

Since seizing power in a 2021 coup, Myanmar's military junta has engaged in aggressive digital repression tactics. Millions of people in the country today struggle with little-to-no internet connectivity, and online expression is subject to harsh punishment if deemed to be "anti-regime." Independent media—including one of the largest outlets *Myanmar Now*—is also almost entirely blocked.

In an effort to help residents access English and Burmese versions of this important publication, one of OTF's Rapid Response Fund Partners (Quirium Media Foundation) deployed mirror sites—replicas of the original, blocked sites. This publisher-side circumvention technique provides easily-shareable news and information to populations living under repressive censorship.

Securing Digital Infrastructure & Helping People in Russia Access the Open Internet

The information space and public square in Russia continued to deteriorate in 2023. Punishments for online expression were heavy-handed, and more than 10,000 websites and apps were blocked within the country. Hungry for news and other uncensored information in the wake of the full-scale invasion of Ukraine, residents of Russia increased their usage of circumvention tools like **Lantern**, **nthLink**, and **Psiphon** and delivered historic audience peaks to USAGM Russian-language broadcasters during this time of uncertainty and crisis. Rapid Response funding to cover the infrastructure costs associated with this surging user-base helped approximately 6 million individuals in Russia retain access to the broader internet and stay safe from government surveillance.

OTF also helped the Mass Media Defense Centre—a Russian civil society organization supporting media freedom that Russian authorities labeled a "foreign agent"—secure their digital infrastructure during this tumultuous period. This entailed moving their website outside the Russian domain.

08 Supported Projects

Internet Freedom Fund

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

Digital Democracy

$47,500

Dtwo Ltd. (Digital Democracy)

Digital Democracy empowers marginalized communities in repressive contexts to use technology to defend their rights by providing technical support and building collaborative technology projects. OTF's funding supported Digital Democracy's Mapeo, an open source toolkit for documenting, monitoring, and mapping that is utilized by indigenous communities to document human rights abuses in 12 projects in Peru, Ecuador, and Colombia. Mapeo fills the need for a secure human rights documentation tool that works during internet shutdowns and in remote locations with limited or no connectivity, as it enables data to be shared offline between devices. The local-first database is also easy to use, as it does not require any setup and is embedded in mobile and desktop apps.

Visualizing and Explaining App Censorship

$10,000

GreatFire

GreatFire's AppleCensorship.com is a censorship monitoring project that documents instances of Apple Inc.'s collaboration with government censorship efforts—often through the removal of apps from the App store. In China, AppleCensorship.com identified a chilling level of complicity with government censorship demands. Nearly 10,000 apps in the China App store are unavailable, including many supported by OTF. The Session app, a secure messaging app, was removed in 2022 just before the Tiananmen Square Massacre commemoration and remains unavailable today—denying Chinese citizens a vital tool for communication and organizing. AppleCensorship.com aims to shed light on Apple Inc.'s practices, underscoring their implications on free expression, privacy, and human rights. OTF's most recent funding improved data accessibility and supported collaboration with partner organizations to provide a more complete picture of Apple Inc.'s global censorship.

Mailvelope

$38,000

Mailvelope GmbH

Mailvelope is an open source browser extension designed to securely encrypt emails on webmail providers using OpenPGP standards. The tool enhances webmail services such as Gmail™ with encryption and decryption functionality. It offers key management, and is therefore compatible with existing PGP implementations. OTF's funding improved the usability of Mailvelope by adding more features to make it competitive with existing PGP applications, improving its website and documentation, making the project more open to contributors, and supporting multiple languages.

Lower the Barrier to Adopt Awala

$46,003

Relaycorp, Inc.

Awala (formerly known as Relaynet) is a new computer network that enables compatible apps to use the internet as normal when it is available, but then switch to a secure sneakernet (transfer of digital information by physically moving media such as a USB drive) when the internet is cut off. Developers can use Awala to make existing internet services—like social networks—resilient to internet blackouts, or build Awala-native apps to unlock additional benefits such as decentralization or spam protection. OTF's funding worked to drastically lower the barriers to adopt Awala, including the delivery of a basic version of Letro (an Awala-native service analogous to email).

Protecting At-Risk Populations from Surveillance

$25,898

Arizona State University Foundation for A New American University

Arizona State University Biodesign Center for Biocomputation, Security and Society partnered with TibCERT/Tibet Action Institute (an organization focused on reducing and mitigating online threats in the Tibetan community) to investigate security vulnerabilities in six prominent Chinese web browsers commonly used in Asian markets, including at-risk communities that TibCERT serves. Understanding the risks associated with browsers is essential, as they are often the application individuals use with censorship circumvention or privacy tools. Researchers for the project found that all six browsers (Baidu Searchbox, Alibaba's UC Browser, OPPO Browser, Redmi Browser, Tencent's QQ Browser, and VIVO Browser) collect data and send it with poor or missing cryptography, and also leak web or search activity (or both) along with other personally identifiable information and network/device information. Leaked information includes full URLs and page titles of pages visited (even in HTTPS), search terms, GPS coordinates, device identifiers, and client IP addresses. The project's findings are informative for not only users, but also for developers of circumvention and privacy tools that run in browsers.

Disguiser: End-to-End Censorship Measurement

$1,025

Old Dominion University Research Foundation

Conducting large-scale internet censorship measurement is challenging, as it involves triggering censors through artificial requests and identifying abnormalities from corresponding responses. Due to the lack of "ground truth" on the expected responses from legitimate services, many efforts to conduct large-scale censorship measurement typically require unscalable manual inspection. In response, this project developed and deployed Disguiser, a novel framework that enables end-to-end measurement for accurately and automatically detecting censorship activities and revealing the censor deployment without manual efforts. The core of Disguiser is a control server that replies with a static payload to provide the "ground truth" of server responses. Requests from various types of vantage points across the world are sent to the control server and censorship activities can be recognized if a vantage point receives a different response. Disguiser can also facilitate extended measurements for investigating more aspects of internet censorship—such as pinpointing censor device locations and exploring their policies and deployment. The project found that inconsistent censorship activities can be due, in part, to the destination-server location and to different hosting platforms because the network paths through which a request traverses can be significantly influenced by the different peering relationships between the hosting platforms and ISPs.

Tella

$55,058

Horizontal

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 also securely send the material to the servers of an organization or partner with whom they are working. Tella is used by at-risk individuals and groups to protect against repressive surveillance when documenting rights violations and injustice. OTF's funding improved the performance and maintainability of Tella on Android, achieved parity between iOS and Android in terms of security and privacy features, and enhanced Tella's security and privacy on Android, iOS, and web.

nthlink Multi-Protocol Architecture

$30,600

Advanced Circuiting Inc.

nthLink is a powerful and free anti-censorship application, and also one of the most continuously effective circumvention solutions for Chinese users. In response to increased blocking by censors in China, nthLink integrated V2Ray—a new, multi-protocol architecture that incorporates the strength of other censorship protocols to create a robust circumvention service with heightened blocking recovery, scalability, and availability. The protocols benefit USAGM broadcasters, journalists, and at-risk populations in information-repressive geographies.

Rodrigue Hajjar – Surge and Sustain Fund Pricing Consultant

$5,160

Rodrigue Hajjar

OTF hired Rodrigue Hajjar as an independent consultant to help craft a framework for the Surge and Sustain Fund, a funding vehicle through which OTF supports the user-carrying costs for VPN providers operating at scale in highly repressive countries. Hajjar, a VPN expert in the internet freedom community, worked as a Director of Engineering at TunnelBear VPN and managed its free VPN bandwidth program for restrictive countries. Hajjar's expertise helped OTF create and apply a methodology for pricing the marginal cost of carrying users in specific countries beyond the core costs of running a tool.

Securing eclips.is Sustainability

$260,751

Greenhost

eclips.is offers a secure hosting service relied upon by many in the internet freedom community. The service represents critical infrastructure for human rights defenders across the globe, serving hundreds of thousands of end users who cannot or would prefer not to use other commercially available options due to privacy concerns or because of risk of surveillance and threat to themselves and their constituents. OTF's funding helped design for the long-term sustainability of eclips.is through improvements in technology (such as payment processing and developer tools), usability (user experience overhaul of the eclips.is dashboard and onboarding), and community (new and diverse financing models, and community ownership and governance).

China in the World Summit 2022

$80,000

Doublethink Lab

This project expanded the number of members, geographical regions, and focus-areas in the China in the World (CITW) Network—a group of stakeholders researching China's influence and disinformation strategies. The CITW 2022 Summit brought together experts, researchers, civil society practitioners, and digital rights activists to address the challenges presented by China's constantly evolving and increasingly sophisticated forms of digital repression, authoritarian technology, and censorship tactics. OTF's funding helped 25 stakeholders attend this important convening. OTF's funding facilitated valuable cross-regional and multi-sectoral collaboration to strengthen the study of China's authoritarian influences, particularly in the areas of internet freedom, digital surveillance, and censorship.

ACME for .onion Domains

$43,564

AS207960 Cyfyngedig

Many websites offer Tor services via .onion addresses (websites that are only available via the anonymous Tor Network), especially those which might otherwise be blocked in certain regions of the world. Transport layer security (TLS) certificates allow for the encryption of data between web browsers and websites, yet obtaining TLS certificates for .onion domains is currently quite expensive or time consuming (or both). Given this, many .onion domains do not have TLS certificates, leaving their users more vulnerable to data interception. This project worked to remedy this vulnerability by extending the Automated Certificate Management Environment (ACME) protocol to work with sites running on Tor.

Tor Relay Operator Community Health

$80,560

SR2 Communications Limited

The Tor Project's software and network system allows for anonymous and secure communication on the internet—enabling users to access websites and online resources that are typically blocked in countries with censorship. In order to operate, the Tor Network relies on volunteers who run relays, which are essentially routers that receive and transmit traffic. The more relays there are, the faster, safer, and more reliable the Tor Network becomes. This research project improved the health and safety of the Network.

Círculo

$252,142

Oliver+Coady Inc.

Círculo is an open source safety app for Android and iOS devices that offers users a secure place to share locations and check-in while traveling or engaging in high-risk work, such as investigative journalism in repressive countries. Originally designed to strengthen support networks among female journalists in Latin America, the app complements protocols-of-action established by a group of people, in which each member knows their role in possible high-risk scenarios. Círculo is a protected place, outside of normal communication channels where harassment may be happening, and ensures that high-importance messages and alerts are not lost in other conversations. Responding to the shifting nature of threats in the region and needs expressed by target users, this project incorporated user-experience improvements and additional security features, and also developed additional training and outreach-focused resources for target communities.

Decentralized and Private DNS Lookup with Quad9

$750,530

CleanerDNS (dba Quad9)

The Domain Name System (DNS) serves as a translator between the human-recognizable domain names and machine-recognizable locations on the internet (and is a core service for the latter's function). DNS is also increasingly being used as a form of information control, and it is now commonplace for a DNS service to prevent the translation of domains deemed to be "malicious." While new encryption standards are creating privacy in the vital DNS function, existing tools for censorship circumvention, decentralized browsing, and private messaging are likely weakened by utilization of unprotected DNS services—which remain dominant in most network environments. Quad9 provides encryption protection as a basic part of DNS service. In addition to protection against observation and interception of user site access metadata, Quad9's free, open, and recursive DNS anycast resolver provides an extra layer of protection from malware, phishing, and spam. These DNS protections are offered at zero cost for all users, with no account-based personal information required in order to provide benefit. OTF's funding expanded Quad9's secure and privacy-respecting DNS resolver infrastructure, and helped to deliver its global-to-local service provision of secure domain lookups to end users. The project also supported public-interest research activities.

Digital Rights and Inclusion Forum (DRIF) 2023: Digital Security Clinic

$133,100

Paradigm Initiative

DRIF is a three-day, community-driven, annual convening where digital rights defenders promoting internet freedom in Africa and beyond meet to learn, share experiences, research outcomes, and collaborate to advance internet freedom on the continent. More than 300 attendees from media, civil society, and academia attended the April 2023 iteration. OTF's funding supported a Digital Security Clinic (DSC) at the event for media practitioners, human rights defenders, and civil society actors from repressive contexts across Africa. The DSC provided digital security training to 60 participants and introduced them to secure communication tools and other forms of privacy and security technology. In addition, three digital security helpdesks provided practical skills to help users stay safe online.

Bitpart

$614,456

Throneless LLC

Human rights defenders in repressive states continue to need a simpler, more secure tool to organize large-scale, encrypted text blasts. Additionally, organizations supporting these human rights defenders need a secure, scalable way to distribute surveillance-circumvention tools. Enter the secure chatbot engine Bitpart, which will be the only consistently maintained, open source, security-driven chatbot platform made for human rights defenders.

Bitpart will enable easy, mass communication of news, software, organizing information, or any other kind of broadcast data via secure, proven communication platforms like Signal—all without requiring any additional software on user phones. The new tool can be used more easily to warn of a crackdown on protests, provide an invasion or disaster alert, or disseminate instructions and software for accessing the uncensored internet. OTF's funding supported designing the platform to connect with a variety of services where human rights defenders already do their organizing (initially targeting Signal, WhatsApp, Telegram, and Slack).

Building Resilient Community & Communications: Fiesta Mantequilla

$362,329

Oliver+Coady Inc.

This project supported at-risk internet users in repressive environments during internet shutdowns by providing them with access to Resilient Communications Boxes ("RCBoxes"), a customizable collection of mobile apps and digital resources useful in both day-to-day life and emergencies. The available set of apps and content can be curated and updated by the local provider of the RCBox—ensuring it is an up-to-date and useful resource for people without other forms of connectivity.

ConnectCon: Consolidating a Network of Digital Security Practitioners in Southern Africa

$88,759

Digital Society Africa

This two-day, knowledge-sharing event in June 2023 connected new digital security trainers with advanced practitioners. Recognizing the dearth of digital security practitioners in southern Africa alongside an alarming increase in digital threats, the event's host Digital Society Africa used the program to provide digital security skills to 60 trainers from Zimbabwe, Zambia, Mozambique, Malawi, South Africa, and Eswatini. This important community convening imparted advanced skills to the new trainers and strengthened the nascent network of digital security experts in the region.

DEfO-2: Developing Encrypted Client Hello for OpenSSL

$392,933

Tolerant Networks, LTD

Encrypted ClientHello (ECH) plugs a privacy-hole in the transport layer security (TLS) protocol by hiding previously visible details from observers. The most important, newly shielded detail is the name of the website a client wishes to visit, which—when visible—provides a straightforward method for censors to block websites and internet services. DEfO-2 was a continuation of an effort OTF previously supported to develop interoperable implementations of ECH for OpenSSL, Conscrypt, and—via those software libraries—a range of ECH-enabled web servers and clients. The key objectives of the new effort included upstreaming integration of ECH into more clients and servers, and publishing open source ECH provisioning tools.

Documenting and Preventing Information Controls During the Electoral Period in the Democratic Republic of Congo

$345,946

Partenariat Pour La Protection Integree (PPI)

Restrictions on freedom of expression are increasing in the Democratic Republic of Congo—undermining democracy and the respect for human rights. Because the government shut down the internet during the three elections prior to 2023, this project documented all forms and methods used to control information ahead of the December 2023 elections. Support was also utilized to set up a digital security helpline platform and provide digital security training for digital rights defenders and incident handlers. Insights into the information controls used during the electoral period were provided as part of this effort.

Internet Freedom Network Resilience

$903,515

Article 19

Digital rights defenders (DRDs) face increased risks related to online censorship and surveillance, overt online harassment, and the escalation of sophisticated legal, digital, and physical attacks. And with repressive autocratic actors becoming better at sharing tactics, DRDs are encountering more challenges related to coordinating and sharing information with one another. Building on their previous work supporting global DRDs, Team CommUNITY (a community-based membership network of DRDs) enhanced internet freedom by building more resilient frontline communities. These efforts included "Global Gathering" events, which brought together approximately 800 DRDs from across the globe for collective goal setting and network development.

Monitoring Mobile App Store Censorship

$138,160

GreatFire

App censorship is one of the most prevalent forms of mobile censorship, yet it has only recently attracted attention from civil society and regulators. As a result, the scale of mobile app censorship by country has not been comprehensively measured and many stakeholders do not fully understand the extent of the problem. In response, this project developed the "Play Store Monitor (PSM)"—a novel tool to track the availability and removal of Android apps from the Play Store. The effort built upon prior work to increase app-store transparency, including through App Store Monitor which records iOS app censorship.

Mobile Surveillance Monitor Enhancements

$166,650

Mobile Intelligence Alliance

Due to the lack of transparency within the mobile industry, the digital rights of activists and other at-risk individuals have long been violated through surveillance-software technologies. This has been accomplished through exploitations in the complex ecosystem of devices and networks used to provide services. Mobile Surveillance Monitor is a multi-source, threat-intelligence solution designed to analyze and provide insights into active surveillance threats targeting the phones of at-risk individuals and groups around the world. The tool can identify threats by type, attack method, and network technology, as well as threat-activity volume. This project improved the tool as a resource for digital security help desks, as well as journalists and researchers in the internet freedom community.

New features include a "3G vs. 4G" attack dimension filter to isolate and measure surveillance attacks from these networks, and a forensic "Malware Decoder" research tool to query and obtain over 800 indicators-of-compromise of high-profile, targeted spyware and attributed threat groups with global targeting data.

Forum on Internet Freedom in Africa

$78,281

Collaboration on International ICT Policy for East and Southern Africa

The Forum on Internet Freedom in Africa is an annual event that brings together stakeholders from across the internet governance and digital rights arenas in Africa and beyond to deliberate on gaps, concerns, and opportunities for advancing online privacy, free expression, inclusion, innovation, civic participation, and the free flow of information. This project supported the tenth edition of the convening, hosted in Tanzania in September 2023.

Delta Chat: Secure Chat-Mail Instances

$126,390

Merlinux GmbH

This project explored a new model for decentralized, offline-first, and interoperable communications for repressed, fragmented, or locked-down network environments by creating secure chat-mail instance setups and bringing instant onboarding to the cross-platform Delta Chat messenger. While Delta Chat could already be used with a wide variety of existing email servers, secure chat-mail instances enabled instant onboarding with pseudonymous accounts. These instances also offer ephemeral messaging with sub-second delivery speeds and consist of standard components that are cheap to set up and maintain. Secure chat-mail improved Delta Chat apps with pervasive and user-tested protections against compromised networks or servers.

OpenVPN2.x

$28,160

Mandelbit SRL

OpenVPN2 supports OpenVPN, a VPN system that is widely used for censorship circumvention and privacy from surveillance. This project improved the performance of OpenVPN servers by offloading the data channel into the kernel space (a core component of a computer's operating system that has control over everything in the system), allowing users to obtain better performance when adopting OpenVPN and making them less inclined to use less secure VPN options.

Surge and Sustain Fund

As internet censorship continues to escalate globally, more users than ever before are relying on circumvention technologies to counter censorship and access the free and open internet. In response to this increasing demand, OTF established the Surge and Sustain Fund to provide leading circumvention tools with the resources they need to sustain their current users and respond to growing demands for their tools.

Psiphon

$3,089,202

Psiphon Inc.

Psiphon is one of the most technically advanced and widely used circumvention tools in the world, helping more than 37 million people every month overcome censorship and connect to the open internet. Following the full-scale invasion of Ukraine in February 2022, Psiphon experienced a surge of over 2.6 million monthly active users (MAUs) in Russia in just one month. In Iran, usage of the tool spiked to 17.7 million MAUs after the wide-reaching internet censorship imposed by the Iranian regime in the aftermath of Mahsa Amini's death in September 2022. This Surge and Sustain Fund effort supported the infrastructure costs associated with carrying these additional users—helping approximately 4.6 million Russian citizens and nearly 18 million users in Iran retain access to the broader internet.

Lantern

$2,987,755

Innovate Labs LLC

Lantern is a free software application that delivers private, fast, reliable, and secure access to blocked websites and apps. Through its mobile application, Lantern's peer-to-peer functionality allows mobile users in uncensored regions to provide access to content for users in censored regions.

This project provided circumvention technology services to USAGM networks in seven highly censored markets (including China and Iran), allowing for the secure development and distribution of digital content and facilitating access to this content as well as the broader internet. During 2023, Lantern served more than half a million daily users. In February 2023, daily data usage in China and Iran peaked at 1,210 TB and 13,715 TB respectively—illustrating the tool's efficacy in providing vital news and other information to repressed individuals. The Surge and Sustain Fund project also supported the surge of users in Russia and Iran. In Russia, Lantern traffic increased by 2,000% in the month following the full-scale invasion of Ukraine, while in Iran the tool experienced a four-fold increase in monthly active users—surging to 8.5 million—following the wide-reaching internet censorship imposed by the Iranian government. OTF's funding helped Lantern scale their proxy infrastructure and cover the associated costs with sustaining service for this huge surge in users.

nthLink

$2,581,042

Advanced Circuiting Inc.

nthLink is a powerful anti-censorship application capable of circumventing internet censorship and self-recovering from blocking events. The tool incorporates strong encryption to protect the information flow between the consumer and the source. During the period covered by FY 2022 funding, nthLink helped approximately 8 million people in the world's most heavily censored environments access USAGM network content and other information. nthLink's effective content delivery provides USAGM entity language services' landing pages and headline news in 15 countries, including China, Iran, Myanmar, and Russia. In the latter, nthLink traffic increased 11-fold in the month following the full-scale invasion of Ukraine. OTF supported emergency funding for nthLink to scale up their proxy infrastructure to accommodate the surge in nearly 2.8 million users in the country. In Iran, monthly active users of the tool jumped by nearly 2 million in the aftermath of the protests and subsequent censorship crackdown. OTF's funding also helped to sustain this surge in users.

Rapid Response Fund

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

QMF Rapid Response

$138,600

Quirium Media Foundation

Qurium Media Foundation (QMF) helps resolve digital threats and emergencies in a timely and comprehensive manner for individuals, communities, and organizations whose free expression, access to information, or security have recently been repressed. QMF services include organizational security and digital security support, digital attacks response and forensic analysis, secure web hosting, and connectivity-issue remediation. During 2023, QMF helped restore and securely host websites of independent news outlets and human rights activists in some of the most repressive contexts, including Azerbaijan, Cuba, Myanmar, Russia, and Uganda. In Myanmar, QMF deployed mirror sites (replicas of original sites that have been blocked) for *Myanmar Now*'s English and Burmese sites. One of the largest independent media outlets in Myanmar, *Myanmar Now* is blocked by most, if not all, ISPs in the country.

Women at Risk in Brazil

$2,000

Anonymous

This effort provided emergency support for women and their families involved in an ongoing trial in Brazil who were victims of digital threats. The project supported them through mediation with organizations involved, conducted forensic investigations into whether or not victims were being digitally monitored, helped with incident-response plans to address threats, and provided support to gather evidence for use in court.

Rapid Respond to Tor Censorship in Iran

$69,912

Tor Project

This project increased the availability of the Tor Browser (a secure web browsing service) for Android and other circumvention techniques in Iran, and increased localized support to users in the country. Since September 2022, the Iranian government has systematically restricted internet access and other forms of communication after protests erupted in the country.

While Iranian citizens were already using Tor prior to the start of the protests due to the frequency of internet censorship by the government, this usage increased tremendously as a result of the heightened digital repression.

Persian Security Manual

$40,875

Iran Security Team

This 15-topic security manual provided timely and practical security guidance to activists and journalists in Iran. The manual prioritizes direct, actionable advice (such as creating a plan-of-action in the event of device seizure) to help these at-risk individuals mitigate risk and ensure their online and offline activities are secure. Since finalizing the manual in March 2023, the authors trained 10 activists and journalists, published 83 additional promotional and educational pieces, and published nearly 100 content pieces on social media aimed at disseminating key insights for at-risk individuals in Iran.

Election Violence Tracker: Proofing Access During Nigeria's Elections

$25,500

PolicyLab Africa

Nigeria's elections have been associated with widespread fraud and violence and often lead to internet shutdowns and disruptions. Ahead of contested elections in March 2023, PolicyLab Africa, a Nigerian think tank, integrated censorship and network outage-resilience features into its Election Violence Tracker (an election monitoring tool) and developed resources to help civil society prepare for possible internet shutdowns and disruptions. The project shared resources with more than 40,000 citizens via social media, and the implementation of censorship-resilient features led to the successful logging of nearly 200 reports during the emergency reporting period.

Integrating New DNS Manipulation Detection into Censorship Observatories

$87,000

Armin Huremagic

Domain Name System (DNS) manipulation is a common technique used by censors and other adversaries to prevent users from reaching restricted internet content, but detecting DNS manipulation is challenging due to the variety of techniques, a dearth of clear signals of manipulation, and the volatility of the DNS ecosystem. CensoredPlanet, an organization that monitors internet censorship, researched a new DNS measurement strategy to improve the accuracy of detecting manipulation by using certificate validation and blockpage matching. This project quickly implemented these essential research findings into a production-ready code within Satellite—CensoredPlanet's remote measurement technique that detects DNS interference. The new code introduced two new measurement steps (certificate validation and blockpage matching) and eliminated inaccuracies the tool was previously measuring.

Organizations that monitor censorship can now more accurately track and report on DNS manipulation around the world, raise awareness of the tactic, and support efforts to combat it.

GreatFire in Turkmenistan

$200,000

GreatFire

In 2022, Turkmenistan's government aggressively cracked down on the use of VPNs in the country and blocked servers hosting VPNs—leading to near-complete internet shutdowns on several occasions. Despite this censorship, downloads of FreeBrowser (an Android mobile browser app with circumvention technology) increased substantially in December 2022 and the tool consistently ranks among the top 20 apps in the Turkmenistan Google Play Store. At the end of the period covered by FY 2022 funding, FreeBrowser had approximately 400,000 unique users in Turkmenistan, helping provide about 15% of the online population with uncensored access to the internet. OTF's funding supported the increased infrastructure costs associated with this surge in users.

OTF Resource Labs

OTF Resource Labs provide critical services to internet freedom projects which are not otherwise covered by OTF's other funding mechanisms. The Labs ensure internet freedom projects are as effective, secure, and accessible as possible.

Learning Lab

The Learning Lab helps OTF-supported projects with their communications needs and contributes to knowledge sharing among the internet freedom community. The Lab provides writing, editing, graphic design, and other support. Outputs range from final research reports and blog posts to promotional plans for new tools.

Simply Secure

$300,000

Superbloom Design (formerly known as Simply Secure)

Superbloom is a nonprofit organization focused on building technology that enhances and protects human rights by centering the needs of marginalized populations. The organization's experienced design professionals support projects by developing materials essential to communicating results. In doing so, Superbloom provides graphic design, visualization assistance, and training to OTF-supported projects.

Red Team Lab

The Red Team Lab strengthens the security of open source internet freedom software by providing security audits, advancing project software security best practices, validating project privacy and security claims, and more. These services 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. During the period covered by FY 2022 funding, the Lab performed 22 audits—improving the security of vital internet freedom technology tools like Tella (a human rights documentation tool) and Amnezia VPN (a free, open source, and easy-to-use circumvention tool).

7ASecurity

$104,556

7ASecurity

7ASecurity is an 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. The organization tests against all kinds of web applications, online services, hardware interfaces, mobile applications, libraries, and crypto tools. Their efforts support OTF's commitment to establishing high-level internet freedom technology privacy and security standards.

Secure Usability and Accessibility Lab

The Secure Usability and Accessibility Lab offers secure usability and user-interface assistance, as well as accessibility assessments for internet freedom and digital security tools, to help software development teams recognize and solve usability and accessibility challenges that could hamper tool adoption in repressive contexts. Through the Lab, OTF partners with service providers that offer secure usability and accessibility coaching, consultation, and audits that help protect the internet freedom community and advance the accumulation of practical knowledge through peer-to-peer learning.

Simply Secure

$100,000

Superbloom Design (formerly known as Simply Secure)

Superbloom is a nonprofit organization 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. Services include secure usability audits, user experience (UX) reviews, user research, and strategy consultations.

Plaintext Design

$100,000

Plaintext Design

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

Ura Design

$100,000

Ura Design

Ura Design provides user experience, accessibility, visual communication, and innovative design services to internet freedom and open source communities. Their team is based in Albania, Germany, France, and Spain. They have supported over 100 open source and privacy-preserving technology tools and contribute to various internet censorship and security research projects.

Localization Lab

$804,864

Localization Lab

The Localization Lab helps expand the reach of internet freedom tools by making open source and public-interest technology available to underrepresented communities in over 200 languages. In working to secure equal access to information and better representation online, the Lab connects a community of more than 7,000 volunteer language contributors and a broad network of human rights and civil society organizations with developers and content creators of digital-safety resources.

Research Fellowships

The Information Controls Fellowship Program (ICFP) supports researchers examining how governments in countries, regions, or areas of OTF's core focus are restricting the free flow of information, cutting access to the open internet, and implementing censorship mechanisms.

Evaluating Privacy and Security of WeChat

$15,000

Mona Wang

ICFP Fellow Mona Wang investigated the data privacy and security practices of WeChat, the most popular messaging and social media platform in China (and third most popular in the world, with over 1.2 billion monthly active users). Many individuals inside China, as well as diaspora populations, use WeChat out of necessity rather than choice. For vulnerable populations that must use the application, precise threat modeling is of utmost importance. Wang found that the app collects more usage data than is disclosed in its privacy policy, with most fine-grained tracking data being sent during Mini-Program execution (Mini Programs are apps accessed within WeChat).

Reverse Bloatware in Central America

$70,000

Beau Kujath

In Mexico, government-sponsored mass and targeted surveillance using spyware is particularly pronounced due to the region's complicated history relating to the authorities' influence over the flow of information and the large amount of applications that are pre-installed on end devices ("bloatware") by powerful entities. Mobile bloatware apps are a major security threat to end-users because they commonly have root access to potentially install packages, access encrypted messages, or make escalated changes to a device. ICFP Fellow Beau Kujath analyzed nine suspicious apps in Latin America to determine the level of encryption, type of information collected (and how clear it is for users that this data is being retrieved), and security level of the app update processes. Kujath found that major commercial apps in Latin America have the potential to put their users at risk with demonstrable security and privacy issues.

Investigation of HTTPS Interception from a Global Perspective

$94,000

Alexandra Dirksen

ICFP Fellow Alexandra Dirksen investigated the possibility of mass state surveillance through an attack known as "HTTPS eavesdropping," an interception attack in which the attacker cooperates with a Certificate Authority (CA) to obtain a rogue certificate—thereby circumventing traditional protection mechanisms.

In cryptography, a CA is used to store, sign, and issue digital certificates certifying ownership of a public key for secure browsing protocols of the internet. Dirksen's research examined the development and use of Russia's domestic Certificate Authority. As part of the project, Dirksen created a cross-regional collection of certificates for the same websites through Secure Socket Layer probing, which could reveal anomalies in the Web PKI and thus, potential HTTPS interception.

Hardware Restrictions and Information Controls

$94,000

Joshua Beaker

ICFP Fellow Joshua Beaker examined how the system design of popular mobile devices can be used in closed spaces for information control. This research was significant because the implementation of restrictions and monitoring through hardware is nearly impossible to overcome on a per-user basis. Beaker worked on developing glitching tools to help researchers better understand existing—and potential—hardware security controls.

Monitoring Censorship with Comprehensive Client-Side Error Logging

$94,000

Amir Gh

Censorship systems are constantly changing strategies and evolving in an effort to control the free flow of information online. In turn, it is imperative for anti-censorship systems to adapt quickly to neutralize deployed tactics and force censors to pursue tedious, manual work. Identifying these tactics requires testing and measuring the censorship systems from many different connection points and aggregating and analyzing the collected data to derive a new strategy that can be swiftly deployed. ICFP Fellow Amir Gh's research effort helped develop tools and frameworks for measuring network disruptions and blocking through a comprehensive set of network-level error logging and reporting to a designated target.

USAGM Entity Support

OTF's USAGM Entity Support initiatives are tailored, innovative privacy-enhancing and censorship circumvention solutions for USAGM networks and their journalists.

Digital Security Resource Animations for USAGM Network Journalists

$27,250

Aisuluu Tekimbaeva

This project created 12 animated videos in Russian, English, French, Spanish, and Kyrgyz on key digital security and circumvention topics for use by USAGM network journalist colleagues and their training teams. It also helped integrate support for Advocacy Assembly, a free online training platform for human rights activists, campaigners, and journalists.

Guardian Project

$696,642

Oliver+Coady Inc.

The Guardian Project uses their expertise in the anti-censorship space to help USAGM broadcasters reach audiences experiencing heavy censorship and even shutdowns. This entails the creation, deployment, and maintenance of mirror sites for USAGM entity language services (which allow direct access to USAGM content and other internet content without the need for a separate circumvention app), and AnyNews-style progressive web apps as an alternative distribution strategy. Guardian continues to develop a shutdown preparedness kit to help USAGM content reach intended audiences and to keep journalists safely connected with sources under adverse scenarios. OTF's funding also provided Guardian with the project management resources to develop, deploy, and manage these circumvention solutions.

Psiphon SDK and Promotion/Circumvention

$901,103

Psiphon Inc.

Psiphon is a free, open source, multi-platform software that helps people circumvent censorship and connect to content on the internet. It is one of the most technically advanced and widely used circumvention tools in the world, providing uncensored access to USAGM network content, as well as access to the broader internet, for more than 37 million people each month. Psiphon's technology uses a combination of secure communication and obfuscation technologies and has proven consistently effective in the world's most highly censored areas. OTF provided support for SDK (software development kit) services and API (application programming interface) access for circumvention support for USAGM network applications. The SDK service has the capability to support up to 500,000 simultaneous users across all services.

Psiphon delivers nearly 2 billion page views of USAGM content per year, enabling 24 USAGM entity language services to reach audiences under some of the most repressive censorship conditions in the world, including China, Iran, Russia, and Myanmar.

Tor Secure Access Package & Maintenance

$354,589

Tor Project

Tor is a free, open source software enabling anonymous communications. The Tor Secure Access Package involved a holistic solution for each USAGM network entity's website and provided an end-to-end solution for web content distribution in censored or surveilled areas. The project deployed Onion Services (Tor's secure web browsing service) for all 113 USAGM services across Radio Free Europe/Radio Liberty, Voice of America, Middle East Broadcasting Network, Office of Cuba Broadcasting, and Radio Free Asia. In addition, USAGM language services received a custom landing page to promote to their audiences, a dedicated point-of-contact at Tor, and training and support on censorship-circumvention best practices. The project also maintained this essential USAGM Tor infrastructure.

OutlineVPN Into the Pangea App

$17,340

CAMELO IT SOLUTIONS s.r.o.

This project integrated and tested the performance of the Outline SDK as a possible in-app circumvention solution for censored services using the Pangea app. Outline SDK is a cross-platform library and set of tools for app developers to easily reuse OutlineVPN's advanced networking strategies to mitigate even the most complex network-level interference. The Pangea app is a unique, custom-built platform used by Radio Free Europe/Radio Liberty and other USAGM entities.

OPEN TECHNOLOGY FUND

FY 2022

ANNUAL REPORT