Written Statement

Laura Cunningham
President
Open Technology Fund

United States Senate Committee on Foreign Relations
Subcommittee on East Asia, the Pacific, and International Cybersecurity Policy

"Cyberspace Under Threat in the Era of Rising Authoritarianism and Global Competition"

24 September 2024

Chairman Van Hollen, Ranking Member Romney, and distinguished Members of the Subcommittee, thank you for inviting me to testify today on the threat of digital authoritarianism and how we can ensure the global digital ecosystem reinforces our democratic principles.

Today two-thirds of the world's population – nearly 5.5 billion people – live in a country where the global internet is censored.

And this number is only increasing as authoritarian governments around the world are harnessing technological advances to increase the scale, scope, and efficiency of digital repression. But this is not merely a technical challenge. At its core, it is a normative contest to determine whether governments use technology to entrench authoritarian control or empower democratic freedoms.

About OTF and Internet Freedom

The Open Technology Fund (OTF) was established over a decade ago – with bipartisan support and funding from Congress – in recognition of the dire consequences that unchecked digital authoritarianism poses to democratic principles, our national security, and human rights globally.

Today, OTF is a Congressionally-authorized non-profit funded through a grant from the U.S. Agency for Global Media. OTF's mission is to advance internet freedom in repressive environments by supporting the research, development, implementation, and maintenance of open source technologies that provide secure and uncensored access to the internet and counter attempts by authoritarian governments to control the internet and restrict freedom online.

OTF fulfills this mission by providing funding and support services to individuals and organizations around the world that are addressing threats to internet freedom with technical solutions. Broadly speaking, we invest in technologies that provide uncensored access to the internet to those living in information restrictive countries; and tools that protect at-risk

populations, like journalists and their sources, from repressive authoritarian surveillance. For example:

- We provide anti-censorship technologies – specifically VPNs – to over 45 million people each month in countries where they would otherwise be cut off from the global internet, including China and Russia.

- We also support critical digital security technologies that enable journalists and human rights defenders working in repressive environments, like Myanmar and Cuba, to communicate, report, and share information safely.

- In addition, we invest in peer-to-peer and decentralized messaging tools that allow users to stay connected and access critical information during internet shutdowns, like those implemented by the Iranian government to suppress the anti-regime protests following the death of Mahsa Amini.

In total, over two billion people globally use OTF-supported technology daily, and more than two-thirds of all mobile users have OTF-incubated technology on their devices.

OTF's primary focus is on the human rights abuses that result from the application of repressive technologies. However, the threat I want to focus the Subcommittee's attention on today is far broader. The core challenge the United States must confront is a new authoritarian model that information control technologies have enabled, and not merely the technologies themselves.

Once considered politically extreme and technically implausible, digital authoritarianism has now been adopted worldwide as more and more governments are substituting repressive technical shortcuts for the hard work of good governance in a bid to control their populations in ways that were previously unimaginable.

Today, there is no longer a meaningful distinction between digital authoritarianism and authoritarianism of any other kind as online information control has become foundational to a newly possible form of illiberal governance. This is the greatest danger to democracy of our time, with profound implications for our democratic principles, national security, and global economic competitiveness.

Online Censorship: Blocking Free Expression & Independent Information

Online censorship has become a central component to digital authoritarianism, facilitating easy and effective information control, which stifles dissent, eliminates government accountability, and obfuscates the truth. As a result, online censorship has become commonplace around the world.

According to Freedom House's Freedom on the Net Report, online censorship is at a historic high, with more governments censoring the internet than ever before. While many are familiar

with the long history of internet censorship in the most extreme authoritarian contexts, like Russia and Iran, the reality is that online censorship is now normalized in dozens of countries around the world, including Belarus, Egypt, Ethiopia, Hungary, Kazakhstan, Myanmar, Nicaragua, Pakistan, Turkey, Uganda, Venezuela, Vietnam, and many more.

As online censorship has become more and more pervasive, autocats are emboldened to utilize far more aggressive and blunt censorship techniques, including total internet shutdowns. Rather than narrowly blocking specific content and websites that a regime deems undesirable, authoritarians now regularly sever their citizens' connection to the internet entirely. For example, following the military coup in Myanmar, the junta implemented an internet shutdown, cutting millions of people off from the global internet in order to solidify political control. In fact, in 2023, 39 governments shut down the internet 283 times – a new record.

To further enhance their control, authoritarian regimes are leveraging AI to augment their censorship efforts to increase the scale, speed, and efficiency of online censorship.For example, the Russian government launched their own internet censorship and surveillance system called Oculus in February 2023. The new AI system automatically detects and blocks content the government considers "undesirable." And many other countries are following suit: at least 22 other countries now mandate or incentivize digital platforms to deploy machine learning to remove disfavored political, social, and religious speech at a rate and magnitude that was previously impossible for human censors to achieve.

With truthful information broadly blocked, digital authoritarians are able to perpetuate disinformation unchallenged. For example, Chinese media regularly reports that COVID originated from a U.S. lab; while in Russian media, the full-scale war in Ukraine is righteous and legitimate; and there are countless other examples. These narratives follow classic propaganda patterns designed to project domestic strength and unity, vilify perceived enemies; and establish a new, widely accepted "truth" that further cements political control.

Ultimately, online censorship erodes democracy by obscuring the truth, disempowering citizens, and creating extreme national echo chambers that create a more fractured and dangerous world.

Mass Real-Time Surveillance: Silencing Dissent at Home

Once only available to a small number of well-resourced autocrats, authoritarian governments are now pairing online censorship technologies with highly advanced surveillance tools. Distinct from more narrow forms of technical surveillance conducted within strictly prescribed limits and specific legal frameworks, leading digital authoritarians have normalized the unencumbered use of the world's most sophisticated surveillance tools to harass, intimidate, imprison, and stifle political opposition.

In the past two years, authoritarian governments – led by China and Russia – have taken extraordinary steps to expand their domestic surveillance capabilities. They have asserted

authority to digitally collect personal information; engaged in widespread location tracking, tracing individuals' every movements; and pursued aggressive offline punishments for online activities.

Nowhere is the evolution in sophistication and scale of mass surveillance more evident than in China. The Uyghur community in Xinjiang experiences perhaps the most extreme version of surveillance imaginable. They are subject to constant monitoring from facial recognition-equipped cameras, mandatory use of surveillance software, police checkpoints, and informants. Police in Xinjiang use an app to collect massive amounts of personal information, which the app then uses to flag activities considered to be suspicious. The use of these tactics, and others like them, led directly to the imprisonment of as many as one million mostly ethnic Uyghur and Kazakh people.

Similarly in Russia, authorities are harnessing the power of biometric surveillance to target anyone critical of Vladimir Putin's regime and the full-scale war in Ukraine. More than 60 regions in the country have installed half a million cameras with facial recognition technology. A 2023 report revealed this technology played an important role in the arrests of hundreds of protesters in Russia.

As if these technical advancements and the resulting domestic repression were not alarming enough, research supported by OTF found that over the last decade, more than 110 countries purchased, imitated, or received training on information controls from China or Russia. For example, the Chinese telecom company ZTE is helping Venezuela develop a smart ID card that many fear will be used by the government as a powerful surveillance tool. The Serbian government also turned to a Chinese telecom company, acquiring a 1,000-camera-strong surveillance system from Huawei. And Huawei has built over 70% of the 4G networks on the African continent, raising concerns around surveillance and user privacy. Validating these fears, the Wall Street Journal revealed that Huawei technicians had helped the governments of Uganda and Zambia spy on political dissidents.

The near-universal reach of mass, domestic surveillance effectively contains and constrains billions of people worldwide. One of the more pernicious aspects is the extent to which the specter of surveillance, and very real fear of real world consequences, incentivizes a culture of self-censorship, further perpetuating unchecked authoritarian control.

With such powerful tools at their disposal, few authoritarians are willing to stop at their own national borders. Increasingly autocrats are attempting to extend their reach, and impose globally the same level of absolute control that they wield within their national boundaries.

Commercial Spyware: Powering Transnational Repression

The impunity with which authoritarians are able to surveil their citizens at home and abroad has been supercharged by the ready availability of commercial spyware products. These technologies have been used disproportionately to intimidate and harass journalists, human

rights defenders, and political opposition figures. In the last decade, at least 75 countries – nearly 40 percent of all nations – have acquired commercial spyware, giving rise to a lucrative mercenary industry, now worth billions, that is flourishing despite U.S. import restrictions and sanctions against some of the known actors in this space.

Today, any government with an interest in surveilling its citizens at home and abroad can easily acquire the tools necessary to conduct near real-time mass surveillance as a result of off-the-shelf, enterprise solutions to any malicious surveillance need.

Perhaps the most highly-publicized of these tools is Pegasus, the chief product sold by the NSO Group, which has been used largely by governments to target thousands of human rights activists, journalists, politicians, and government officials across 50 countries. Public reporting has found that from 2016 to 2021, at least 180 journalists were selected for potential targeting in 20 countries, including those with limited or declining media freedom. Our colleagues at Radio Free Europe/Radio Liberty in Azerbaijan and Armenia are among these. Infamously, family members of Jamal Khashoggi were targeted before and after his murder by Saudi operatives; and separately, as were members of the UK Prime Minister's Office.

The NSO Group is only one actor in the surveillance industry ecosystem, yet has caused tremendous, specific harm. And there are others, multiplying at a rapid pace, whose products are wielded to silence and control. The Russian Federal Security Service is reported to have used COLDRIVER in an extensive campaign against Russian and Belarusian non-profit organizations active abroad, Russian independent media in exile, and at least one former U.S. Ambassador. Similarly, the government of Egypt deployed Intellexa's Predator spyware to surveil a former political opposition figure living in Turkey and an exiled journalist. Predator is also known to have targeted, although not necessarily infected, members of the U.S. Congress including Congressman Michael McCaul, the Chairman of the House Foreign Affairs Committee.

What is particularly striking about each of these examples is the audacity with which governments targeted individuals outside their borders regardless of victims' nationality. This element is the true autocratic innovation inherent in commercial spyware, which has accelerated transnational repression, making it too straightforward and mainstream.

Recommendations

Authoritarian use of technology could convince some that these tools are inherently oppressive, but nothing could be farther from the truth. It is crucial to remember – as this Subcommittee knows well – that the internet offers extraordinary potential for global connection, inclusive democratic participation, and economic growth at a speed and on a scale unprecedented in human history. Digital technologies fuel learning, improve healthcare, drive scientific and economic development, and enhance government services. While authoritarians would like us to believe otherwise, the reality is that a free and open internet meaningfully improves the lives of billions of citizens worldwide.

It is clear that the true appeal of the digital authoritarian model is not its supposed benefits to citizens, but its simplicity: it boasts a novel tech stack; provides compelling solutions to short-term governance problems; and is increasingly accepted as legitimate. In short, it is cheap and easy to become a digital authoritarian.

To counter its spread effectively, we must raise the costs of digital authoritarianism while offering a positive, democratic vision in exchange. This will require action by multiple stakeholders.

Raise the Cost of Digital Authoritarianism

Digital authoritarians have functionally purchased their hold on power by spending billions of dollars to control what billions of people can say, share, and access online. And for the most part, they have gotten their money's worth. While the United States and its allies cannot match autocratic investment dollar for dollar, we must proportionally increase our efforts to make digital authoritarianism more difficult, more expensive, and less effective.

First, we need to increase our investments in internet freedom technologies to reduce the efficacy of repressive tools. People living under digital authoritarian regimes are our greatest ally in this cause, and we must ensure they have tools and technologies to counter the worst effects of authoritarian digital controls for themselves. This is why OTF supports tools that mitigate the effects of even the most advanced control technologies. When Iran cuts off access to the internet to stifle protests and silence critics, we provide shutdown resistant communications tools to keep people connected. When Belarus attempts to surveil journalists, we can keep their communications with their sources safe. When Russia censors objective reporting on the war in Ukraine, we can unblock independent news sites for tens of millions of people.

Second, we need to empower civil society coordination to bring it in line with the speed of authoritarian information sharing in order to increase the cost of digital authoritarianism.

Digital repression is now "plug and play," and even comes with great customer service. Through both authoritarian information sharing and a robust market for commercial surveillance tools, governments looking for easier answers find them in this model. And the effects on those they govern are tragic.

In many countries, civil society organizations are working individually in isolation to identify and counter digital threats to their organizations and communities. Few have the resources or expertise to keep up with the pace or sophistication of new surveillance threats emerging from globally connected authoritarians. There is an urgent need for coordination among civil society organizations to collect, analyze, and ultimately mitigate digital threats and attacks. OTF is already investing in such coordination.

Beyond the tangible benefits to those under attack, this coordination makes more costly digital authoritarians' means of control. When an authoritarian purchases an expensive digital exploit it will prove effective for only a matter of days rather than for years on end.

Strengthen the Democratic Model

While we must counter digital authoritarianism where it originates – in China, Iran, Russia – we must also advocate for a better model where it is spreading, in many cases to weakly institutionalized states whose populations will be materially affected by their governments' choice of governance technologies.

The United States and its allies should advance a positive vision of a global internet that reinforces our democratic principles. In order to be successful in this endeavor, we must show that it is possible to protect national security and combat crime without undermining human rights and our democratic values.

While technologies themselves are generally value neutral, their design, deployment, and application rarely are. In many cases, states are confronted with legitimate governance challenges that digital authoritarian models solve for leaders who are unconcerned with the human rights cost. We must demonstrate that there is a better way to solve these problems that harnesses the positive power of newly-emergent technologies within a rights-preserving framework.

The private sector will also be vital to realizing this new model. As U.S. companies have been collateral damage in authoritarians' quest for control, they share common cause. Digital authoritarianism excludes the U.S. private technology sector from important markets unless they are willing to make unreasonable accommodations to authoritarian demands that conflict with many of these companies' stated values. The private sector is often left with the choice between their bottom line and respect for democratic values and human rights. We must strive to keep global markets open and fair without sacrificing principles.

This is a shared challenge, and we need shared solutions. The public sector, private sector, and civil society benefit from a free and open global internet. We must collectively defend it.

Conclusion

The challenges posed by digital authoritarianism are daunting and the path to a competing model is hard. But it is unquestionably worthwhile. Given a choice, many countries will opt for free, human rights-respecting digital governance approaches – if they are shown that this is possible. But we need to lead the way. If we don't, China and Russia certainly will.

Thank you and I look forward to your questions.