Ukraine’s Rapid Digitalization

*Human Rights Risks and Opportunities in a Postwar Environment*

AUTHORS
Marti Flacks
Caitlin Chin-Rothmann
Lauren Burke
Julia V. Brock
Iryna Tiasko

A report of the CSIS Human Rights Initiative and Strategic Technologies Program
About CSIS

The Center for Strategic and International Studies (CSIS) is a bipartisan, nonprofit policy research organization dedicated to advancing practical ideas to address the world’s greatest challenges.

Thomas J. Pritzker was named chairman of the CSIS Board of Trustees in 2015, succeeding former U.S. senator Sam Nunn (D-GA). Founded in 1962, CSIS is led by John J. Hamre, who has served as president and chief executive officer since 2000.

CSIS’s purpose is to define the future of national security. We are guided by a distinct set of values–nonpartisanship, independent thought, innovative thinking, cross-disciplinary scholarship, integrity and professionalism, and talent development. CSIS’s values work in concert toward the goal of making real-world impact.

CSIS scholars bring their policy expertise, judgment, and robust networks to their research, analysis, and recommendations. We organize conferences, publish, lecture, and make media appearances that aim to increase the knowledge, awareness, and salience of policy issues with relevant stakeholders and the interested public.

CSIS has impact when our research helps to inform the decisionmaking of key policymakers and the thinking of key influencers. We work toward a vision of a safer and more prosperous world.

CSIS does not take specific policy positions; accordingly, all views expressed herein should be understood to be solely those of the author(s).

© 2024 by the Center for Strategic and International Studies. All rights reserved.
Acknowledgments

The authors would like to thank Evan Brown for his research support, as well as Katherine Stark and Julia Huh for their support in the editing and design of the report.

In addition, the authors would like to thank the experts who participated in discussions and interviews during this project under the Chatham House rule, including Lucie Audibert, Tetiana Avdieieva, Grant Baker, Romina Bandura, Katya Lysova, Gulsanna Mamedieva, Lee Matheson, Mari Pedak, and Anastasiya Zhyrmont.

This report was made possible with the generous support of the Open Society Foundations.
Contents

Executive Summary 1
Background on Ukraine’s Digitalization 3
Four Strategies to Center Human Rights in Post-conflict Digital Governance 8
Conclusion and Recommendations 21
About the Authors 24
Endnotes 26
Executive Summary

Ukraine is one of the most digitally advanced and integrated societies anywhere in the world. While its more well-known neighbor in this space, Estonia, began its digitalization in earnest more than 20 years ago, Ukraine’s e-government initiatives have taken place rapidly and largely in crisis conditions. The government launched early innovations primarily to combat corruption, such as the e-procurement platform ProZorro, after the Maidan revolution in 2014, but it escalated its digitalization push after the election of President Volodymyr Zelensky in 2019 and onset of the Covid-19 pandemic in 2020. The full-scale invasion of Ukraine in February 2022 gave even greater urgency to move public services online, and the government was well positioned to respond, building on a foundation that had been laid over the previous four years.

As the government of Ukraine and its international partners look to the postwar future and begin planning for reconstruction, this rapid and widespread digitalization presents both innovative opportunities and unprecedented risks. This report outlines four strategies to center human rights values within a future post-conflict digital governance framework in Ukraine.

First, the government must continue to effectively safeguard e-governance systems and critical private infrastructure from external attacks. The widespread reliance on digital systems means that outages, whether accidental or intentional, will seriously impact the ability of vulnerable Ukrainians to access public services. Similarly, these systems must safeguard personal information from malicious external actors, both state-sponsored and criminal.

Second, even as digitalization continues to expand, government ministries must take concrete action to ensure the accessibility of services for all Ukrainians. Both the public and private sectors
should expand solutions for populations who cannot access online services, whether due to lack of
digital infrastructure, affordability of access, limited digital literacy or Ukrainian language ability,
or disability. The expansion of online access should go hand in hand with offline options to reach
populations whose voices would otherwise be excluded.

Third, the government should engage in dialogue with citizens on the appropriate limitations of
surveillance technologies in peacetime. The success of digitalization relies on public trust that the
government will use data and authorities to benefit citizens and not to undermine their rights.
To that end, the surveillance authorities and tools developed during the war should be subject to
public discussion and debate, and any continued deployment in a post-conflict environment should
be subject to high standards of transparency and accountability.

Finally, as Ukraine works toward membership in the European Union, it will need to ensure
consistency with emerging EU standards on digital technology, including with respect to privacy
and surveillance, facial recognition technology, and other emerging human rights issues. Ukraine
should carefully consider the European Union’s direction of travel as it continues to develop the
legal architecture that governs its digital space.
Background on Ukraine’s Digitalization

The Rapid Rise of Ukraine’s Digital State

Ukraine’s move toward e-government has taken place at unprecedented speed. Estonia—the country most known for its extensive e-government systems—began developing its architecture and socializing the idea of online services with its citizens in the early 2000s. By contrast, Ukraine’s development of digital solutions—which now matches, and in some cases exceeds, Estonia’s own offerings—has taken place entirely since the Maidan revolution of 2014 and in large part over the last four years. This effort has revolutionized how the government of Ukraine manages information and how citizens engage with their government. In 2016, none of Ukraine’s government registries, which house everything from birth certificates to drivers’ licenses, were digitalized. By 2020, nearly all of them were. In 2019, only 8 percent of Ukrainians used online public services; today at least 44 percent of Ukrainians—nearly 20 million people—use the e-government app Diia.¹

ProZorro—Ukraine’s groundbreaking open-source public procurement platform designed to reduce corruption in government projects—was launched in 2015, and the government estimates it has saved more than $1.6 billion (60 billion Ukrainian hryvnia) by using the platform.² Trembita, an interoperability system built on the Estonian model that facilitates the secure exchange of data between users and state databases, began operating in 2019. Working together with the Vulyk automation system that stores digital versions of documents from about 600 administrative service centers across Ukraine, Trembita paved the way for the world’s first fully digital ID, which rolled out in 2020, and which Ukrainians can use as an official form of identification for all government transactions inside the country.
These systems also paved the way for the cellphone app Diia, which launched in February 2020 and offers users access to government services from one digital location.\textsuperscript{3} The app was originally designed to reduce corruption by allowing Ukrainians to directly apply for permits and conduct other basic business with government offices without the opportunity for bribery.\textsuperscript{4} It does not store data directly, relying on Trembita and Vulyk to access information. This provides an important security measure. Before the full-scale Russian invasion, Diia allowed citizens to access 50 government services, including applying for benefits, paying taxes, registering businesses, acquiring permits, and—perhaps most crucially in the context of the war—accessing important documents.\textsuperscript{5} Since then, it has expanded to include over 120 services, with new applications coming online nearly every week.\textsuperscript{6}

However, while Ukraine is a highly technological society, there is a large digital literacy gap, with demographic factors like age, income, geographic location, and gender playing a role. A 2023 survey by the Ministry of Digital Transformation found that approximately 40 percent of Ukrainians aged 18 to 70 had “no” or “low” digital literacy skills.\textsuperscript{7} Age was a major factor; 74 percent of individuals ages 60 to 70 reported low to no digital skills, compared to just 15.4 percent of those ages 18 to 29.\textsuperscript{8} In addition, the ministry found that 60 percent of adults with below average incomes had no or low digital skills, compared to 18 percent of those with above average incomes.\textsuperscript{9} In 2019, during the ministry’s most recent assessment of digital accessibility gaps by geographic location, 20 percent of Ukraine’s rural population had no digital skills, with the majority of those individuals above age 60.\textsuperscript{10} The International Telecommunication Union has also noted a slight gender gap: 82 percent of Ukrainian men and 77 percent of women were online in 2021, suggesting that women in Ukraine may have somewhat fewer opportunities to utilize digital services.\textsuperscript{11} Ukraine will need to continue to address these disparities, alongside other risks, as it ramps up its digitalization efforts.
Comparison of Estonia and Ukraine’s Adoption of E-Government Services

**Estonia**

- **2002**: Estonia launches digital national ID system used for taxes, banking, voting, etc.
- **2005**: Estonia becomes first country to allow online voting in national election
- **2008**: Tallinn starts hosting NATO’s Cooperative Cyber Defence Centre of Excellence
- **2014**: Estonia launches e-residency program for businesses
- **2015**: Estonia creates world’s first data embassy to store critical data abroad
- **2021**: Bürokratt, AI-powered Estonian state virtual assistant, launches

**Ukraine**

- **2015**: Ukraine launches ProZorro public procurement platform
- **2016**: Ukraine adopts Trembita and Vulyk
- **2019**: Ukraine establishes Ministry of Digital Transformation
- **2022**: Ukraine launches Diia.City, tax regime for IT businesses, and wartime features in Diia
- **2023**: Ukraine unveils its AI regulatory roadmap, aims to release AI regulations in 2024

Source: Authors’ research based on multiple sources. Please consult the endnotes for complete references.\(^{12}\)

### The Importance of Building Trust

E-government solutions are often deployed as a strategy to build public trust in government, as has been the case in Ukraine with the ProZorro procurement platform and the Diia app, both of which were designed to reduce corruption. But the reverse is also true: the successful expansion of e-government services requires high levels of public trust, as governments seek to access and collect sensitive personal information online. Trust is especially crucial as e-government evolves beyond the digitalization of traditional government functions like issuing ID cards or business licenses—where citizens might expect their government to already store their information—to the collection and use of newer or more sensitive information such as biometric data, job status, health metrics, or physical location.

The government of Ukraine has already moved in this direction. Electronic health records were introduced in 2019, including newborn registration via “e-Baby” and later electronic Covid-19 vaccination records. “Diia.Digital Signature” allows users to digitally sign documents by taking a face scan on their cell phone, which it then compares to biometric data stored in existing government databases to verify identity in real time. In the context of the war, Ukrainians have been able to use the Diia app to report the location of alleged Russian troops or spies (e-Enemy).
and report physical damage to their homes in order to receive refugee, repair, and economic recovery payments.\textsuperscript{13}

\textbf{The successful expansion of e-government services requires high levels of public trust, as governments seek to access and collect sensitive personal information online.}

Before Ukraine’s 2019 election, trust in government among Ukrainians was the lowest in Europe, at a mere 8 percent.\textsuperscript{14} This rose in the early days of President Zelensky’s term and amid the Covid-19 pandemic to the low 20s, matching highs experienced by previous Ukrainian administrations.\textsuperscript{15} However, the government still faced an enormous trust gap, with more than half the population expressing little or no trust in government. Following the Russian invasion, trust in President Zelensky shot up, hitting 80 percent by May 2023, while 32 percent reported trusting the national government to fight corruption.\textsuperscript{16}

This boost in public confidence, along with Ukraine’s high internet penetration rates and above-average internet literacy, has likely facilitated the relatively easy expansion of Ukraine’s e-government solutions. The creation of a digital state was central to President Zelensky’s presidential campaign, and this theme has remained a priority throughout his time in office. Building on citizens’ enthusiasm for digitalization, the Ukrainian government implemented a successful advertising campaign ahead of Diia’s launch. This campaign, which was supported by the U.S. Agency for International Development (USAID), helped spread awareness of the app and build trust in the government’s broader digitalization goals. Diia was largely welcomed by Ukrainians and did not experience organized opposition during its initial launch or subsequent expansion.\textsuperscript{17} Despite the app’s novelty, Diia launched seamlessly with no glitches and has continued to function throughout the pandemic and war, which has allowed trust to deepen over time. This is evidenced by the addition of nearly 6 million Diia users in 2022, reaching 18.5 million Ukrainians on the app and almost 22 million on the web portal by January 2023.\textsuperscript{18}

Still, in a 2022 Gallup poll, 74 percent of Ukrainians believed corruption was widespread in government and 78 percent believed it was widespread in the private sector.\textsuperscript{19} Ukraine’s score on the Corruption Perceptions Index has risen only slightly—from 25 out of 100 in 2013 to 36 out of 100 in 2023 (lower than Belarus, 37, and only slightly higher than Russia, 26).\textsuperscript{20} However, 2023 saw a decrease in trust following major corruption scandals unveiled by the media.\textsuperscript{21} The World Justice Project Rule of Law Index, which assesses countries on corruption and other factors, placed Ukraine 118th out of 142 countries surveyed in 2023.\textsuperscript{22} As a result, although the war has increased Ukrainians’ confidence in their government, the historical perception of pervasive corruption and recent scandals remain an obstacle to long-term trust building that the Ukrainian government and private sector will both need to overcome.
Furthermore, while the recent boost in confidence is well-earned, driven by the government’s unexpected successes both on and off the battlefield, it is not clear whether it will persist in the long term. In similar circumstances where societies faced a common enemy—the United States after 9/11, France after the 2015 Paris attacks—rapid increases in trust in government quickly fell as the crises passed. To channel this momentum into long-term change, the government of Ukraine must continue to proactively build public trust—not only through the deployment of technology to further its anti-corruption mission but also by maintaining transparency, accountability, and open dialogue about the expansion of its digitalization. Digitalization alone cannot guarantee trust in government; technology can reduce opportunities for corruption, but it can also enable the misuse of data, crackdowns on civil society and free speech, and invasions of privacy. In the end, whether digitalization is a force for good or ill in Ukrainian government will hinge on the transparency and accountability mechanisms that are built into these systems and the enforcement of laws to protect individuals from abuse.

In the end, whether digitalization is a force for good or ill in Ukrainian government will hinge on the transparency and accountability mechanisms that are built into these systems and the enforcement of laws to protect individuals from abuse.
Four Strategies to Center Human Rights in Post-conflict Digital Governance

As the government of Ukraine and its international partners look to the postwar future and begin planning for reconstruction, this rapid and widespread digitalization presents both unprecedented opportunities and risks. This report outlines four strategies to center human rights values within a future post-conflict digital governance framework in Ukraine.

Safeguarding E-Governance and Critical Private Systems from Future Attack

Today, all of Ukraine’s government databases are online and connected by default—including those that handle civil, tax, social security, healthcare, and voter information. This expands the availability of services and creates more efficient and accountable government but also introduces risks of cyberattacks. Breaches could compromise personal data or cut off citizens’ ability to access government websites and applications. Since Ukrainians cannot opt out of the online storage of their personal information, the government’s ability to consistently secure those systems against attack is vital to building institutional trust.  

MITIGATING AND PREVENTING CYBERATTACKS

Cyberattacks can disrupt government activity and threaten critical infrastructure in nearly any country. There are few countries, however, where government services are as dependent on digital infrastructure as Ukraine’s. The e-governance system—and its enormous impact on public trust in government, as described above—is therefore a key target of state and non-state actors seeking to defeat Ukraine militarily or otherwise undermine its sovereignty and stability.
Cyberattacks have been a hallmark of Russia’s efforts to undermine Ukraine’s government, both prior to and throughout the full-scale invasion. In the weeks leading up to and following the invasion, Russian government hackers and private actors launched several cyberattacks against the Ukrainian government and private sector. These included distributed denial-of-service (DDoS) attacks that knocked the Ministry of Foreign Affairs and the Ukrainian embassy in the United States offline.25 Russian cyber criminals also reportedly spread misinformation suggesting that Ukrainian ATMs were offline, presumably in an attempt to undermine the public confidence in the banking system.26 These attacks have continued throughout the war. According to senior Ukrainian officials, Russian hackers were responsible for 1,655 cyberattacks against Ukraine between February and December 2022.27 Of these attacks, more than 300 targeted the security and defense sector, 500 targeted other government entities, and 400 targeted private organizations with a direct impact on civilians (including energy, telecommunications, financial, and software companies).28 One recent cyberattack disrupted access to Ukraine’s biggest cellular network, Kyivstar, for 24.3 million people and damaged the air raid alert system.29

Cyberattacks can disrupt government activity and threaten critical infrastructure in nearly any country. There are few countries, however, where government services are as dependent on digital infrastructure as Ukraine’s.

Ukraine has responded to these threats by implementing state-of-the-art cybersecurity protections that have thus far kept government services online and safeguarded personal data. Diia, for example, does not retain information, which minimizes opportunities for data leaks, and Trembita’s state-of-the-art cryptography ensures that it conveys information securely.30 Investments from allied governments have also played a key role in shoring up cybersecurity defenses. The United States, United Kingdom, and European Union have worked with Ukraine on its digitalization efforts since 2016, via the Transparency and Accountability in Public Administration and Services (TAPAS) project and the EGOV4UKRAINE project implemented through the Estonian eGovernance Academy.31 In June 2023, the United States pledged to provide at least $37 million in cybersecurity support for Ukraine, which would increase total assistance to at least $82 million since February 2022 (of a total $120 million since 2016) to “strengthen Ukraine’s capacity to detect, deter, and respond to cyber incidents and threats, and . . . protect critical networks and digital infrastructure.”32 USAID has also pledged an additional $200 million to fund democracy, governance, and human rights work in Ukraine, which includes funding for the Digital Restoration Ecosystem for Accountable Management (DREAM) project and other digitalization efforts to support Ukraine’s post-conflict recovery.33 The EU4DigitalUA project also provided significant support toward additional Diia functions in response to emerging needs, and the United Kingdom also provided support for cyber incident response, information sharing, software, and hardware.34 In December 2023, the United States and nine other countries formalized the Tallinn Mechanism, an initiative to help Ukraine improve its long-term cyber resilience and defend itself in cyberspace.35
Soon after the conflict began, U.S. private companies worked with Ukrainian government ministries and NGOs to secure critical public and private systems. Google, for example, expanded its free distribution of Project Shield, a DDoS protection solution, to additional organizations within close proximity to the war, which included over 150 Ukrainian institutions as of November 2023. Cloudflare’s Project Galileo, which offers free DDoS protection to NGOs, saw a 177 percent increase in applications for services from Ukrainian organizations in March 2022. Amazon Web Services (AWS) and Microsoft helped private and public entities migrate their data securely to remote cloud servers located outside Ukraine, which has prevented the destruction of data stored on physical hardware. As of June 2022, AWS reported having migrated 10 petabytes (10 million gigabytes) of data from government ministries, schools, and industry to the cloud, with more being migrated each day. However, storing and securing that data is expensive, and the government of Ukraine will eventually need to come up with a long-term plan to finance it. When it transitions into the reconstruction process, Ukraine could consider ways to best leverage partnerships with private technology companies to monitor and respond to evolving trends in the cyber threat landscape.

**REBUILDING AND PROTECTING PHYSICAL INFRASTRUCTURE**

Russia has also targeted the physical infrastructure that supports Ukraine’s digitalization. According to the Ukrainian government, as of October 2022 the Russian military had destroyed at least 4,000 telecommunications base stations, 60,000 kilometers of fiber-optic lines, and 18 TV/radio signal antennas. One year later, Ukrainian minister of digital transformation Mykhailo Fedorov stated that 25 percent of internet networks in the country had been destroyed. Local technicians have since repaired some of this equipment (often at great personal risk to their safety), and the effort has been a top priority for the government, especially in recaptured territories. By October 2022, Ukrainian telecommunications workers had repaired 1,232 destroyed cell towers, including 71 in liberated areas, and provided temporary Wi-Fi hotspots for residents to use in the interim. However, as of December 2022, the full cost of repairing Ukraine’s telecommunications sector was estimated to be $1.79 billion.

For Ukrainians in Russian-occupied territory, access to internet and information has been severely limited and will require substantial work to restore when Ukraine retakes those areas. Ukrainians in those zones have often been cut off from at-home internet access, forcing them to use public Wi-Fi provided by an internet service provider (ISP) that uses Russian-controlled infrastructure, which in turn allows the Russian government to block access to certain content. Ukrainian mobile carriers, internet providers, and television stations are also frequently inaccessible, creating what amounts to an “information blockade” that prevents those in occupied areas from communicating with the outside world, encountering news from sources other than Russian-approved propaganda, or receiving timely alerts of attacks. This formula echoes Russia’s practices in Crimea, where residents are subjected to censorship and surveillance, as well as those exercised inside Russia. In an effort to prevent occupying forces from rerouting ISPs to Russian internet providers located in Crimea, Ukrainian ISPs like Ukrtelecom sabotaged their own equipment as Russian troops advanced, resulting in mass blackouts that further diminished internet access rates in that area.
There are several challenges involved in restoring internet access to previously occupied areas, including the need to secure funding, replace destroyed infrastructure, work around mines, and mitigate continued risks of attack. Still, these activities are among Ukraine’s top priorities, with assistance from the international community. In April 2022, USAID partnered with SpaceX to deliver 5,000 Starlink terminals to the government of Ukraine, which provide satellite-based internet access in areas with destroyed fiber optic infrastructure. In October 2023, Ukraine signed a memorandum of cooperation with Latvia to restore broadband infrastructure that Russia damaged during its invasion, which included commitments to reconnect physical infrastructure, support Ukraine’s access to EU telecommunications funds, and provide guidance on adapting to the European Union’s radio spectrum policies, among other actions.

## Ensuring Access to Digital Services for All Ukrainians

Ukraine’s digitalization effort has taken place in the context of a dramatic rise in internet usage across the population, but gaps in accessibility remain. Before the start of the war in 2022, the World Bank reported that 79 percent of Ukrainians were using the internet—a large number, though lower than some of its neighbors (85 percent in Poland and 88 percent in Russia). Like in many countries, Ukraine’s internet users have largely leapfrogged older technology. The International Telecommunication Union reports that in 2021 and 2020, 91 percent of individuals owned a mobile phone, while only 66 percent of households had a computer. Similarly, Ukraine had approximately 80 mobile broadband subscriptions but only 18 fixed broadband subscriptions for every 100 individuals in 2021. High mobile adoption rates facilitate the use of e-government services via apps, such as Diia, while lower rates of computer usage make more intensive online activities, like remote work or online school, more difficult.

Ukraine boasts an extensive 4G network (92 percent of Ukraine’s population had 4G coverage as of 2021) and has revived plans for 5G development starting in 2024. However, internet accessibility is not consistent across Ukraine. Approximately 65 percent of rural Ukrainian villages are not covered by broadband, while nearly half of elderly Ukrainians say they do not use the internet. In addition, the war has decreased the quality of data transmission by 13 percent for fixed broadband and 26 percent for mobile networks. Disruptions to data transmission can result in slower load times or internet lags or pauses, which make it harder for people to access websites or services that require high bandwidth. As a result, internet users in Ukraine actually decreased by 16.8 percent between 2022 and 2023, and an estimated 7.5 million Ukrainians still did not have reliable internet access at the start of 2023.

Russia’s attacks against Ukraine’s digital infrastructure disproportionately harm refugees, individuals with disabilities, children, and the elderly, some of whom may require additional support and accommodations to access the internet and online resources. There were 2.7 million persons with disabilities officially registered in Ukraine before the war, a number which has likely increased since then. The United Nations High Commissioner for Refugees (UNHCR) has found that many persons with disabilities “face a digital divide that is present due to a lack of accessibility considerations within the digital ecosystem” and that as a result, refugees with disabilities may
have trouble accessing information about and communicating their needs, even when services are available. Though research into this field has been limited, UNHCR notes that digitalization efforts should focus on making technology affordable as well as accessible, and that there should be greater investment in programs that train persons with disabilities in digital skills that they need to fully participate. In July 2023, Ukraine took a positive step in this direction, adopting a resolution requiring all state bodies to make their content more accessible to people with visual, hearing, and motor impairments in alignment with the international standards set forth in the Web Content Accessibility Guidelines (WCAG 2.1). In the private sector, Ukrainian developers are also increasingly adopting WCAG standards following their translation into Ukrainian in February 2023.

RESTORING AND IMPROVING INTERNET AND DIGITAL DEVICE ACCESS
Going forward, Ukraine faces the twofold challenge of reconstructing the infrastructure that has been destroyed during the war while also building out new 5G networks. Major internet providers like Kyivstar, Vodafone, and Lifecell offered 4G coverage for roughly 90 percent of Ukraine in 2022. While the government announced a plan back in 2019 to deploy 5G networks, it was delayed in 2020 and then halted due to Russia’s full-scale invasion in 2022. However, Ukraine has announced more recent plans to roll out a pilot test of 5G in 2024 to continue pursuing the most advanced infrastructure for the country’s increasingly digital needs. The Ukraine-Latvia pact in October 2023 also committed to promoting 5G deployment in Ukraine, building upon Ukraine’s continued pursuit of broader broadband reconstruction in rural and urban areas to ensure more uniform connectivity as online services continue to expand.

Going forward, Ukraine faces the twofold challenge of reconstructing the infrastructure that has been destroyed during the war while also building out new 5G networks.

High-speed broadband access is crucial for Ukrainians to take advantage of digital opportunities, including remote work, online education, and online government resources. Ukraine’s broadband is slower than most in the European Union and United States, meaning that users may struggle to run multiple devices at once, livestream content, or undertake other high-bandwidth activities. Fixed internet connection speed in Ukraine increased between 2022 and 2023, but mobile internet connection speeds decreased during that same period. UNHCR reports that broadband access rates are lower among the rural Roma community in Ukraine.

Along with restoring and improving internet access, Ukraine needs to invest in partnerships that expand digital device access for Ukrainians. The relatively high uptake of mobile devices (approximately 91 percent) among the Ukrainian population facilitates the adoption of smartphone apps like Diia, but the lower rate of computer ownership (approximately 66 percent) could reduce the ability of Ukrainians to engage in remote work or educational activities. International government agencies and technology companies have already supported the accessibility of both laptops and smartphones in Ukraine. These initiatives include the European Union’s Laptops for
Ukraine program that donated over 25,000 laptops, phones, and other digital devices to Ukraine’s schools, hospitals, and municipalities. UNICEF has also given 5,000 laptops and tablets to Ukrainian teachers and 10,000 to students. In addition, HP and Microsoft partnered with local nonprofits, USAID, and the Ukrainian embassy to the United States to deliver tens of thousands of laptops, tablets, and software to classrooms across 12 regions of Ukraine. European operators have also established Wi-Fi hotspots near refugee camps and public transport locations where refugees arrive and have distributed over 2.5 million free SIM cards. USAID has provided almost $1.2 million in FDI to support Ukraine’s tech sector since the Russian invasion, which has improved the sector’s resilience and helped the country to continue its digital transformation.

PROMOTING DIGITAL LITERACY AND LANGUAGE ACCESSIBILITY

To address the uneven digital skills attainment among the Ukrainian population by age, income, geographic location, and gender, as described in this report introduction, Ukraine will need to continue investing in digital literacy resources. In November 2023, the Ministry of Digital Transformation completed the Development of Digital Education Hubs Libraries’ Capabilities project, in partnership with the Ukrainian Library Association and the UN Development Programme, which trained librarians to teach digital literacy workshops to local residents. The ministry also developed a Diia.Digital Education Platform—online education courses that cover basic digital rights and skills for older people and professionals (such as teachers, civil servants, and medical workers). This platform could help Ukraine close the digital literacy gaps that the Ministry of Digital Transformation noted in its 2023 survey. The ministry is also developing a new app, Mriya (or “Dream” in Ukrainian) to expand access to online education for students across the country, with the goal of including all Ukrainian education institutions on the platform by the end of 2024.

In addition to continuing its existing digital literacy initiatives, the ministry should also ensure that Diia and all other government online platforms are available in the languages necessary to ensure access to services for all Ukrainians. An estimated 29 percent of Ukrainians, or 14.3 million people, spoke Russian as a first language according to a 2001 census. That number dropped to 15 percent in 2022 as more people began primarily speaking Ukrainian as an act of resistance after the war started, though it’s unclear if the survey included Russian-occupied areas. In 2019, the government adopted a law making Ukrainian the sole national language and requiring that all public and private enterprises provide all services in Ukrainian. As a result, while Ukrainian versions of digital apps and government services are always available, translations to other languages are not necessarily provided or required. In addition, as Ukraine seeks to attract foreign investment, it could be beneficial to develop English-language services for Ukraine’s growing expatriate community.

Regulating Digitalization and Surveillance with Transparency and Accountability

While many governments collect and store personal information to promote national security or offer essential services, they require strong mechanisms to prevent secondary uses or other privacy violations that citizens might not anticipate. Ukraine is not exempt from this dynamic, especially due to its history of previous government administrations targeting surveillance toward...
The current Ukrainian government’s attempt to purchase Pegasus spyware—technology designed to hack into phones and encrypted communications apps without requiring any user action—has understandably raised red flags among Ukrainian civil society, even though Israel’s export control agency reportedly blocked the sale. This concern is exacerbated by the fact that many of these surveillance developments have taken place in wartime, with little opportunity for public debate. Diia features such as eVorog (eEnemy), designed to allow citizens to report alleged Russian military activities, have generated valuable intelligence in occupied areas but also resemble tactics used by Soviet forces during the Cold War. By December 2022, Ukrainians had provided more than 450,000 reports of suspicious activity around the country. These new social norms, where citizens feel it is permissible and even expected to report on the activities of their neighbors, are a trend that should be subject to public debate, particularly in a post-conflict peacetime environment.

Ukraine’s own domestic laws have not kept pace with its rapid digitalization, leaving legal gaps in permissible uses of surveillance tools and accountability for potential misuse. Over the past three years, Ukraine has enacted new laws that have enlarged the government’s authority to conduct surveillance without a court order. In 2020, Ukraine passed the Law on Electronic Communications, which requires online communications services to retain users’ location data and grant government access during legal investigations. The same year, it adopted the Law on Intelligence, which expands government authority to intercept communications before a court order is issued. The Anti-Corruption Research & Education Centre, which is affiliated with the National University of Kyiv, contends that the Law on Intelligence lacked public input during its initial enactment and transparency during its subsequent use. Under martial law, Ukraine amended its Code of Criminal Procedure in April 2022 to allow law enforcement to access telecommunications systems, including surveillance cameras, without a court order. These new laws have sparked civil society concerns that government surveillance without sufficient checks and balances, combined with a general lack of transparency, could lead to misuse.

New social norms, where citizens feel it is permissible and even expected to report on the activities of their neighbors, are a trend that should be subject to public debate, particularly in a post-conflict peacetime environment.

To provide more transparency on data usage, the Ministry of Digital Transformation has developed a feature in the Diia app that informs the user when their data is accessed. Building in features that reduce bad actors’ ability to misuse data and publicizing those safeguards is vital to getting Ukrainians to download—and continue using—apps like Diia. However, to avoid the misuse of personal data, Ukraine will need to adopt and enforce comprehensive data protection policies.
REGULATING THE DEPLOYMENT OF FACIAL RECOGNITION TECHNOLOGY

Facial recognition technology, which is software used to determine the similarity between two face images, is widely used by many governments and private companies for a range of purposes including law enforcement, fraud prevention, distribution of services, and border management. It is most often used to either identify a person (comparing an image against a database) or to verify a known person’s identity (matching someone 1:1 against an existing record). Facial characterization is a separate but related process used to classify an image according to certain characteristics such as race, gender, or age. Almost 80 percent of countries use facial recognition of some kind; however, the reach of the technology and the legal framework applicable to it differ significantly from country to country. Its use comes with significant human rights risks. These include privacy risks—where personal data can be collected, processed, and shared beyond what is necessary, proportional, or consented to by the user—as well as risks associated with biases and errors built into facial recognition algorithms. The use of facial recognition in public spaces can also have a chilling effect on freedom of movement, assembly, and association.

Ukraine is no stranger to the use of facial recognition. The Diia app uses facial recognition for its “Diia.Digital Signature” function and the “Safe Cities” program uses it for video surveillance in public areas, according to local municipalities. Ukraine began using facial recognition sourced from Clearview AI early in the war—primarily to identify deceased Russian soldiers, as part of an effort to counter false Russian narratives about the cost of the war. Since then, its use has dramatically expanded. Ukrainian government officials and Clearview AI report that as of November 2023, more than 1,500 officials across 18 government agencies have run more than 350,000 searches on the system since the war started. The government of Ukraine has used facial recognition for everything from reuniting abducted children with their families and linking captured Russian soldiers with alleged war crimes to assisting Ukrainians who have lost their IDs and scanning visitors at the border.

Beyond Ukraine’s deployment of facial recognition systems, the Cabinet of Ministers approved a national strategy in 2020 that aims “to embed AI technologies in every aspect of the country’s development.” However, Ukraine generally has not updated its legal framework to address recent developments in artificial intelligence (AI) and facial recognition, leaving government agencies without specific, modern boundaries on their use. Article 40 of the Law of Ukraine on National Police allows law enforcement officers to use “automatic” or “analytical” systems to process photos and videos, but it does not contain clear limitations on such use. Ukraine’s Draft Law No. 8153 on Personal Data Protection, if enacted, would require data controllers to obtain individuals’ consent to process their biometric information, but it would also explicitly allow law enforcement agencies to install surveillance cameras in public. The draft bill includes a general opt-out for automated processing, but it does not distinguish between various levels of risk of AI use.

MANAGING THE DEPLOYMENT OF VIDEO SURVEILLANCE TOOLS IN PUBLIC SPACES

Ukraine adopted a country-wide video surveillance system in 2016 as part of a “Safe City” program. Between 2016 and 2019, more than 6,300 cameras were installed in Kyiv, including 4,000 with facial recognition functions (400 cameras capable of detecting body temperature were also
deployed during the pandemic). As a result, Kyiv has become one of the top 50 most surveilled cities in the world. More than 12,700 cameras were deployed across Ukraine during this period. Initially, management of these systems fell under the jurisdiction of local municipalities. Since the full-scale invasion began, however, civil-military administrations (temporary local government units established by the president) assumed authority over them. In a postwar environment, Ukrainians will need to develop a more transparent and accountable system for regulating the deployment and use of this technology.

In addition, most of the cameras installed in Ukraine are Chinese-produced Hikvision and Dahua devices. ProZorro, the Ukrainian open-source procurement platform, references over 3,000 Hikvision and Dahua-related transactions between 2016 and 2023. In 2020, for example, Kyiv purchased around $21 million worth of Hikvision cameras for its “Smart City” project. Hikvision cameras are installed in the biggest cities in Ukraine and now are under the jurisdiction of military units, security services, municipal administrations, and border guards.

ZTE (a partially state-owned Chinese telecommunications company) has been working with Ukrtelecom and other major Ukrainian telecom operators and enterprises since 2003. Huawei was vital to the rollout of Ukraine’s 2G and 3G broadband networks, which increased Ukraine’s broadband penetration rate from 8 percent to 65 percent between 2016 and 2019. In 2019, Kyivstar, Vodafone, and LifeCell awarded Huawei a contract to build a 4G network on the Kyiv subway system. The State Service for Special Communications and Information Protection of Ukraine signed a memorandum with Huawei to cooperate on issues of cybersecurity and telecommunication, and Huawei has partnered with Diia to open “Diia.Business,” centers that support small and medium-sized businesses, in Kharkiv, Kryvyi Rih, Odesa, and Poltava.

Ukraine has used Chinese technology because it is less expensive to procure than non-Chinese alternatives. However, this partnership comes with inherent risks, as Chinese companies may be required to share data collected by these products with the Chinese government under state security laws. Given the close relationship between Moscow and Beijing, even in a postwar environment Ukraine should be wary of the risk of information sharing between the two. The U.S. Department of Commerce and Federal Communications Commission have restricted Dahua, Hikvision, ZTE, and Huawei from conducting transactions or exporting products to the United States due to national security concerns. The European Parliament has also banned the use of Hikvision cameras within its premises in April 2021, though some individual member states continue to use them. Ten European Union countries have already restricted Huawei from their 5G networks—a decision the European Commission described as “justified and compliant” with the EU Toolbox on 5G Cybersecurity in 2023. As of June 2023, the European Union has reportedly considered mandating a broader ban on high-risk 5G equipment providers, which could include Huawei or ZTE, across member states.
Ensuring Consistency with Emerging EU Standards on Digital Human Rights

As Ukraine continues its ongoing bid for EU membership, it will need to align its legal standards at the intersection of technology and human rights with the rest of the bloc. The European Union has already taken sweeping actions to regulate how digital platforms handle sensitive data and create legal rights for individuals to access and exercise control over their personal information. In 2016, the European Union adopted the General Data Protection Regulation (GDPR), which became one of the world’s most comprehensive data protection laws to date. In December 2023, the European Parliament and European Council reached a provisional agreement on the draft Artificial Intelligence Act (AI Act), which, after receiving unanimous approval from the Permanent Representatives Committee in February 2024, is expected to pass a final vote in the coming months. Since Ukraine’s economy is already highly digitalized, alignment with EU law may require major and difficult changes to its current regulatory structure.

Despite these challenges, EU policy alignment could present practical benefits for Ukraine. In addition to easing its integration into the European Union, the alignment of Ukraine’s digital governance structures could encourage long-term economic and democratic growth in several ways. First, the European Union has taken steps to encourage the free flow of data between its member states, based on shared bloc-wide standards for privacy and security. By aligning privacy frameworks, Ukraine could support the economic benefits of this data-sharing infrastructure, which could lead to multi-sector innovation that the European Commission estimates could generate €270 billion in GDP growth across member states by 2028. Second, harmonization with EU laws could provide a guide for Ukrainian public and private sector entities to address fundamental principles like transparency and fairness in their deployment of novel technologies during the reconstruction phase. Ukraine and EU law could particularly benefit from alignment on the topics of data privacy, facial recognition, and AI—which, in turn, could create long-term consistency.

EU policy alignment could present practical benefits for Ukraine. In addition to easing its integration into the European Union, the alignment of Ukraine’s digital governance structures could encourage long-term economic and democratic growth.

Ukraine’s history of regulatory alignment with the European Union on cybersecurity dates back years, from the start of the country’s digital transformation. Ukraine finalized its Strategy on Cybersecurity in 2016 and its Law on the Basic Principles of Cybersecurity in 2017, both of which contained language of “openness, accessibility, stability and security of cyberspace,” similar to the European Union’s Cybersecurity Strategy. In May 2020, USAID supported the Cybersecurity for Critical Infrastructure program which, among other goals, aimed to update regulations in Ukraine to promote IT growth and cybersecurity. Shortly thereafter, the European Union and Ukraine agreed to establish an ongoing Cybersecurity Dialogue, which subsequently lent economic and
political support to protect Ukraine’s critical infrastructure following Russia’s full-scale invasion. These bilateral Cybersecurity Dialogues coincide with Ukraine’s efforts to further align with EU and international cybersecurity frameworks, including to incorporate Budapest Convention provisions into its federal cybercrime law.

The European Union’s foreign assistance program has also supported Ukraine’s digital integration with Europe. Its Digital Transformation for Ukraine (DT4UA) project has helped add more functions to Diia in response to emerging needs, and it has also supported Ukraine to develop electronic ID infrastructure that is compliant with EU eIDAS regulations. These regulations are a legal framework for the EU interoperability system that facilitates safe electronic interactions for businesses, citizens, and public authorities. Ukrainian electronic signatures and seals on digital documents can be verified in EU member states due to these developments, allowing EU countries to accept electronic signatures and applications signed using the Diia app.

**PROMOTING DATA PRIVACY**

Despite this strong foundation for collaboration, there are still substantive gaps between Ukrainian and EU legal frameworks that require reconciliation, particularly with respect to data privacy. While Ukraine’s 2010 Law on Personal Data Protection (PDP) sets basic guardrails on both private and public sector use of personal information, it contains generalized or outdated terms that predate modern data collection and processing. Data protection experts like Member of Parliament Yegor Chernev and Access Now’s Natalia Krapiva have emphasized the need to modernize the PDP to align with both technological advancements and the GDPR. Members of the Ukrainian Parliament submitted Draft Law No. 8153 on Personal Data Protection (PPD) in October 2022, but the bill has not yet been enacted into law. Draft Law No. 8153 mirrors language within the GDPR, including the individual rights to access or delete personal information, requirements for entities to minimize their collection and retention of data, and enhanced protections for sensitive information like biometrics. In other words, this draft bill could grant individuals legal tools to understand and exercise control over the processing of their personal information, while preventing public or private organizations from using or transferring personal data for unnecessary or abusive purposes.

In September 2022, several Ukrainian government ministries partnered with the Council of Europe to launch an ongoing, two-year “Project on Supporting Implementation of Human Rights Standards in Ukraine” to align data protection laws between the European Union and Ukraine. This project has underscored the need for more specific guardrails within Draft Law No. 8153 on government access to private communications and location data. In addition to the 2010 PDP, Access Now has also advocated in favor of revising the Law on Operative Investigative Activity, which grants law enforcement and intelligence agencies broad authority to wiretap without clear restrictions on purpose or duration. In general, there is little public information on the extent of wiretapping, although rumors of such tactics have appeared in past Ukrainian elections.

If Ukraine’s trend toward more expansive surveillance continues into the postwar period, the country’s practices may run counter to the Council of Europe’s amended Convention 108+ treaty and the European Union’s Law Enforcement Directive, both of which specify that government agencies should limit data processing to what “constitutes a necessary and proportionate measure
Because the EU Charter of Fundamental Rights affirms individuals’ rights to data protection, privacy is afforded high value under EU law. At the same time, it is possible that the definition of “necessary” and “proportionate” surveillance may be higher in Ukraine due to its unique security situation, which may persist even after the war ends. On the other hand, it is also possible that Ukraine’s long-term trade-offs between government surveillance and civil liberties may shift in a peacetime environment, especially as global privacy norms increasingly become a prerequisite for digital trade and commerce. While Article 4(2) of the Treaty Establishing the European Union generally leaves national security matters to individual member states, EU law generally applies in the case of any potential conflicts with national law. Either way, legal and cultural inconsistencies in privacy could create uncertainty for businesses and governments, and both Ukraine and the European Union could benefit from shared standards for government access in non-security contexts in their long-term future.

ALIGNING FACIAL RECOGNITION AND AI POLICIES

The European Union is moving ahead with more prescriptive human rights protections for AI and facial recognition, potentially widening the gap between the current stage of Ukraine’s laws and its technological deployment. The February 2024 version of the European Union’s AI Act would prohibit law enforcement government agencies from using real-time biometric products like Clearview, Hikvision, and Dahua in public areas, except if “strictly necessary” to advance select purposes like counterterrorism or human trafficking. Although it proposes allowing law enforcement authorities to continue to use “post-remote” biometric surveillance in a broader range of contexts, it would subject them to enhanced requirements for “high-risk” algorithms, such as undergoing risk assessments, documenting training datasets for accuracy, maintaining human oversight, and ensuring transparency. The AI Act further considers any AI system related to law enforcement, public benefits, or immigration—even if it does not process biometric data—to be subject to these same guardrails for “high-risk” use. At least four EU member states have already taken actions to either ban or fine Clearview AI under the GDPR, which assigns special protections to biometric information. The GDPR also guarantees individuals a legal right to opt out of AI-based decisionmaking that would significantly affect them—data rights that do not yet exist in Ukraine.

Although the European Union is one of the first governments to finalize a major AI law, AI governance frameworks are still emerging around the world and democratic governments have not reached a clear consensus on their ethical norms. When the Council of Europe adopted facial recognition guidelines in January 2021, it recognized the need for further work: “The use of live facial recognition technologies in uncontrolled environments, in light of the intrusiveness it bares upon the right to privacy . . . should be subject to a democratic debate on its use and the possibility of a moratorium pending complete analysis.” Furthermore, when the Organization for Economic Cooperation and Development (OECD) released landmark voluntary principles on government surveillance in December 2022, it also acknowledged the need for future multilateral dialogues between its 46 member countries to address government access to commercial or publicly available data like Clearview AI. In October 2023, President Biden signed an executive order that recognized the importance of engagement with international partners on voluntary standards to promote the benefits of AI while mitigating its challenges.
Ukraine has already begun to participate in global dialogues on how to define and classify risk in algorithms, where to place clear restrictions on the use of AI, and how to hold human actors responsible for biased outcomes within algorithms. In November 2023, Ukraine attended the United Kingdom’s AI Safety Summit alongside 27 other countries and the European Union. These governments signed the Bletchley Declaration, which pledged to build transparent approaches to address AI risks, support multilateral collaboration on AI safety research, and maintain open international dialogue on the opportunities and consequences of AI. The Bletchley Declaration included a commitment to collaborate “as appropriate while recognising our approaches may differ based on national circumstances and applicable legal frameworks.” These governments will reportedly meet again in 2024, demonstrating the importance of multilateral dialogue—and where appropriate, alignment—on the uses of AI.
Conclusion and Recommendations

By shoring up cybersecurity, investing in digital literacy, and rebuilding damaged telecommunications infrastructure, Ukraine has established itself as a leader in the digitalization of its government and society. This technological transformation has already come with numerous benefits, including more convenient access to services, new remote employment and educational opportunities, and security features in the wake of Russia’s military invasion. However, Ukraine will also need to maintain a strong framework to promote the equitable distribution of these benefits while also mitigating novel risks to data privacy, cybersecurity, and civil liberties in the long term. Below are 10 priority areas for Ukraine to continue building upon its robust technological foundation in a manner consistent with long-standing human rights values.

1. Establish a plan to repair damaged 4G infrastructure and build out new 5G networks that prioritizes responsible procurement and technological advancement. The reconstruction and maintenance of high-speed internet across both rural and urban areas is a prerequisite for Ukraine’s plans to deploy AI, digitalize government services, and expand its IT sector. However, it must also weigh the risks to national security and human rights that Chinese providers like ZTE and Huawei might pose—especially accounting for ongoing concerns raised by U.S. and EU officials. In the end, Ukraine requires a long-term plan to finance the installation and maintenance of cutting-edge and secure telecommunications equipment.

2. Support partnerships with international technology companies to further expand digital accessibility and grow Ukraine’s information technology sector. Building upon support from the international community, Ukraine could consider formalizing
public-private partnerships with international technology companies that have provided devices and migrated essential data to cloud servers during wartime. In addition to encouraging public-private partnerships, Ukraine could continue to promote policies that attract foreign direct investment in the country, including creating a friendly environment for remote IT workers, providing language resources for a global workforce, and supporting digital education and reskilling across the entire population.

3. **Support digital literacy and specialized resources for vulnerable populations.** Building on current initiatives, the Ministry of Digital Transformation could consider broadening the reach of “Diia.Digital Education” and Mriya to center to enhance access to digital literacy trainings for targeted populations, particularly for individuals over the age of 60 or those with disabilities. The ministry could also partner with local groups in areas with low digital penetration to ensure that resources are reaching those who need them most. To support its citizens as they navigate an increasingly digitalized resource system, Ukraine could provide additional resources and training to digital community managers such as the employees of local libraries that have been helping residents withdraw pensions, apply for government assistance, and register businesses through Diia.

4. **Continue following Web Content Accessibility Guidelines (WCAG) as essential resources become increasingly available online.** Both the public and private sectors of Ukraine should continue to follow the WCAG to ensure that any new digital resources they develop are accessible to as many people as possible, including persons with disabilities. In the European Union, the European Accessibility Act sets accessibility rules for many digital products and services from e-commerce websites to smartphones. Ensuring compliance with the EAA could further harmonize Ukrainian and EU standards and enable cross-border commerce of digital goods, increasing market access for Ukrainian individuals and businesses.

5. **Solicit and incorporate feedback from civil society, academia, and general stakeholders on the appropriate boundaries of surveillance technologies in a postwar environment.** After the war ends, Ukrainian citizens may have distinct levels of comfort around surveillance technologies that can pose human rights risks—but could also enhance personal safety or national security. As a result, the government should actively encourage input and feedback from citizens around the long-term deployment of these tools, including facial recognition, public cameras, and location trackers. It could open formal channels (which could include town halls, public opinion surveys, hearings, and more) for interested stakeholders to submit verbal or written comments on the contexts and conditions under which data collection might be permissible, as well as the possible impacts of surveillance on local communities.

6. **Promote user transparency and control over the collection and processing of individuals’ personal information by both public and private sector entities.** Holistic transparency measures—which could include independent audits and public reporting requirements—could increase internal accountability over the collection and use of sensitive personal information. These could support the public’s trust that private companies and
government agencies will only process personal information in a manner consistent with the original purpose of collection, without transferring or storing data for secondary or unnecessary purposes. In addition, mandatory notification of sensitive data breaches to affected individuals could reinforce public trust in the cybersecurity of essential public and private sector systems.

7. **Modernize national data protection laws in line with the GDPR.** Building upon current efforts such as the Council of Europe’s “Project on Supporting Implementation of Human Rights Standards in Ukraine,” Ukraine should consider implementing new safeguards to minimize data collection by public and private entities, especially regarding sensitive data like private communications, geolocation history, and biometrics.

8. **Establish an independent regulatory body to oversee data processing in both the public and private sectors.** While the Verkhovna Rada’s (Ukrainian Parliament’s) commissioner for human rights monitors compliance with the 2010 Law on Personal Data Protection, the commissioner operates as a parliamentary ombudsperson. An independent agency could provide more impartial oversight of public and private sector data processing activities. An independent regulator could also build specialized expertise to swiftly adapt rules to evolving technologies and offer guidance to organizations that wish to facilitate compliance with any new legislation.

9. **Increase staffing and financial resources for privacy regulators.** Historically, the ombudsperson’s data protection department has suffered from persistent under-resourcing. In 2019, it operated with only 13 employees and a budget capped at €150,000, despite overseeing a growing digitalized economy serving 40 million people. Companies that violate Ukraine’s 2010 PDP law are subject to initial administrative fines of approximately €425, which are significantly lower than GDPR penalties. To increase funding for enforcement, Ukraine could increase monetary fines for noncompliance, as well as assess the feasibility of allocating additional government appropriations and levying data protection taxes on technology platforms.

10. **Engage in global discussions on government surveillance, AI, facial recognition, and human rights.** Existing multilateral dialogues, including those led by the Council of Europe, OECD, United Kingdom, and United States, provide forums for Ukraine to shape the development of AI standards. Given Ukraine’s unique national security concerns during the postwar reconstruction period, it can contribute valuable insights on the need to balance privacy and civil liberties protections during the deployment of AI and biometric surveillance.
About the Authors

**Marti Flacks** is the former Khosravi Chair in Principled Internationalism and former director of the Human Rights Initiative at CSIS. The initiative seeks to bring innovative thinking and a multidisciplinary approach to tackle pressing global human rights challenges and better integrate human rights across foreign policy priorities. Ms. Flacks spent more than a decade in the U.S. government, most recently serving at the National Security Council (NSC) as director of African affairs from 2015 to 17, where she coordinated U.S. policy across East and Southern Africa and on continent-wide trade and economic issues. Prior to the NSC, Ms. Flacks spent three years as deputy director of the Office of Energy Programs at the U.S. State Department, leading the department’s work on energy transparency and good governance, and four years working for the U.S. special envoy for Sudan on implementation of the Comprehensive Peace Agreement and the independence of South Sudan. She joined the U.S. government through the Presidential Management Fellows program at the Department of Homeland Security. Prior to joining CSIS, Ms. Flacks served as deputy director & head of the North America office at the Business & Human Rights Resource Centre, a human rights organization focused on the role of business in respecting human rights. Ms. Flacks received a BS in foreign service from Georgetown University, a master’s degree from the Fletcher School at Tufts University, and a JD from Columbia Law School. She is originally from Solon, Ohio.

**Caitlin Chin-Rothmann** is a fellow with the Strategic Technologies Program at CSIS, where she researches the impact of technology on geopolitics and society. Her current research interests include the relationships between data brokers and government agencies, the evolution of news in a digital era, and the role of technology platforms in countering online harmful content. Prior to joining CSIS, she worked as a research analyst at the Brookings Institution, where she primarily
analyzed developments in U.S. privacy and antitrust legislation. At Brookings, Chin-Rothmann coauthored “Bridging the gaps: A path forward to federal privacy legislation” with Cameron F. Kerry, John B. Morris Jr., and Nicol Turner Lee, which put forward a comprehensive framework for national commercial privacy standards in the United States. Her work has been published with CSIS, the Brookings Institution, Slate, Barron's, the Georgetown Journal of International Affairs, the Georgetown Public Policy Review, and the University of Pennsylvania's Regulatory Review. In addition, she has provided commentary for U.S. and international television, radio, and digital news outlets including the New York Times, CNN, CBS News, and BBC News. She has a BA in government and Spanish from the University of Maryland and an MPP from Georgetown University's McCourt School of Public Policy. Her master's thesis, “Examining national privacy laws in the context of international trade,” won a student paper award at the 48th Research Conference on Communications, Information, and Internet Policy (TPRC48) in 2020. She was also a recipient of Public Knowledge’s 20/20 Visionaries award in 2021.

Lauren Burke is the senior program manager for the Human Rights Initiative at CSIS. Prior to joining CSIS, she spent four years as the senior program coordinator for the German Marshall Fund (GMF) Cities program, where she played a critical role in managing the Young Transatlantic Innovation Leaders Initiative (YTILI) and launching the Cities Fortifying Democracy project. Before joining the GMF, Ms. Burke worked as a program assistant on the Middle East and North Africa team at the Center for International Private Enterprise, where her portfolio included business association development in Jordan and Palestine, business advocacy in Lebanon, and promoting enterprise ecosystems in Syria. She also interned at Management Systems International, the International Foundation for Electoral Systems, and the Irish parliament. Ms. Burke holds a master of arts in democracy and governance from Georgetown University and a bachelor of arts in political science from Illinois Wesleyan University.

Julia V. Brock is the program coordinator and research assistant for the Strategic Technologies Program at CSIS. She provides research and program support on a range of issues, including cybersecurity, emerging technologies, digital governance, and the role of technology in power and conflict. Prior to joining CSIS, she worked for the National Association of Attorneys General, where she supported training, research, and developmental initiatives for various attorneys general offices. She has also held internships with the International Rescue Committee and International Association of Women Judges. Julia graduated with highest honors from Scripps College, earning a BA in Middle East/North African studies and politics. She is proficient in Arabic and Spanish.

Iryna Tiasko is a former research intern for the Human Rights Initiative at CSIS. Her research interests include the intersections of technology and human rights, democratization and conflict, and regional security dynamics in Eastern Europe with a focus on Ukraine and Russia. Prior to CSIS, she worked as a research assistant at Georgetown Institute for Women, Peace and Security and as a teaching assistant at the Walsh School of Foreign Service. She holds a BS in international politics from Georgetown University with a concentration in international security and a minor in Japanese. She is fluent in Ukrainian and Russian.
Endnotes

1 Vladyslava Aleksenko, *Diia Mobile Application Case Study Report: Implementation of a Digital Services Eco-

system by the Government of Ukraine* (Ottawa: Office of Senator Colin Deacon, September 2022), https://

static1.squarespace.com/static/63851cbda1f15c69b8a9a2b9/t/6398f63a9d78ae73d2fd5725/1670968891

441/2022-case-study-report-diia-mobile-application.pdf; and email correspondence with Garth Willis,

USAID foreign service officer, December 18, 2023.

2 Tato Urjumelashvili and David Marghania, “Open Contracting in Ukraine: A Collaborative Effort for


org/2015/06/02/open_contracting_in_ukraine_a_collaborative_effort_for_procurement_reform/; and


3 “Цифрова Держава” [Digital state], Державні послуги онлайн [Digital service online], https://plan2.

diia.gov.ua/.

4 Intelligencer Staff, “How Diia Is Becoming the Ukrainian Government’s Real Everything App,” *Intelli-


s-real-everything-app-diia.html.

5 Прес-Офіс Міністерства, Міністерство Цифрової Трансформації [Minister’s Press Office, Ministry

of Digital Transformation of Ukraine], “Михайло Федоров Презентував 100 Перемог Мінцифри

За 2020 Пік” [Mykhailo Fedorov presented 100 successes of 2020], Press release, December 23, 2020,

a-anonsuvav-mashtabni-natsionalni-proekti.


App Accelerated the Digital Transformation of Ukraine; Now Ukraine Is Working to Scale the Solu-


Ibid., 32.

Ibid., 33.


Ibid.


Email correspondence with Garth Willis, USAID foreign service officer, December 18, 2023.

Zapryanova, “Ukrainians Rally.”


40 Storage of personal information by U.S.-based cloud providers could raise longer-term debates about data sovereignty and potential extraterritorial access in Ukraine. Shortly before Russia invaded Ukraine, the Ukrainian parliament enacted legislation on February 17, 2022, to facilitate the migration of public and private sector data to cloud servers. However, many EU member states have expressed concern that the CLOUD Act permits U.S. government agencies to more easily access data that U.S. cloud providers hold all around the world, raising potential privacy and civil liberties concerns. In turn, the European Union Agency for Cybersecurity has proposed limitations on U.S. cloud providers, including Google, AWS, and Microsoft, from operating within the European Union. See Microsoft, Defending Ukraine: Early Lessons from the Cyber War (Microsoft, June 2022), https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK; Georgia Wood and James A. Lewis, “The CLOUD Act and Transatlantic Trust,” CSIS, March 29, 2023, https://www.csis.org/analysis/cloud-act-and-transatlantic-trust; and “U.S. Opening Remarks at the Trade Policy Review of the European Union,” U.S. Mission to International Organizations in Geneva, June 5, 2023, https://geneva.usmission.gov/2023/06/05/us-opening-remarks-at-the-trade-policy-review-of-the-eu/.


43 Bergengruen, “The Battle for Control over Ukraine’s Internet.”

44 Ibid.


Ibid.


“Digital Development Dashboard - Ukraine,” ITU.

Ibid.


Neseniuk, “Electromagnetic Warfare Army.”


Ibid.

Kemp, “Digital 2023: Ukraine.”


Ibid.


Ibid.


Liudva and Avdieieva, “How ‘Clear’ Is the Legality of Clearview AI.”


Євгенія Корольова [Ievgeniia Koroliova], “Інструмент Для Ворога. Чи Дійсно в Україні Треба Заблоковувати Всі Камери Спостереження. - Експерт” [Enemy’s instruments. Should Ukraine ban all surveillance cameras, according to an expert], ФОКУС [Focus], May 19, 2023, https://focus.ua/ukr/voenny-neovosti/56716-instrument-dlya-voroga-chi-diysno-v-ukrajini-treba-zablokuvati-vsi-kameri-sposterezhennya-ekspert.


Ibid.

Самуїл Просяруков [Samuil Proskuriakov], “Камери Спостереження Використовують у Боротьбі з Коронавірусом. Ми Вивчили, Як Ця Система Працює в Києві й Чому Це Небезпечне” [Surveillance cameras are used to detect COVID. We studied how this system works in Kyiv and why it is dangerous], Заборона [Zaborona], April 27, 2020, https://zaborona.com/kamery-sposterezhennya-vykorystovuyut/.


133 “Data Protection Day,” COE.


Ibid.


UN Women Ukraine, “Summary: Digital Empowerment of Women.”


“Data Protection Day,” COE.

