AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

119th CONGRESS
1st Session

Printed for the use of the
Commission on Security and Cooperation in Europe

The MAX App: Russia's Pocket-Sized Approach to Mass Surveillance

DECEMBER 2, 2025

Briefing of the
Commission on Security and Cooperation in Europe

Washington: 2026

Commission on Security and Cooperation in Europe
234 Ford House Office Building
Washington, DC 20515
202–225–1901
csce@mail.house.gov
http://www.csce.gov
@HelsinkiComm

Legislative Branch Commissioners

SENATE
ROGER F. WICKER, Mississippi *Chairman*
SHELDON WHITEHOUSE, Rhode Island
Ranking Member
JOHN BOOZMAN, Arkansas
KATIE BRITT, Alabama
JOHN FETTERMAN, Pennsylvania
JEANNE SHAHEEN, New Hampshire
TINA SMITH, Minnesota
THOM TILLIS, North Carolina
MIKE ROUNDS, South Dakota

HOUSE
JOE WILSON, South Carolina
Co-Chairman
STEVE COHEN, Tennessee *Ranking Member*
ROBERT ADERHOLT, Alabama
EMMANUEL CLEAVER, Missouri
LLOYD DOGGETT, Texas
JAKE ELLZEY, Texas
RICHARD HUDSON, North Carolina
GREG MURPHY, North Carolina
MARC VEASEY, Texas

Executive Branch Commissioners

Department of State, *to be appointed*
Department of Defense, *to be appointed*
Department of Commerce, *to be appointed*

ABOUT THE ORGANIZATION FOR SECURITY AND COOPERATION IN EUROPE

The Helsinki process, formally titled the Conference on Security and Cooperation in Europe, traces its origin to the signing of the Helsinki Final Act in Finland on August 1, 1975, by the leaders of 33 European countries, the United States and Canada. As of January 1, 1995, the Helsinki process was renamed the Organization for Security and Cooperation in Europe [OSCE].

The membership of the OSCE has expanded to 57 participating States, reflecting the breakup of the Soviet Union, Czechoslovakia, and Yugoslavia.

The OSCE Secretariat is in Vienna, Austria, where weekly meetings of the participating States' permanent representatives are held. In addition, specialized seminars and meetings are convened in various locations. Periodic consultations are held among Senior Officials, Ministers and Heads of State or Government.

Although the OSCE continues to engage in standard setting in the fields of military security, economic and environmental cooperation, and human rights and humanitarian concerns, the Organization is primarily focused on initiatives designed to prevent, manage and resolve conflict within and among the participating States. The Organization deploys numerous missions and field activities located in Southeastern and Eastern Europe, the Caucasus, and Central Asia. The website of the OSCE is: <www.osce.org>.

ABOUT THE COMMISSION ON SECURITY AND COOPERATION IN EUROPE

The Commission on Security and Cooperation in Europe, also known as the Helsinki Commission, is an independent U.S. Government commission created in 1976 to monitor and encourage compliance by the participating States with their OSCE commitments, with a particular emphasis on human rights.

The Commission consists of nine members from the United States Senate, nine members from the House of Representatives, and one member each from the Departments of State, Defense and Commerce. The positions of Chair and Co-Chair rotate between the Senate and House every two years, when a new Congress convenes. A professional staff assists the Commissioners in their work.

In fulfilling its mandate, the Commission gathers and disseminates relevant information to the U.S. Congress and the public by convening hearings, issuing reports that reflect the views of Members of the Commission and/or its staff, and providing details about the activities of the Helsinki process and developments in OSCE participating States.

The Commission also contributes to the formulation and execution of U.S. policy regarding the OSCE, including through Member and staff participation on U.S. Delegations to OSCE meetings. Members of the Commission have regular contact with parliamentarians, government officials, representatives of non-governmental organizations, and private individuals from participating States. The website of the Commission is: <www.csce.gov>.

The MAX App: Russia's Pocket-Sized Approach to Mass Surveillance

DECEMBER 2, 2025

The MAX App: Russia's Pocket-Sized Approach to Mass Surveillance

---

December 2, 2025

Commission on Security and Cooperation in Europe
Washington, DC

The briefing was held from 2 p.m. to 3:08 p.m., Room 2358–C, Rayburn House Office Building, Alanna Novetsky, Communications Director, Commission on Security and Cooperation in Europe, presiding.

Ms. NOVETSKY: Good afternoon. My name is Alanna Novetsky, and I am the communications director with the U.S. Helsinki Commission. I am pleased to welcome you to this briefing on "The MAX App: Russia's Pocket-Sized Approach to Mass Surveillance." Thank you all for joining us.

Before I turn it over to our esteemed members of our panel, I will share a few words about why we are choosing to focus on this issue now. On a trip to Kyiv in September, my colleagues and I met with members of civil society who support and help evacuate Ukrainians living under Russian occupation. They discussed how the information environment there has made every aspect of their jobs more difficult. Occupation authorities flood Ukrainians with propaganda, and search their devices and homes for any tools to connect with the open internet and communicate freely. Ukrainians live in a constant State of fear. They do not know who to trust or what to believe.

For the Kremlin, creating an information bubble in occupied Ukraine is central to their genocidal project to erase the Ukrainian State. By purging occupied territories of any means of connection with the outside world, authorities believe they can isolate and dishearten the population, discourage resistance, and brainwash the next generation.

Yet, despite relentless pressure, Ukrainian parents and grandparents continue to risk everything to find virtual and physical pathways out of this hell for their children. They teach their children Ukrainian in secret and use VPNs to give them a Ukrainian education. They find ways to talk to their neighbors undetected to help avoid conscription into the Russian army. In some cases, they find routes out of the occupied territories and lead their families through treacherous escapes. Through their kids, using the limited resources and technology they have, these parents and grandparents keep hope alive for a future in which Ukraine is free and united.

Over the past several months, the Kremlin has doubled down on its efforts to digitally monitor and isolate those under its thumb in Russia, Ukraine, and elsewhere.

They are implementing a novel approach to censorship and surveillance that pairs old-school authoritarian tactics with software solutions that allow authorities to police people's digital lives on their personal devices. As part of this strategy, they have launched MAX, a super app that gives Russian officials wide-ranging access to users' messages, contacts, internet usage, and location—which is the topic of this briefing.

With that, I am honored to introduce our panelists, who will discuss the implications of Russia's approach to wide-scale digital surveillance, the potential for Russia to export this paradigm further beyond its borders, and strategies to circumvent and counter this approach to repression.

First up, we will have Anastasiya Zhyrmont. She spearheads Access Now's Eastern Europe and Central Asia policy work, building coalitions, influencing stakeholders, and bringing digital rights issues in restrictive environments into the international spotlight. Anastasiya previously worked as an advocate for the rights of people with disabilities and currently serves as a board member for Inclusion Europe.

Laura Cunningham is the president of the Open Technology Fund, a nonprofit organization supporting the counteraction of repressive censorship and surveillance globally. Laura has over a decade of experience working on internet freedom across a variety of donor, nonprofit, and government organizations. Prior to joining OTF, Laura was the senior advisor for internet freedom in the U.S. State Department's Bureau of Democracy, Human Rights, and Labor, where she led the Department's internet freedom programs focused on technology development, digital security, internet policy advocacy, and research.

Last but not least, we have Justin Sherman, who is the founder and CEO of Global Cyber Strategies, a D.C.-based research and advisory firm, an adjunct professor at Georgetown University's School of Foreign Service, and a distinguished fellow at Georgetown's Law Center on Privacy and Technology. He was previously a fellow at Stanford's U.S.-Russia Forum, where he participated in track-two dialogs with Russian counterparts on international security issues. Justin has consulted for and advised CEOs, government officials, investors, attorneys, product managers, communications strategists, and threat intelligence teams, including volatile, complex, and high-risk scenarios. He has consulted on projects and programs for organizations ranging from HBO to DARPA.

Now I will turn it over to Anastasiya for her opening statement. Once everyone has had an opportunity to give their opening remarks, I will ask a round of questions, and then we will open it up to audience questions. So, Anastasiya.

Ms. ZHYRMONT: First of all, thank you so much for the opportunity to appear before you today. Of course, it is an honor for me to address the issue of accelerating crisis of digital censorship and surveillance in the Russian Federation, including the growing role of MAX messenger, a state-controlled tool that exposes users to State surveillance, undermines their privacy, exposes them to State propaganda, and further limits access to independent information.

Well, first of all, let me start by outlining the current status of the digital space within Russia and how authorities are driving the country into the complete shutdown and informational blockade from the rest of the world. Since the full-scale invasion of Ukraine, Russian authorities have blocked access to almost all websites of independent media, NGO's, and global social media platforms. Facebook and Instagram—whose parent company, Meta, was declared extremist organization in 2022—are banned, as TikTok, X, Discord, and even Signal. YouTube is heavily throttled, so it is barely functional for many users within Russia. Starting this summer this year, authorities went as far as they also disabled voice calls on Telegram and WhatsApp, which are the two last remaining accessible platforms in Russia. Recent reports indicate that WhatsApp is experiencing dysfunctions. It is not functioning well in many regions of Russia, and this has led some experts to believe that it soon will be blocked as well.

Adding to all of this, since May this year, millions of Russians and people in the occupied territories have been experiencing mobile internet shutdowns. What started as sporadic outages has now escalated to frequent, in some regions even daily disruptions of mobile and cellular data services. Since September this year, Russia has also begun whitelisting during the internet shutdowns, meaning that only a narrowly approved list of websites, usually state-controlled, is accessible during the shutdowns. Usually, it includes services such as Yandex, state-controlled media outlets, et cetera.

It has been done to promote MAX messenger, not only a messenger in itself but a comprehensive surveillance tool, which now comes preinstalled on all the devices sold in Russia starting September 1st. According to independent assessments, MAX does not merely record user messages and metadata; it embeds deep tracking analytics and compiles a wide—a wide digital dossier on the user, mixing personal identifiers like gender, age, your email, your phone number with external account IDs linked to other social media and the usage data.

Also, precise geolocation tracking is built in, so if granted“Always On” location permission, MAX can report your real-time movements. In repressive conditions, as you can imagine, this can expose attendance at political protests, political gatherings, or simply trace your mobility and all of your contacts.

Another feature of MAX is also the collection of your search history within the app, linked to your identity. In light of the recent legislation that targets people who are not only searching for extremist material—including materials by independent media—the app can potentially expose such users to heavy fines or even tougher penalties. The app is reportedly capable of more invasive operations like secretly switching on your microphone, your camera, or even screen recording.

Despite all of those risks, it is becoming more and more popular due to the combination of aggressive promotion by the authorities, but also the way essential services are funneled in ways through it. Many of our partners on the ground, parents and students, report their school group chat, for instance, often circulates official reminders that you need to install this app. Beyond schools, regional authorities in some areas went as far as tying access to critical public safety notifications, such as air raid alerts or emergency alerts in the app. Since November 5, the MAX app has also been launched in Belarus, Kazakhstan, Kyrgyzstan, Uzbekistan, Tajikistan, Armenia, and Azerbaijan.

At the same time, it is very difficult for users to still make resistance and escape such a type of control because of the ongoing crackdown on circumvention tools and privacy tools, such as VPNs. In recent years, Roskomnadzor, the censorship body in Russia, has pressured major big tech companies to remove VPNs from the App Store in Russia. Unfortunately, Apple, for instance, succumbed to this censorship request. As a result, more than 100 VPNs are right now unavailable in the App Store in Russia.

Just let me underline that without VPN and other security tools, people in Russia and in the occupied territories are deprived of ways to securely access independent information, to communicate privately, or to evade digital surveillance. This is why we as Access Now, but as civil society as a whole, we call on the governments to condemn the use of mandatory or state-controlled and preferred apps that collect invasive privacy data under the guise of national sovereignty, support civil society and digital rights group in exposing such invasive practices, but also providing resilience tools and digital security tools for the users in order to increase their safety; and to recognize that shutting down or reengineering the whole internet to serve State propaganda and surveillance is tantamount to curtailing freedom, dissent, and democracy. We also call on big tech companies and Apple not to concede to the Russian government's attempts and efforts to suppress freedom of expression and to, instead, restore all of the blocked and deplatformed VPNs in the App Store in Russia.

Thank you. I would love to answer any questions that you might have.

Ms. NOVETSKY: Thank you so much.

Yes, Laura, go ahead.

Ms. CUNNINGHAM: Wonderful. Thanks again for having us here today, Alanna. I am really excited to talk about such an important issue. I think, just kind of taking off of what Anastasiya started with, I think MAX really does represent a significant evolution in the Kremlin's approach to information controls. Obviously, has hugely concerning implications for freedom of expression, access to information, privacy, and security for Russian citizens. However, in this context, I think it is really important to remember that MAX, in and of itself, should not be our primary concern. Rather, the aggressive model of internet control that the implementation of MAX predicts is the true challenge that we are confronted with today.

As Anastasiya explained, since the full-scale invasion of Ukraine, the Russian government has demonstrated both the will and the technical capacity to implement a sophisticated model of total internet control. We refer to this in the Chinese context as the Locknet. The Russian government has not only brought a largely decentralized infrastructure to heel, but also instituted a centralized censorship regime and made significant strides toward even more totalitizing solutions, including the much-discussed Runet, and more recently and potentially more concerning, a Chinese-style Locknet supported in part by the implementation of MAX.

By capturing their citizens on a single app, the Kremlin, as Anastasiya said, can leverage backend control to far more effectively censor and surveil their citizens. Which serves to not only teach but reinforce self-censorship among citizens themselves. Simultaneously, the app provides all the information and services a citizen is supposed to need in Russia, thereby prescribing the bounds of what should and should not be permissible within the country. When that is combined with significant impediments to accessing the global internet or nonState platforms, such as censorship, meta-censorship, legal consequences, and offline consequences that we know are common in Russia, the stage is really set for near-complete information control.

If this model of control is successfully implemented over a long enough period of time, it is likely—and we have seen this happen in China—to fundamentally reengineer how Russian citizens think about, search for, and engage with independent media over the long term. I think—kind of to put it most simply, I think the Kremlin really hopes to force their people to choose between convenience and ease of a super app over freedom—over freedom, until they no longer have any meaningful conception of what the global internet looks like outside of this walled garden that has been created by the State.

In this context, I think it is really important that we not confuse tactics with a longer-term strategy. Our goal should not be to compete with Russia tool for tool. I do not think we should respond to MAX with the anti-MAX app. Rather, to provide a compelling alternative environment where Russian citizens can continue to actively connect to the global internet and engage with a diversity of technologies and information. In this formulation, success is not about eliminating MAX entirely but, more importantly, rendering it just irrelevant to the Kremlin's information control goals.

I think, honestly, in these terms in this moment, we—the U.S. Government has an upper hand. We are still able to offer Russian citizens access to the entire global internet, something that they clearly remember and desire. That is far more compelling than a single app is going to be. Think we need to work to honor and channel the desire that Russian citizens have to access tools and techniques to easily reach the global internet, and to help them to avoid the ever-increasing state-imposed friction and chokepoints designed by the Kremlin to discourage their access.

To do this, I think, from a technological perspective, there are two things that we really need to focus on. We need to support a diversity of tools and technologies, not that respond individually tool for tool or app for app but instead work collectively to undermine the Russian government's model as a whole. First, we should continue to facilitate Russian citizens' access to the global internet and independent information. This means continuing to support a range of secure privacy-enhancing circumvention tools and secure communication tools to empower Russian users and impede the Kremlin's ability to force citizens onto apps like MAX.

Second, we should simultaneously invest in new solutions to stay ahead of quickly evolving Russian information controls. In preparation for the next generation of Russian information controls, we should invest now in forward-looking internet freedom solutions, such as advanced circumvention techniques, novel security and privacy-enhancing technologies, and innovative shutdown mitigation tools that are becoming ever more critical in this environment, as Anastasiya pointed out.

I think the speed and scale with which the Russian government has prioritized and is investing in information controls only raise the stakes for the U.S. to support internet freedom and free expression in Russia. Currently, the population of Russia still remembers how to access independent information and connect to the wider world. Like I said earlier, as we have seen in China, they risk losing this muscle memory the longer the Russian government censorship remains unchecked.

Ms. NOVETSKY: Thanks so much, Laura.

Yes, Justin, go ahead.

Mr. SHERMAN: All right. Thank you. Thank you to the Commission as well for the chance to talk about an issue that, as my fellow panelists have said, is not just critical for human rights in Russia and Ukraine and the region, but also for U.S. and Western security as well. Hopefully, this will dovetail well with what we have just heard.

To step back for a second, over the past several decades, but especially the last 10 to 15 years, the Russian government has built out an extensive domestic surveillance apparatus. It spans phone and internet monitoring, mobile device surveillance capabilities, cyber actors that can break into devices and networks, facial recognition systems, biometric surveillance data bases, censorship and web blocking, and, among others, outright coercion. It is, as Julien Nocetti has put it, a dictatorship of law approach to internet policy, fused, I would add, with sophisticated State intelligence capabilities, and what Masha Gessen has rightfully called “the economy of terror” approach to information control. The MAX app, developed by VK [VKontakte], is therefore part of this broader surveillance ecosystem.

The mixed origins of where this comes from, as we all know, we had, you know, Soviet security apparatuses that were migrated to their post-USSR collapse forms, keeping many of the same technology and surveillance capabilities. You had law enforcement, you know, systems that were set up in the 1990’s that were then converted into what we now see as the form of modern internet monitoring in Russia. All the way to the paranoia and distrust of the internet, the internet awakening of the Kremlin I call it sometimes, across 2008 Russo-Georgian war, the 2010’s Arab Spring, the 2013 Snowden leaks—coming to view the internet as not just a threat to regime security but as a tool of the U.S. Government—which, of course, many here would find fanciful—but a tool of the U.S. Government to project power. All to say, the Putin regime today views the internet both as a threat to regime security and a weapon to wield against Russia’s enemies. The MAX app is a direct follow-on of this worldview.

As we heard, MAX is built by the Russian tech company VK. As of September 1st, it is required to be installed on every new phone sold in Russia, implemented through coercive and legal pressure, both on phone-selling companies as well as individuals who will use those devices. MAX enables users to do all of the things we heard, messaging, and much more. The Kremlin’s vision is much more expansive—talking about replacing physical documentation, enabling people to verify their identities entirely through the app, both for business and government purposes, replacing, as we heard, State alerts, forms of communication, and other document-sharing systems that currently exist on State servers, or in less-centralized fora.

At the same time, as we heard, as the Kremlin has required MAX’s installation on devices in Russia, it has also blocked alternatives. Again, something we have seen time and time again as a means of pushing people onto a particular platform. I will also add that VK, much like Kaspersky and other Russian tech companies, may have had the opportunity 25 years ago to exist fairly independently from the Kremlin. That is obviously not the case today. These companies have long ago more than willingly bent the knee to the Putin regime.

When past Russian domestic tech or digital surveillance efforts have failed in recent years, it is typically fallen victim to at least one of three factors. [A], terribly built, dysfunctional technology. [B], a lack of political will, meshed with bureaucratic incompetence. Or, [C], both. We will put corruption under the incompetence umbrella, right? The problem here, at least from my vantage point, is MAX may be poised to avoid all three of these stumbling blocks. You have a product from a fairly successful consumer-facing technology company. You have, as we have heard, seemingly enforced legal requirements in Russia on device manufacturers, on individuals to use it. The technical throttling of alternatives. We see that political will. We see that capability there now.

Further complicating the challenge ahead is Russia’s growing techno-isolationism, leaving Russians with fewer technological systems in general that are not heavily Russian state-monitored and controlled. If they are not Russian these days, they are more, in fact, in some cases, from China than they are from Europe, or the U.S., or Japan, or elsewhere.

You have persistently growing Kremlin paranoia, as mentioned, about Western tech platforms. You had Meta designated as a terrorist organization 3 years ago, as an example of that view. You also have suboptimal or harmful policy decisions from U.S. tech companies. In some of these cases, U.S. tech firms, such as with YouTube, are dealing with highly complicated tradeoffs, decisions, often more so than the public might appreciate, in terms of information access, censorship, and content requests.

At the same time, you have other firms making disastrous decisions, such as with Apple and Google a couple of years ago, deciding to open local offices in Russia, which, of course, demonstrates some degree of naivety about the risk. All to say, as we have heard, MAX threatens human rights in Russia. As was mentioned, I recently wrote in The Atlantic about this as well. Russian forces are stopping individuals entering and leaving temporarily occupied territories to do technical inspections of devices, the details of which we will not get into, but to include looking for the MAX app on people's phones. As mentioned, it is also now permeating the near abroad.

Then the second set of concerns really, to me, relates to broader U.S. and Western security, which is, as Laura was just saying, not every country has the political will, the intelligence sophistication—as in intelligence agency sophistication—the policing apparatus, the tech talent to control and surveil in the way China does. Not every country has the same underlying digital infrastructure layout as China does, which is quite centralized. In many other countries, like Russia, it is much more diffuse. Enter then an approach that requires less technical centralization, that requires less of a broader tech talent base to implement, and that may require less financial investment to carry out. Yet, as some, you know, have already analogized MAX to China's WeChat, as an attractive means of conducting State surveillance, of trying to suppress dissent and free expression, or—this was not mentioned yet—of trying to root out Western spies, and adverse Ukrainian spies, and an adversarial and authoritarian regime, through this messaging app.

Looking forward, there are several solutions that Congress can undertake in this area. These include renewed funding, as was mentioned, for anticensorship circumvention capabilities, privacy-forward encrypted messaging systems, to continue engagements or renew engagements, we will say, in some cases, with European partners on this issue set, and, importantly, continuing to study the problem and to conduct effective oversight of executive branch activities in this area. I look forward to your questions. I will stop there.

Ms. NOVETSKY: Thank you so much.

Yes, so I will ask the first round of questions, and then following that, we will open it up to audience questions, so you can ask questions from that podium and that microphone over there. Just make sure to introduce yourself when you do so.

I will start with you, Anastasiya. Historically, as Justin mentioned, Russian attempts to create an isolated internet for those under Russian control have made life worse for users in many ways. You have written extensively about how local and regional internet blackouts, for example, make it difficult for Russians to complete daily tasks, like withdrawing money from ATMs. However, it seems like recently Moscow has shifted its approach and is prioritizing user experience. It did so, you know, including through the MAX app. Do you think that Russians will mind using the censored internet if the user experience is improved? What further steps could Moscow take to ease the discomfort of using this censored or restricted internet and quell resistance to surveillance and censorship?

Ms. ZHYRMONT: Well, thank you for the question. It is a very justifiable concern indeed that users in Russia, but also in the occupied territories, will, as Laura said, lose the muscle memory to use the independent internet, and will somehow get used to this all limited possibilities. We have seen this with YouTube. Several years ago, two or 3 years ago, it was difficult to imagine the daily life of Russian people where YouTube played a huge role in their daily life, that even if blocked, they would not search for opportunities to circumvent this. The throttling of YouTube, which made it extremely inconvenient for Russians to watch YouTube, actually switched many of them to alternatives, like RUTUBE and other, like, ways to receive this content.

Which, of course, makes us believe that the same will happen with MAX. Indeed, Alanna, not only is it all the entertainment and ability to, well, basically call your friends and relatives, because on other platforms, as I said, video calls are blocked, but also, as you said, it is more and more user-friendly. All the content is in there. All the State services are embedded and funneled through it. If not in the repressive environment, just imagine—all platforms in one app, and you do not need to switch. You do not need to choose. Like, all your friends, all your work-related contacts are in there. Yes, Russian authorities are investing a lot, not only in advertisement of the MAX app, but also in increasing its usability and user friendliness. Russia is a tech-savvy country that can actually compete, at the moment, with all of this.

People also have no choice. We are hearing reports that employers are forcing their employees to install the app. You are somehow banned from the community in those parent or student group chats if you are not using it. You are simply receiving no reports, no updates. It is very difficult not to use it. Even people who are well-aware of all the risks prefer to minimize them through acquiring a new device and installing MAX on it. It is a temporary solution. One way—first of all, not all people can afford to buy a second phone. Of course, one way or another it will become—[phone rings]—oh, I am so sorry—impossible not to use it. So sorry. [LAUGHS]Alert. [LAUGHTER.] MAX app. [LAUGHTER.] Yes.

Ms. NOVETSKY: Thank you so much.

Laura, so you discussed how the Russian government has systematically increased its online information control since the full-scale invasion of Ukraine in 2022, and the deployment of the MAX is sort of the latest step in this progression. What do you think this progression tells us about the Kremlin's longer-term strategy for internet control, both in Russia and in the occupied territories of Ukraine? What do you think is next?

Ms. CUNNINGHAM: Yes. I think what we are starting to see is a very similar kind of Chinese Locknet model being deployed in Russia as well. Obviously, given the differences between kind of the starting points of Russia's infrastructure and China's infrastructure, kind of, that path is going to look very different. I think ultimately the goal that the Russian government is pushing toward right now looks very similar to where China is headed as well. What that is to say is creating, rather than, I think, for a long time, many people thought of, you know, in China they had a great firewall and kind of censorship happened at the border. That was kind of the only impediment to access to the global internet.

What we have seen in China instead is creating these kinds of concentric circles of control, making it more difficult, basically at every step, for a user to access the global internet. Starting with, we see in China a kind of WeChat being this walled garden providing all the information you could possibly want, being, in fact, very content-rich. A place that people are not necessarily dying to escape, so you start with this kind of platform substitution that really captures the audience. Then, adding layers of meta-censorship, making it impossible to even kind of search for or know about circumvention. Even if you wanted to get beyond WeChat, like, what would be the process for that and how? Then seeing VPNs themselves blocked and disabled, so that by the time—you know, even to get to the great firewall, you have had to go through so many barriers and steps of unknown information that is difficult to ascertain even to get there.

What that does, I think, is two things. One, it obviously disincentivizes many users from seeking out—knowing about, frankly, and then going above and beyond to seek out that information. To the kind of muscle memory point, you have a whole generation in China that has started to forget what the global internet looks like. They are no longer compelled by that desire to connect with the international community, to connect with the global internet. I think—I think why MAX feels like such an inflection point for us in the Russian model is because it is starting to create those layers of control, and starting to create a situation where you might actively capture a population on a single app or platform, and start to wither that muscle memory of the global internet.

Which is why I think it is especially critical we have this conversation right now, and we are trying to engage in this topic in this moment. Because you still do have, you know, the majority of the Russian citizenry who remembers the global internet, who still remembers YouTube, who still is eager to access this type of information. I think we will start to see that go away unless we are really actively engaged quickly in the short term to make sure those connections remain open.

Ms. NOVETSKY: Thank you.

Before I open it up, just one more question for Justin. As you mentioned, in recent years, Russian authorities have cracked down on tech developers and other companies that demonstrate any reticence to comply with State orders or try to assert any independence. It seems relatively unlikely that any company like VK would resist government efforts to use and abuse user data collected by MAX. What about American and international companies operating in Russia? Are there ways we can reasonably expect them to resist or refuse to comply with orders and laws that infringe on people's freedoms and violate their privacy?

Mr. SHERMAN: Yes, it is a good—I was going to say, if it is the VK one, that is a short answer. [LAUGHTER.] It is a good question. We have seen—it has been interesting to see—and I, you know, worked on some of these issues as this was unfolding—but companies that, you know, completely immediately left Russia in 2022, that I think did it for good reasons and in a good way. Companies that left for good reasons but did it very poorly, such as—I will not name, although folks will know who I am referring to—but certain telecom companies that left immediately, and immediately the State seized control of the telecommunications fibers and other things that they left there. Which was not good.

Then we have this complicated category, I think like we are talking about, where, you know, a company like Google or Apple does not maintain any more—even though they did and it was used to coerce—they do not maintain a local office anymore in Russia. There is still product presence. There are still questions of, you know, even if, let us say, Apple is not opening up a new store in, you know, St. Petersburg next week to sell the new iPhone, are they still providing security updates to the many, many people in Russia who own existing Apple products, right? All to say, there are all kinds of complex touch points that I think are underappreciated when we just look at headlines that say: This many companies left Russia, or this company does not operate in the country. As we are all talking about, it is a lot more complicated.

In terms of levers, I would say app stores removing VPN tools in particular countries is especially problematic. Even more so, I think—at least, based on what we can see publicly—what might appear to be the absence of real, robust corporate policy around when to do that. I am not saying you should never do that. You know, there have been bad actors known to create VPN apps that are malware. I am not saying you should never take down a VPN, per se. You know, at the whim of the Kremlin, without a robust policy, is not exactly a good framework, so that would be the first thing.

The second, I think, as we are talking about, is that Russia is making a push toward a much more autarkic, maybe the right word, technology ecosystem. In some areas, it is failing miserably. Microelectronics, as we all know, has been one area for years. Russia has basically no manufacturing capacity. All this stuff's either still stolen from the U.S., Japan, the Netherlands, or it comes from China now, but software, as Laura was just saying, is an area where Russia is making a lot of progress. That is another space where we need to think about U.S. companies that touch those firms. For example, if VK—as MAX app spreads throughout parts of Europe—what are U.S. companies' and other companies' positions on working with it, interoperability? You get into all these questions that, you know, unsurprisingly, but I do not think a lot of companies have thought through and will ultimately have serious impacts on the very issues that we are talking about today.

Ms. NOVETSKY: Great. Thank you so much.

If anyone has any questions, I am sure—yes, please. Francois will help with the mic.

QUESTION: Thank you very much. Ray Celeste with Congressman Dr. Murphy.

I wrote a question that was very similar to the one that was just asked, but I think it bears to be asked again. This is what I wrote: Are the tech giants—such as Meta, Apple, Alphabet, and others—doing all they can to combat these shutdowns done under the order of the Russian government? Or are they just hanging back due to fears the Russian government will find ways to hurt their bottom line in other places around the world?

You know, I do not know what the Congress can do. I know this administration maybe they could do more in this area. What that is, I do not know. Maybe you all can talk about that. I do not know if throwing more dollars at it—I mean, we already, you know, throw lots of dollars. I mean, these companies have huge contracts. I remember at one time—you know, I am old enough to remember the BlackBerry.

Well, now everybody in the Pentagon carries what? An iPhone. Who are these trillion-dollar companies? There are all these Meta and Google and, unfortunately, they are making—I do not know if they have a moral compass in that they are making tons of money, these big giant centers that they are building all across the United States, that the administration has brought back all this money, and yet I think they are getting it in both ways.

I hate to say this—they do not care if they get money from democracies or China or these—you know, these dictatorships. They just like money.

Thank you. That is a pretty complicated question.

Mr. SHERMAN: Happy to start. I think it is a really good point.

Sam Bresnick and some others at CSET have written papers on this. I will just say the number of these companies that have pulled out of the Russian market or, as I said, left Russia in some way and signaled a lot about that.

Well, actually, when you look at it, of course, their dependencies in certain other autocratic areas or their dependencies in Taiwan or other places are very, very different, and so this notion that, you know, they would always do that, I think you are right that that is not a correct assumption.

I would say that—can the companies do more to help circumvent? Absolutely. I will kick that to some of the experts here, but the answer is yes, right? We have had cases before where companies have, for example, leaned pretty far forward on domain fronting and other ways of getting around censorship mechanisms and then backed off because of pressure from that government.

Again, we probably know one of the examples I am talking about, but that is an example where if the company really wanted to do more there, they could. What are their pressure points? In Russia's case, it is going to be less market—small market to begin with.

How many users do they have there? You know, we are thinking broad spectrum. If the Kremlin really was mad about that, obviously, there are lots of other ways, including hacking and other kinds of things that you could do to apply pressure to a U.S. tech company.

Again, I think the point stands that, back to your question of incentives, how do we ensure that if they have the capability to lean further forward on censorship circumvention, which technically they absolutely do, and in corporate policy they absolutely do, what are those incentives? I think it is the right question to ask.

I will let my fellow panelists weigh in.

Ms. CUNNINGHAM: Yes, I will maybe add a little bit more fuel to that fire, even.

To take a step back here on OTF, OTF is a U.S. government-funded nonprofit. We receive our resources from Congress. The majority of our resources go to support VPNs that are used by tens of millions of people in authoritarian contexts to access the global internet around authoritarian censorship.

Those exact VPNs that are funded by U.S. Government dollars have been taken out of the Apple store—the Apple app store in China, out of the Apple app store in Russia. I think to Justin's point, certainly the answer should not be never take a VPN out of an app store, but when there are apps actively being funded by the U.S. Government to advance human rights in authoritarian contexts to support our foreign policy and our national security, to see American companies removing them from those app stores and making it difficult if not impossible for those exact users that we are attempting to support to actually access those technologies, I mean, frankly, we are just working against ourselves.

Also, to Justin's point, I mean, it seems like the bare minimum should be allowing those applications to be available to the beneficiaries who need them, to the beneficiaries that those resources are being provided.

Certainly, there are ways to go beyond that in terms of technical support, in terms of public-private collaborations that could help bring down the per-user cost of VPNs. There is a lot of work that could be done proactively once we get over the hurdle of actually being prevented from doing that work and providing those services.

Ms. ZHYRMONT: Well, just adding my two cents in all of this, well, of course, we do understand the pressures that big tech companies might receive from Russia, and it includes not only economic pressure but sometimes, like, physical safety of their former staff or present staff in the country.

It does not mean that there is no way out. Let us see. Like, Google received the very same censorship request to delete all the VPNs, yet they did not follow. Now they are facing this hilariously big fine in Russia. I do not even know how to pronounce this number in English.

It does not mean that I know how to pronounce it in Russian—[LAUGHS]—because it is, like, just a joke. They did not, and as a matter of fact, they are very transparent what requests they are receiving. They are making this public.

At least Apple might follow the steps of their peers, but also, like, this is a slippery slope. Like, first VPNs, but what if later on, Russia asks Apple and Google to delete all the apps of independent media?

Later on, it will follow to further requests. Context is very much important, and a human rights assessment within the context is very much important as well, and, of course, Apple and big tech need to support civil society and digital resilience.

They need to invest their resources into—like, into progress of circumvention tools and finding new creative solutions. This is how they can compensate for some wrongdoings, in a way, but also pulling out completely of the market is not the solution also.

Like, stop providing updates to their own devices, will be the end of the security of users in Russia, because what gives us a little hope that the security features within iPhones will somehow cope with the ability of MAX to gather information from other apps on your devices. Probably in the future, with no support, it will not be the case anymore.

Ms. NOVETSKY: Thank you. Jordan, go ahead.

QUESTION: Thank you so much, Alanna, and to all of you. This is a really interesting briefing, so I appreciate you.

My name is Jordan Warlick. I am a policy advisor at the Helsinki Commission. I can imagine that the MAX app surveillance has probably resulted in a certain amount of self-censorship, which, obviously, can be hard to measure those invisible consequences.

I wanted to ask if there are reports yet of, you know, raids, arrests, or fines, or any other consequences like that imposed on individuals based on information gathered from surveillance on the MAX app or through, as you mentioned, the technical inspections and failure to download the app.

Mr. SHERMAN: Yes. I mean, you mentioned this, Alanna; there was some conversation around the inspections in the occupied territories in Ukraine. I will let Alanna weigh in, too. We were talking about this. I, at least, was not able to discern a particular case yet where someone was arrested.

There were rumors of different kinds of consequences, but certainly the stops are happening. I do not know if others want to weigh in on the Russia piece.

Like, I will just say, you know, VK broadly we know for many years, of course, is a huge source of—your post was flagged, FSB data requests submitted to VK that are, you know, complied with their eyes shut, so, otherwise wide open. They do not really care.

I will just say so, I do not know necessarily. I have not seen any reports of that. I, obviously, do not think that is dispositive of the fact that probably this is already an information source, but I will let—yes, Okay.

Ms. ZHYRMONT: No, we did not receive any reports yet, but I think this is only a matter of time because it is very difficult to promote a new app within the users and to reach this critical amount of users needed if you start with the massive arrests for all who are using MAX.

I think they created the necessary infrastructure. Later on, they will first target people that they want to target among civil society—journalists, opposition leaders, and et cetera, where probably some of them are still in Russia. I doubt that it will reach out massive scale because, like, even with this new law who target people for searching extremist materials, of course, at the moment, many people are still using Instagram, so if you start, like, arresting all Instagram divas in Russia, it will be a bad start. [LAUGHS.]

Yes, the point is that they can target anybody at a certain point, so yes, I will stop there.

Ms. NOVETSKY: Okay, good. Yes, Max, go ahead.

QUESTION: Thank you for—thank you for being here and for the work that you do. It is really important, and it is really eye-opening for me.

I am kind of cursing my parents at the moment. My name is Max—[LAUGHTER]—and I am Max Undeland. I work for Senator Boozman. I do not work for VK. [LAUGHTER.]

I was just wondering what the likelihood is that this app rolls out in countries where maybe there has been a little bit of a Russian lean, maybe in countries that might even be in NATO or Europe and—or to be used in the developing world as sort of a—where there is Russian action present or country where Russia—or countries like the U.S. or Germany or others that Russia might want to influence elections and have disinformation campaigns. What is the connection between them?

Ms. ZHYRMONT: Well, as I mentioned, MAX has been launched in a few neighboring countries to Russia. It has also been launched in Moldova, for instance, which is quite concerning.

It will appear in Europe as well for one simple reason: You need to stay in touch with the close ones in Russia. For them, the only opportunity to be connected with you is through MAX app, especially in the occupied territories.

MAX will appear in Ukraine as well. It is, like, people who want to keep in touch with their relatives in the occupied territories will still need MAX in order to call them, tag them, et cetera. Yes, the simple answer is yes.

Mr. SHERMAN: Nothing to add other than I think Telegram is a great—a different app, different situation, but a great example of where an app that I am sure no one in here is using, perhaps, other than to read Russian posts. You know, clearly backdoored and compliant with the Kremlin and so forth, yet still is quite popular around the world, including in Ukraine, which is an interesting phenomenon.

Ms. NOVETSKY: Yes. Just maybe building on that a bit, like, could you envision a world in which other authoritarian countries or, you know, leaning authoritarian countries might adopt it as a model because it is effective and store the data in their own countries or, you know, use this model even if it is not necessarily the MAX app itself?

Ms. CUNNINGHAM: Yes. I think, as Anastasiya has already said, I think the MAX app is going to find its way to allied neighbors, certainly.

I think, maybe going back to kind of the broader picture on this model-wise just beyond MAX, what I think is really interesting about the Russia model in particular is the ability of other countries to potentially adopt it in ways that other censorship models, particularly the Chinese censorship model, just been too high a bar for most countries.

In the case of China, we see a country that had a centrally controlled or centrally controlled internet infrastructure from the very beginning. They made very few compromises on that and, as a result, were able to kind of perpetuate their control very quickly and centralize their control there.

Most other countries around the world have pretty diverse internet architecture, Russia included, and so there was always a theory that, you know, no one could really follow in China's footsteps because everyone else had kind of let a thousand flowers bloom when it came to the internet.

I think the Russian model is a really interesting counterpoint to that now, where they have taken this—what was a very dispersed network and found a way to actually implement very centralized control, and they have kind of been slowly kind of pulling that control in.

First we saw, you know, through many different laws that they were implementing and then, you know, requiring ISPs to blacklist and then they were requiring ISPs to actually install infrastructure to create, like, centralized control over what is being blocked, and now they have gone so far as to take what was, you know, thousands of ISPs down to basically seven centrally owned ISPs, and that is one example of how they have taken the infrastructure and slowly exerted control over it in a way that has become more and more centralized.

That model, to me, is really fascinating because it is one that another government could replicate. You do not have to say, did you make a decision 40 years ago to forever centrally control your internet? No.

You could take this and potentially replicate it in any kind of environment with—you know, with an authoritarian who is eager enough and has the resources to do it, to actually take something relatively diversified and actually bring that centralized control.

Again, I think MAX is an interesting indicator when it pops up of what governments are thinking and the direction they want to go. The fact that that is matched with a Russian model that might actually enable them to do it, I think, is even more kind of concerning in tandem.

Ms. NOVETSKY: I think we have time for maybe one more audience question and then—yes, Kyle?

QUESTION: Thank you. Kyle Parker, Helsinki Commission.

Laura, I just wanted to clarify. You had mentioned something about Russians losing muscle memory and kind of experience with the open internet. By that, do you mean is it a loss of technical savvy or trade craft, or is it more a loss of interest, initiative, motivation, even hope? That is, I guess, the first question.

The second question for anyone or whoever knows this best, how does the framework and practice of engaging with—so by that I suppose potentially some legislative framework, regulations, also habit and practice, enforcement—differ between Russia, Belarus, occupied territories?

Last—and maybe I missed this at the outset—when we were talking about complicity of Western companies, U.S.-based companies, if Congress were to contemplate something like a foreign corrupt practices act for tech, right, something that, you know, in a sense might liberate them from saying, look, whether we want to do it or not we have to do it and we all have to do it.

Certainly, there would be the moral dimension of that and complicity that could help uncomplicate. Are there enough alternatives out there that its practical effect might just mean a loss of market share for our own tech companies? Thanks.

Ms. CUNNINGHAM: I am happy to start with the first question on muscle memory and then go to others.

On the question of muscle memory, is that kind of forgetting—you know, being less tech savvy, or is it kind of giving up on the memory of the global internet, or I think hope even, as you said. I think it is both, but I think the second bit of that is what is even more troubling.

I am using a lot of China analogies today, but I will do one more on this. There was a really interesting study that Stanford University did with Chinese university students a couple of years ago, and they gave about a thousand university students VPNs. Half of them gave a VPN, said go do with it what you will.

The other half, they gave a VPN and a specific assignment, go research XYZ, and what they found was that the students who were given a VPN and given a specific assignment knew how to use the VPN, went and got the information, came back.

The students who were given a VPN and free range most of them did not use the VPN. Most of them did not know even what they would go search for, given that kind of freedom, and I think that is the really concerning bit, is that they have, like, forgotten even the potential of what the global internet is, the potential of what independent information might look like.

They do not even have that incentive when given the opportunity search something out or know what to look for. That is the kind of muscle memory that I think is most detrimental to be lost in that process. I think certainly there is a tech element to it, but maintaining that connection, especially with Russian users right now to the global internet to independent information, I think that is the most critical bit.

Tech, you can kind of always solve for. Trying to have people understand what the outside world looks like and continue to be incentivized for that, that is a lot harder to rebuild.

Ms. NOVETSKY: Does someone want to talk about the tech company piece of it?

Ms. ZHYRMONT: I can address the issue of how the framework will work in different contexts, like in Russia, Belarus, and the occupied territories.

In the occupied territories, people are extremely vulnerable to this kind of MAX installation and surveillance. We mentioned several times the regular checks, but if not willing to install MAX, you can be subject to further searches, investigations, and et cetera.

Of course, people are willingly installing the MAX apps in order to guarantee their own security. Same as they acquired SIM cards on Russian numbers before because it was impossible to use Ukrainian ones in the current conditions.

In Russia, I might say they are seizing control step by step, so like a frog in a kettle, people are adjusting. They did not ban VPNs per se legally; VPNs are still allowed, but they banned the advertisement of VPNs, so nobody will know about them eventually.

They also did not persecute you before for reading, like, I do not know, independent media, Meduza, or others, but now they will persecute you for searching actively for extremist material, and they can call extremist whatever these days.

Same goes to—yes, VPNs are not banned, but since September this year, it can be aggravated in circumstance in crime, so if you are using a VPN, it can be considered a shady thing to do. People are not—same as they did not shut down the internet all at once, they declared Meta an extremist organization, but Instagram and Facebook were still available.

Then they shut down Instagram and Meta. Then they shut down the other platforms, so people are, yes, adjusting to all of this, and they are willingly switching to Russian alternatives.

In Belarus, in Kazakhstan, in other contexts, it is a bit different because, like, of course, MAX does not go preinstalled on all the devices, and I suppose people want to be so actively downloading it.

If Russian propaganda and Russian advertising come to these countries, of course, they will be exposed to the very same risks. What triggers me the most is also the export of Russian not only technologies or apps, but techniques and authoritarian tactics.

We see more and more how all the countries around Russia are copy-pasting all those legislative innovations like the foreign agent law, anti-extremist legislation, anti-LGBTQ legislation, and et cetera. All this leads to further censorship.

Mr. SHERMAN: I guess that leaves question three—[LAUGHTER]—and I will say, too, right, in a country—like, obviously, as we know, Belarus and Russia have very close intelligence cooperation, the SORM—the actual physical SORM system that Russia uses for domestic internet and data surveillance. There are analogs in a lot of those countries, but Belarus is basically the same architecture, so there are all kinds of other risks there.

FCPA for tech, interesting question. I think I would say we can think about the set of responsible practices that we have been talking about throughout this briefing, around, you know, do companies have policies for takedowns and so forth, and then maybe you could think about some bounds of what is acceptable and not acceptable there.

For example, you know, delete this Navalny app ahead of the election because I do not like opponents, maybe it would not be a real reason to take an app down, but there could be reasons, too.

I think the same thing with—which we have not talked much about, it is a bit outside the remit of the MAX app, I guess. If you own the app a little bit different. Data access requests as well are very complicated and, obviously, in pretty much any country on Earth, there would be data access requests from law enforcement or even from intelligence agencies that—whether every single person in this room would agree or not, I think generally the U.S. Government would agree with, right? Child sexual abuse material enforcement or other things that are criminalized rightfully in most countries, for example.

It is not to say that all data access requests should really be put through some absurd ringer or just denied on their face but, again, I think that is another category where some tech companies have done this, I think, in a thoughtful way over time of saying, we operate in countries that have very strong rule of law; we operate in countries that have very weak rule of law and so we are not going to equate those two.

There are others that do not really draw those lines, and I think that is another place where we can enter into, you know, regimes, sort of throwing around the market pressure as a reason to coerce compliance with outright, you know, dictatorial demands.

Ms. NOVETSKY: Yes, thank you so much, and I want to wrap up in just a minute.

Before we wrap up, I think, you know, it is obvious to many of us sitting in this room and certainly at this table why we care about this, and the human costs of it are obviously, you know, enormous.

I was hoping that someone could touch on why it should be in our interest as Americans and our strategic interests as the United States and the West to promote access to an open internet in Russia and around the world, as we have been talking about.

Mr. SHERMAN: We will go down the line. That is great.

As I mentioned, right, so there is the fact that—Laura can elaborate more on this but, you know, not every country can do the China approach, to be a bit simplistic about it, and so having other ways of approaching internet surveillance and control in other adversarial countries we should be worried about what Russia continues to experiment with and build out.

Two is that there are all kinds of complicated cyber questions—cybersecurity questions, cyber operations questions, et cetera—when an adversary is trying to develop a fairly autarkic technology ecosystem. We are not really going to get into that today, but that is really complicated and concerning from a U.S. military, intelligence, and national security standpoint.

The third, as I mentioned, is alongside undermining human rights and other important, you know, democratic values of free speech and so forth, this is also a way for, much like the biometric surveillance I mentioned, which they're starting to deploy more at the borders in every entry point in Russia, is to root out Western spies, root out Ukrainian spies, root out informants or people who cooperate with anyone to include talking to journalists.

There are lots of cases there where I think from a U.S.-EU-NATO standpoint, we should really be worried about that device-level surveillance and targeting capability.

Ms. CUNNINGHAM: I will reiterate one and then add one more.

I think the reason that most of us are here today, first and foremost, is just the human rights concern and our goal really to be able to empower Russian citizens in particular to be able to exercise their human rights online, and so I think that is first and foremost.

I also think that there are, just as Justin said, real national security concerns that go along with this. A government that is able to kind of fully co-opt their domestic population is going to be in a situation where their citizens are less likely to keep that government in check. It is going to perpetuate authoritarian power. It is going to embolden autocrats if they are able to maintain that type of almost universal control over their populations.

I think, in addition to the very concerning human rights impact on those citizens, the free rein that it gives an authoritarian government to have that level of control should be something that is very concerning.

Ms. ZHYRMONT: Well, it is very difficult to add on top of that, but maybe just to summarize.

If we do not export human rights, access to free information, or creative tech solutions, freedom of expression, then autocrats will export their vision of how the world should work, and they will export those MAX messages, their restrictive legislation.

Ms. NOVETSKY: Thank you.

Thank you all so much for being here, to our panelists and to our audience.

Tune in, we will have another briefing next week on the European and Ukrainian defense supply chain and procurement innovations. Hope to see you all soon, and thanks again to everybody for being here.[APPLAUSE.]

[Whereupon, at 3:08 p.m., the briefing ended.]

○

COMMISSION ON SECURITY AND COOPERATION IN EUROPE

E PLURIBUS UNUM

The United States Helsinki Commission, an independent federal agency, by law monitors and encourages progress in implementing provisions of the Helsinki Accords.

The Commission, created in 1976, is composed of nine Senators, nine Representatives and one official each from the Department of State, Defense, and Commerce.

www.csce.gov

youtube.com/HelsinkiCommission
facebook.com/helsinkicommission
flickr.com/photos/helsinkicommission
x.com/HelsinkiComm